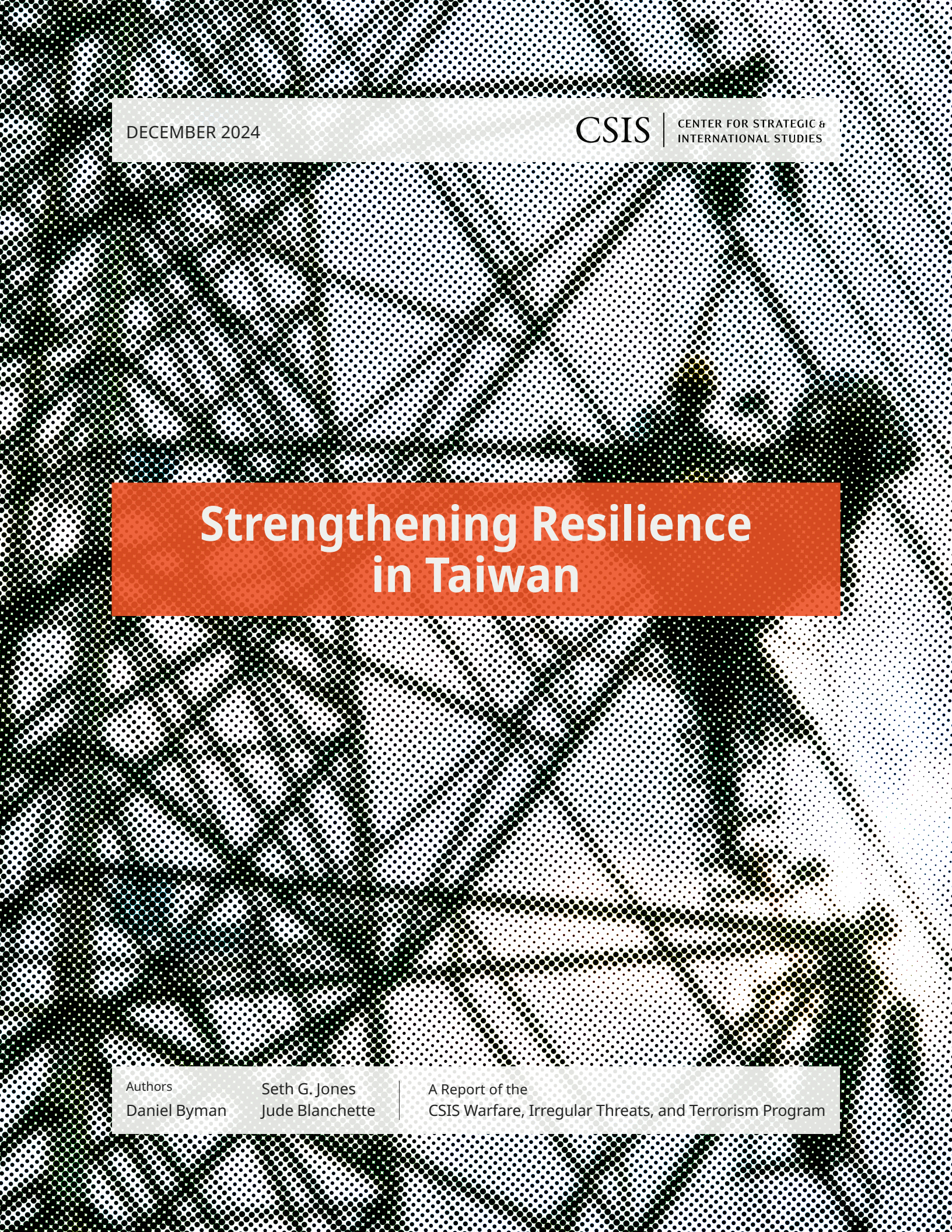
DECEMBER 2024

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

# Strengthening Resilience in Taiwan



Authors

Daniel Byman

Seth G. Jones

Jude Blanchette

A Report of the

CSIS Warfare, Irregular Threats, and Terrorism Program

December 2024

# Strengthening Resilience in Taiwan

Authors
Daniel Byman
Seth G. Jones
Jude Blanchette

A Report of the CSIS Warfare, Irregular Threats, and Terrorism Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

## About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).



ISBN: 978-1-5381-7089-2 (pb); 978-1-5381-7090-8 (eBook)

Center for Strategic and International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

# Acknowledgments

The authors owe an enormous debt of gratitude to the government and nongovernment officials and experts we interviewed from Taiwan, Ukraine, Sweden, Latvia, Lithuania, Estonia, NATO, the European Union, and other governments and organizations. We are especially grateful to officials in Finland for their insights. Many individuals did not want to be identified by name, but they were critical in offering their expertise and time on the topics of resilience in general and Taiwan's overall preparedness. Our thanks go to individuals in the U.S. Department of Defense (especially the Joint Staff and the U.S. Special Operations Command), as well as those in the U.S. State Department and intelligence community, for their insights.

Special thanks go to CSIS president John Hamre for his guidance and thoughts on resilience during the conceptualization, research, and writing phases of this work, including following a trip to Taiwan that he took with two of the authors of this report. In addition, thanks go to Bonny Lin for her comments on Taiwan and to Cynthia Cook for her expertise on resilience. Several others at CSIS—including Jamie Landy, Alexander Palmer, and Katherin Trauger—were helpful in the research and analysis.

Finally, thanks go to the CSIS publications team, including Lauren Bailey, Madison Bruno, Kelsey Hartman, Alex Kisling, Phillip Meylan, and Katherine Stark.

This report was made possible by the generous support of the CSIS Strategic Investment Fund.

# Contents

# Executive Summary

This report examines Taiwan's resilience in the face of external threats, especially from the People's Republic of China. Taiwan's geopolitical, technological, and economic importance in the Indo-Pacific region has made it a focal point of U.S. strategic interests, especially in countering Chinese influence and aggression.

In this report, *resilience* refers to the will and ability of a country, society, or population to resist, mitigate, and recover from external pressure, influence, or potential invasion, as well as non-geopolitical threats, including climate change, natural disasters, and global pandemics. The report develops a framework for assessing a country's resilience that includes eight components: strategic design and command structures, legal authorities, strategic communications, civil defenses, critical infrastructure, will to fight, nonviolent resistance and stay-behind networks, and integration with allies.

In assessing these areas, the report concludes that Taiwan has taken important steps to strengthen resilience over the last several years. But its efforts thus far are insufficient considering the enormity of the near- and long-term threats it faces. For example, while the Taiwanese government conducts annual drills such as the Han Kuang, Wan An, Min An, Tung-Hsin, and Tzu Chiang exercises, which simulate responses to invasions and blockades, there is little evidence of a coordinated and effective civilian readiness program that addresses economic and social disruptions. This gap is critical, especially considering current and future Chinese activities that could target Taiwan's financial systems, electricity grid, telecommunications network, and other aspects of society.

The question of the readiness and resolve of Taiwan's civilian population to resist in the event of foreign aggression also remains concerning. Historically, sentiments seen in widespread public support for movements like the Sunflower Student Movement in 2014, which opposed closer ties with China, suggest the potential for resilience and resistance. However, without clear, robust civil defense education and mobilization strategies, the extent to which ordinary Taiwanese would engage in active resistance remains unclear. As evident in Ukraine's heroic response to Russia's February 2022 full-scale invasion, a population's will to fight is vital not only to the act of resistance but also for galvanizing international support.

**Taiwan has taken important steps to strengthen resilience over the last several years. But its efforts thus far are insufficient considering the enormity of the near- and long-term threats it faces.**

The report also concludes that there is a lack of U.S. and international attention and effort to systematically assess Taiwan's resilience and develop a comprehensive assistance plan to improve resilience. Much of the U.S. military focus has been on providing military capabilities and training to Taiwan to help resist a conventional invasion. The United States has also engaged with Taiwan through initiatives like the U.S.-Taiwan Economic Prosperity Partnership Dialogue (EPPD), which includes a focus on technology and security. However, U.S. efforts have not been sufficient to help Taipei meet the full spectrum of threats it faces, including increasing pressure in the gray zone, or to prepare society as a whole to withstand external threats and coercion. As this report's review of historical cases suggests, a population that lacks resilience is vulnerable to external aggression and internal division. A robust societal resilience strategy is essential not only for deterrence but also for the long-term survival of Taiwan and its society in the face of Chinese aggression.

To help improve resilience in Taiwan, this report contains specific recommendations in such areas as (1) raising threat awareness among the people of Taiwan through a more systematic strategic communications plan; (2) improving ties to the private sector, including companies involved in critical infrastructure; (3) bolstering Taiwan's energy infrastructure, especially in such areas as the power grid; and (4) increasing

**A robust societal resilience strategy is essential not only for deterrence but also for the long-term survival of Taiwan and its society in the face of Chinese aggression.**

strategic reserves and redundancy of food and energy. The report also makes specific recommendations for the United States and other international supporters in such areas as enhancing the effectiveness of the EPPD, bolstering and expanding the Global Cooperation and Training Framework (GCTF), strengthening cooperation between the U.S. Department of Agriculture (USDA) Foreign Agricultural Service and the Taiwanese Ministry of Agriculture, and expanding U.S. military coordination, including in such areas as bolstering the population's will to fight.

These and other steps would not only help strengthen Taiwan's will and ability to resist external pressure, influence, and potential invasion but also strengthen deterrence by raising the costs and risks for an aggressor, reducing the overall risk of conflict.


CHAPTER 01

# Introduction


**Microsoft president Brad Smith announces Microsoft technical assistance for Ukraine, alongside Ukrainian minister of digital transformation Mykhailo Fedorov, on November 3, 2022.**
MICROSOFT/"MICROSOFT ON THE ISSUES"

*"Is this a call to war? Does anyone pretend that preparation for resistance to aggression is unleashing war? I declare it to be the sole guarantee of peace."*

*—Winston Churchill, October 16, 1938*

**Like all previous Chinese leaders, President Xi Jinping has warned that he "will never promise to give up the use of force"** and that he reserves "the option to take all necessary measures" to formally annex Taiwan into the People's Republic of China (PRC).[1] Despite this being Beijing's long-standing policy on Taiwan, past leaders did not have the military capabilities to make good on this threat. But because Xi does, the United States and Taiwan have focused on strengthening defense cooperation to deter the direct use of military force, whether in the form of an invasion or a blockade. There has been far less focus, however, on how China might undermine Taiwan's critical infrastructure, disrupt its economy, leverage a crisis to undermine public morale, or otherwise undermine its overall resilience.

This scenario is not hypothetical: Beijing probes Taiwan's resilience daily. In early 2023, a Chinese vessel was suspected of intentionally damaging an undersea cable linking one of Taiwan's islands to the mainland, disrupting online bank and point-of-sale machines. More recently, a China-linked hacker entity was discovered targeting Taiwan-based semiconductor and aerospace companies.[2]

Serious questions remain about how resilient Taiwan would be in the face of a Chinese invasion or gray zone activity.[3] Taiwan's electricity infrastructure, last significantly updated decades ago, is a critical vulnerability. The grid frequently experiences failures, notably during peak demand periods or extreme weather events. Similarly, Taiwan's communications networks, still reliant on older technologies, face threats of disruption from both physical attacks and cyberattacks, which could isolate communities during crucial times.

Yet there has been little comprehensive analysis of resilience in Taiwan. In addition, the United States and other governments have not developed systematic frameworks to assess the resilience of Taiwan or other countries in the face of foreign threats, identify their strengths and weaknesses, and design aid packages accordingly.

Instead, U.S. military and diplomatic aid to Taiwan has largely neglected the resilience of Taiwan and its society. Much of the U.S. focus has been on ensuring Taiwan has the capabilities to resist a conventional invasion, including providing or selling such weapons systems as F-16 fighter jets, M1 Abrams main battle tanks, High Mobility Artillery Rocket System (HIMARS) multiple rocket launchers, Harpoon coastal defense systems, and Javelin antitank weapon systems. The United States has also provided limited direct training to Taiwan's military, largely owing to the restrictions and ambiguities of the One China Policy, which governs the United States' unofficial relationship with Taiwan. Although these somewhat limited efforts are necessary to strengthen deterrence, U.S. actions and boldness have not been sufficient to help Taipei meet the full spectrum of threats it faces or prepare Taiwanese society to withstand significant external coercion. As a review of historical cases suggests, a population that lacks resilience is in danger from external aggression and internal collapse. As North Atlantic Treaty Organization (NATO) secretary-general Jens Stoltenberg observed in 2020, "Our military cannot be strong if our societies are weak."[4]

## The Challenge of Resilience

Taiwan's dilemma, however, is not unique. Many countries must manage the risk of aggression from powerful neighbors, and Taiwan can learn much from their example. Some countries focus heavily not just on a strong military but also on building societal resilience, an elusive concept involving all of society. The Swedish Ministry of Defence defines resilience in its *Resistance Operating Concept* as "the will and ability to withstand external pressures and influences and/or recover from the effects of these pressures or influences."[5]

As used here, resilience is the will and ability of a country, society, or population to resist and recover from external pressure, influence, and potential invasion as well as major natural disasters such as hurricanes and pandemics.[6] In practice, resilience has many aspects ranging from practical questions, such as how to keep the lights on, to ineffable but vital issues such as building a will to resist and will to fight among the population.[7] Resilience is related to resistance, which includes nonviolent and violent activities to reestablish independence after conquest by a foreign power.[8]

The world saw such resilience in practice in Ukraine. After Russia seized Crimea in 2014 and then fomented an insurgency in eastern Ukraine, the Ukrainian government and society responded effectively to Russian cyberattacks and aggression below the threshold of conventional war.[9] After Russia's full-scale invasion in February 2022, Ukrainians quickly rallied to resist the occupiers. Their resistance efforts, ranging from removing road signs to confuse occupiers to sabotage and assassination, slowed advancing forces, providing valuable time to organize Ukraine's military forces to repel invaders and gain international support. In addition, resilience made life better for ordinary Ukrainians, preserving vital health services and transportation.

Although resilience is vital in a crisis, its greatest value lies in amplifying deterrence. If a country is seen as difficult to disrupt, conquer, or occupy, it becomes a less attractive target, and could change the calculus for the aggressor. Conversely, if an adversary perceives a country as lacking resilience, it may be an appealing target. The 2022 U.S. National Defense Strat-

egy emphasizes the need to build resilience to help advance collective NATO security. Indeed, democratic societies can excel at deterrence by strengthening resilience, drawing on whole-of-society approaches more effectively than autocracies.[10] Finnish scholars have referred to this logic as the idea that "even the biggest bear will not eat a porcupine."[11] During the Cold War, the Baltic states, Norway, Sweden, Switzerland, and other countries pursued a "porcupine" strategy, and some have renewed these programs in the face of renewed Russian aggression.[12]

In recent years, both NATO and the European Union have embraced resilience. The European Union has a Critical Entities Resilience Directive that provides mandatory standards to EU members. Europe, in general, is also improving its standards. NATO has had resilience goals since the 1950s, but often, until recently, these were honored in the breach.[13] Not surprisingly, since the invasion of Ukraine, NATO has emphasized that all its members should build resilience.[14]

Should Taiwan become more resilient, it would be far better able to resist pressure from China, and strengthening deterrence would make an invasion less likely. Before a crisis, Taiwan's infrastructure and morale would be more difficult to disrupt, and various gray zone strategies to create instability would fail. If crisis looms, Beijing's leaders would know the Taiwanese will resist and are well-prepared to do so. Further, should China occupy all or part of Taiwan, this propensity to resist would dramatically complicate Beijing's plans to fully annex the territory.

Ukraine and Taiwan are not alone. Autocracies often use hybrid warfare and other means to undermine resilience and weaken liberal democracies. Thus, lessons that apply to these and other countries are relevant to a wide range of U.S. allies and partners.[15]

# Methodology and Research Design

To examine resilience in Taiwan, this report asks three questions. First, what is resilience, and what are the various factors that comprise it? Second, how resilient is Taiwan in the face of a threat from China? Third, what steps can Taiwan, the United States, and other partners take to increase resilience in Taiwan?

To answer these questions, this paper draws on several sources. First, it draws on a large volume of secondary literature on resilience. Second, it examines secondary and primary sources from NATO and resilience leaders like Finland. Instead of conducting comprehensive case studies, the authors integrated lessons from several countries with a history of resilience, such as Estonia, Finland, Israel, Switzerland, and Ukraine. Third, the authors conducted interviews on background about resilience in the United States, Taiwan, Finland, Estonia, Ukraine, and Israel. The interviews were conducted on the condition of anonymity; in some cases, a general descriptor is provided, while in others the person is not acknowledged as the source.

While it is important to examine lessons from other countries for Taiwan, resilience is context specific. For example, Finland's history (including the November 1939 Soviet invasion during the Winter War), geography (particularly the 833-mile border with Russia), conscription, and other social, cultural, and historical factors have contributed to a sui generis form of resilience. There is, of course, no cookie-cutter solution to strengthening resilience in Taiwan. Nevertheless, this report identifies several factors Taiwan should consider and apply in its own way.

# Outline of the Report

The remainder of this paper has four chapters. Chapter 2 briefly discusses the different dimensions of resilience, noting how resilience matters before, during, and after a potential invasion. The report then identifies different components of resilience, ranging from initial strategic design to protecting infrastructure to developing the capacity to work with supporting countries. Examples from Finland and other countries illustrate these elements. Chapter 3 assesses the state of Taiwanese resilience today. Chapter 4 outlines recommendations, including what Taipei might do to improve resilience in the future and how the United States and regional partners might bolster Taiwanese resilience.

CHAPTER 02

# Building Resilience

**A car burns inside the yard of a hospital in Mariupol, southern Ukraine, on March 9, 2022.**
EVGENIY MALOLETKA/AP

**Resilience is vital at different stages of a conflict.** It is meant to supplement, not replace, traditional military-focused deterrence and defensive measures. One of the most important roles of resilience occurs before a conflict begins. A country believed to be resilient is likely harder to conquer and subjugate. Attackers know that the defenders are prepared and likely to fight and that controlling the population will be difficult and resource intensive. One interviewee referred to this as "deterrence by frustration."[1] Most resilience activities are open; thus an adversary observes many of them in advance.[2]

Should deterrence fail, resilience is also vital during gray zone conflict, or conflict short of all-out hostilities. Adversaries may try to undermine faith in government by disseminating disinformation, launching cyberattacks that disable critical infrastructure, or backing minority groups or political factions that are potentially hostile to the government. Russia sent "little green men"—armed soldiers without insignia who denied ties to Moscow—as part of its successful effort to seize Crimea from Ukraine in 2014. Resiliency efforts that ensure robust infrastructure, educate the population to counter disinformation, enable the government to act decisively in response to covert provocations, and reduce social cleavages all make a country less susceptible to subversion.

At the initiation of all-out war, resiliency takes on additional roles. Adversaries' efforts to take down

power and communications through physical and cyber means affect the warfighting capability of the defending state. A local population can provide intelligence to the adversary or the host nation, aiding the targeting of either side. Lack of resistance can free up adversary forces, helping them devote additional manpower to the front lines.

Finally, resilience is vital should an adversary defeat a host nation's military forces and impose its government on the country. A resilient society can make it harder for the occupier to consolidate its political and economic position.[3] In addition to helping basic services reach a needy population, resiliency can reduce the impact of adversary propaganda and preserve forms of legitimate government. Resilience may involve passive resistance, where workers slow their performance, miscount goods sought by the enemy, or otherwise hinder the adversary war effort without violence.[4] Resilience through better communications and infrastructure can also ensure lifelines to friendly foreign governments, including the United States, which may represent the best hope of liberation. More broadly, resilience sets the stage for successful resistance, which, though not the focus of this study, makes guerrilla war and counterattacks easier.

# Components of Resilience

Resilience has many components. NATO, for example, has stressed the necessity of continuity of government; energy, food, and water supplies; civil communications; and maintaining transportation systems, among other needs. NATO's Resilience Committee has an array of specialized planning groups to this end.[5] Finland, perhaps the world's leader when it comes to resilience, has a different approach to resilience, highlighted in Appendix A. Its diamond model includes such categories as psychological resilience; leadership; international and EU activities; defense capability; internal security; functional capacity of the population and services; and economy, infrastructure, and security of supply.[6] Finland also has developed 57 tasks for resilience, presented in Appendix B.

As illustrated in Table 1, this chapter details eight key components of resilience: (1) strategic design and command structures, (2) legal authorities, (3) strategic communications and educating the population, (4) civil defenses, (5) critical infrastructure, (6) will to fight, (7) nonviolent resistance and stay-behind networks, and (8) integration with partners and allies. The authors identified these components, which represent a framework for understanding resilience in a given country, based on an overview of historical cases, interviews of experts, and relevant literature. The rest of this chapter describes each of the components.

## Strategic Design and Command Structures

Governments require an overall plan that incorporates the many aspects of resilience, specifying the general goals, division of labor, conditions under which parts of the plan go into effect, the locations of caches of medical and communications equipment, and other essentials.[7] It is vital to have a lead agency that develops and coordinates resilience efforts. Often the ministry of defense or its equivalent is the lead planning entity, though there are many possibilities. Other agencies take responsibility in their bureaucratic realms. A ministry of justice might prepare necessary legal authorities to monitor and arrest suspected subversives in advance of a crisis and increase surveillance when necessary. Agencies involved in disaster response or civil emergencies might prepare to ensure the robustness of the electricity grid and alleviate food and medicine shortages. The communications ministry might develop a narrative and distribute preparation materials, while the ministry of foreign affairs might focus on where a government in exile might go and how to ensure external backing.

Duties will vary depending on the relevant stage. Before a crisis, for example, a disaster response–focused agency might educate the public on resources available in a crisis. When the crisis begins, it might turn its focus to identifying shortfalls and implementing protocols. If the enemy occupies the territory, the agency might help the population prepare for power shortages during combat. The list is long.[8]

Resilience is an all-of-society effort. Government usually leads in planning, but civil society and especially the private sector are vital, especially as much

| Components of resilience | Overview |
|---|---|
| **Strategic design and command structure** | Overall plan incorporating various aspects of resilience, such as the general goals, division of labor, conditions under which parts of the plan go into effect, determining budgeting, and other essentials. |
| **Legal authorities** | Laws, policies, and procedures regarding necessary actions to take in—and leading up to—a national emergency. |
| **Strategic communications** | Communication with the public in advance of a crisis and during a national emergency, including during situations when communications are disrupted, disinformation is high, or some of the population is under occupation. |
| **Civil defenses** | Civilian preparations for a national emergency, such as storage of batteries and water at home, training for medical and rescue services, and preparation for guerrilla resistance. |
| **Critical infrastructure** | Public-private sector preparations to continue critical infrastructure services during an emergency, such as in the energy, communications, transportation, water, financial services, healthcare and public health, food and agriculture, emergency services, and information technology sectors. |
| **Will to fight** | Willingness of a population, part of a population, or country to resist an adversary in various ways, including by fighting. |
| **Nonviolent resistance and stay-behind networks** | Networks designed to stay behind in the event of an occupation to help organize local intelligence. Stay-behind networks might include those focused on logistics, messaging, education, transportation, sabotage, or medical support. |
| **Integration with allies and partners** | The establishment of diplomatic, economic, and military relationships with external allies and partners to bolster resilience. |

▲ **TABLE 1**
Components of Resilience

**SOURCE** CSIS analysis.

of the critical infrastructure and other capabilities are in the hands of business—a shift from the Cold War era. In 2016, 90 percent of NATO military transport came from the private sector, as did much of NATO's satellite communications.[9] There must be a planning and command structure that integrates the private sector so the business community knows its roles before and during a crisis and the government knows businesses' requirements, needs, and limits. Although all these actors are important, the most crucial is an empowered and motivated population that is psychologically prepared to deal with a threat. In a crisis, resilience largely involves bottom-up efforts or coordination without government assistance, so strong connections and extensive preparation of citizens are vital. Efforts must be updated regularly as threat conditions change and capabilities move from one entity to another.

An important task is to identify and reduce vulnerabilities before a crisis. NATO has put forward some evaluation criteria to help with resilience assessment.[10] The range is vast, from anticipating and countering adversary propaganda to securing borders,

building cyber protection, and developing rapid-repair capabilities. Governments must determine who will oversee testing and then regularly test capabilities through exercises.[11]

Finland provides a useful model for strategic design and command structures. Its *Security Strategy for Society* outlines a comprehensive strategy jointly formulated by the government and representatives from the private sector, though the planning process includes opportunities for contributions from civic organizations.[12] The concept of preparedness planning outlined in the strategy involves not only national preparedness but also independent preparedness of businesses, communities, and individuals.

Finland seeks to integrate different components of government, business, and society. The Ministry of Defence runs the 24-person Security Committee, which meets monthly with government representatives from various ministries, with representatives from the president's office, businesses, and nongovernmental organizations (NGOs).[13] By bringing together different parts of society outside the government, the goal is a broader "network of trust."[14] Numerous structures at the regional and municipal levels design local approaches that involve the government, businesses, civil society organizations, and communities. The government's role is based on law, while the role of business is based, in part, on law but often on agreements and voluntary decisions. By contrast, civil society and community participation is often voluntary. The goal is a scalable concept where municipalities are in the lead at the local level while the national government is in charge of the whole country.[15]

The goal of the resilience strategy is not for resilience alone to allow Finland to triumph against a threat. Rather, part of the goal is to help Finland survive on its own for several weeks, or perhaps several months, until allies can come to its assistance.[16] In addition, the purpose is to reduce the cost of conflict to society.

Finland's Ministry of Defence plays a lead role, outlining vital functions that must be preserved. Under the ministry, which coordinates and advises (but does not direct) various other ministries, the Security Committee is a key coordinating body, with high officials from other ministries participating. The Security Committee produces a joint situation report and works across the government, while individual ministries are responsible for preparedness in their domain.[17] For example, the Ministry of the Interior has prepared a National Risk Assessment that identifies a range of threat scenarios, including financial pressure, terrorism, and communications technology disruption.[18] This assessment is published every three years, but authorities constantly assess the threat situation.[19]

Finland regularly updates plans to ensure that changing technologies, business models, and other factors are properly integrated. For example, it updates its risk assessment every three to five years.[20] It also makes changes in response to world events, such as increasing the required grain supply reserve after the invasion of Ukraine.

In Finland, government bodies conduct drills and emergency exercises to identify potential weak points. Some of these are tabletop exercises, while others are real-world ones.[21] For example, Finland "cut" power cables in exercises to test repair and response capacity in certain parts of the country.[22] Civil-military relations are at the core of successful resilience. In almost every aspect of resilience design and strategy, civil authorities and civil society participate in the process. As one Finnish official stated, "If that works, all is well."[23]

## Legal Authorities

Resilience functions must be legal, and the government's legitimacy must be sustained. But crises and war can strain these essentials. NATO stresses "continuity of government" as a core part of resilience and civil preparedness.[24] The law must recognize the risk of subversion and make provisions to prevent hostile foreign ownership of sites near military bases, defense production facilities, energy plants, and other critical infrastructure. Governance and legal legitimacy must adjust between peacetime, wartime, and occupation.

Legislation might empower certain local bodies under occupation conditions or, conversely, declare in advance that any government body within occupied territory does not have authority—a way of denying legitimacy to actions by puppet governments and local quislings. Governments will also need to prepare

a body of laws that allow for operational security and resistance to the occupier, most of which are well outside typical democratic civil codes.[25] For example, many countries in Europe have strict limits on the use of their militaries in domestic situations, but those would need to be amended to handle foreign paramilitary forces masquerading as civilians, as happened in Crimea.[26]

Finland has numerous laws on the books for emergency circumstances, and these come into play if Parliament invokes an emergency. Charly Salonius-Pasternak of the Finnish Institute of International Affairs calls this the "boring, unsexy work" vital for preparedness.[27] For example, Section 111 of the Emergency Powers Act states, "In order to increase or maintain military defense readiness . . . the defense forces can, by decision, oblige companies, communities, institutions, and professionals and entrepreneurs to provide the defense forces with renovation, accommodation, repair shops, maintenance, construction and other similar services."[28] In addition, the government can give orders to civilian industry regarding whom they sell to and what they sell.[29] Other parts of the act offer guidance on forced recruitment, wages, requisitioning buildings, and other concerns.

In a crisis, Finland has a series of laws that go into effect, such as automatically allowing reservists to be called up for more than the peacetime maximum number of days or allowing companies to cooperate in ways that, in peacetime, would be considered cartel behavior.[30] The Ministry of Interior also has greater authority to conduct investigations during an emergency, though there is still strong respect for the rule of law. After Russia's invasion of Crimea, Finland amended the law, allowing the military to use force in such circumstances.[31] During the Covid-19 pandemic, Finland invoked the law for the first time since World War II.

Finland also has laws that allow the government to deny property purchases close to military bases or critical infrastructure; it has done so to block Russian purchases of real estate near Finnish industry and military bases in the east.[32] The government may also remove or block companies with subpar critical infrastructure, enabling it to remove companies like Huawei if necessary.[33] In 2024, Finland's government proposed a widespread ban against Russian citizens from buying property in the country, though it exempted dual Finnish-Russian citizens and Russians with permanent residence in Finland or other EU countries.[34]

The government must also plan for its own displacement, exile, or diminishment and ensure it retains legitimate legal authority. In such circumstances, some members will likely be absent, elections will not occur, and other basic components of a democratic system may be lacking. During a conflict, leaders may have to flee one part of the country for another or enter exile, which may require identifying an ally that will host the government-in-exile. In 1940, Latvia authorized its ambassadors in the United Kingdom and the United States to control state money deposited abroad.[35] During the Cold War, Switzerland arranged to have a government-in-exile in Ireland should it be overrun. Norway put personnel records and other information relevant to running a resistance in its embassies in London and Washington. That government-in-exile must maintain contact with, and ideally some command over, any shadow government established in occupied areas.[36]

## Strategic Communications and Educating the Population

Governments must communicate with their publics in advance of a crisis and have means to do so in situations when communications are disrupted, disinformation is high, or some of the population is under occupation. In crisis situations, there is a strong risk of competing narratives, themes, and messages as the adversary sows disinformation and uses its communications to appeal to disaffected minorities and others who might embrace its message. Because of the importance of information operations and propaganda to warfare, helping the population identify and resist propaganda and misinformation is also vital.[37]

In 2015, the Lithuanian government disseminated *Prepare to Survive Emergencies and War: A Cheerful Take on Serious Recommendations*.[38] The 75-page instruction manual offers information on how Russia might conduct information operations, provides images of Russian weaponry so citizens can provide intelligence more accurately, and repeatedly stresses the

need to resist, among other important information. Latvia and Estonia have published similar manuals. Sweden's version—*If Crisis or War Comes*—details how the population should survive without government assistance: "If Sweden is attacked by another country, we will never give up. All information to the effect that resistance is to cease is false."[39]

Finland has similar efforts. It produced a 19-minute film, *Battlefield 2020*, to introduce its population to what modern war might look like. The film depicts cyberattacks on the financial infrastructure, sabotage of water supplies, and other aspects of conflict beyond war itself.[40] Since the February 2022 full-scale Russian invasion of Ukraine, Finnish media have widely distributed video footage and other imagery of Russian missile and drone strikes against Ukrainian civilian and defense targets.

In normal times, each Finnish ministry is highly independent and plans its own communications related to comprehensive security for its area of focus. In a crisis, however, the Prime Minister's Office has more authority and resources to increase its staff, and in a true emergency communications become far more centralized.

The Finnish Ministry of Defence also conducts regular courses for business leaders, politicians, media leaders, and religious figures, among others, with tens of thousands participating, often at a regional level. There are three courses: one at the national level that runs four times a year and lasts three-and-a-half weeks, specialized courses that run two or three times a year and last two-and-a-half days, and regional defense courses that run 20 or more times a year and last for a week. Around 10,000 people have gone through a course at the national level, 3,000 at the specialized level, and 65,000 at the regional level. Such courses, which are by invitation only, are, in part, intended to discover what problems individuals and businesses would face in a crisis, give people a shared threat and response structure, build bonds among participants, and educate people on likely difficulties.[41] An invitation to such courses is prestigious: participants are "joining the anointed."[42] Further, trainers attempt to impress participants, such as by showing them military systems. This contributes to a will to fight by bringing a broad range of important people into the national defense.[43]

In general, Finland is well prepared for resisting disinformation: corruption is low, confidence in government is high, the population is highly educated and learns media literacy, and there are few social cleavages to exploit. NGOs patrol for disinformation, and the Strategic Communications Office in the Prime Minister's Office analyzes the information environment for disinformation about Finland.

Finnish media also play an important role in combating disinformation. As free media, they often take the lead in determining what is accurate, with government officials simply advising them of possible disinformation and the media making decisions about whether and how to respond. In addition, the state national broadcasting company Yle provides a reliable media source and has a legal obligation to communicate with citizens during a crisis.[44] This independence, however, diminishes in an emergency, and the Prime Minister's Office can censor media.

Attribution is often an important part of successful strategic communications and reducing the impact of disinformation. In particular, governments may need to identify who is behind disinformation to discredit it and properly educate the population. In addition, successful attribution makes a population angry at foreign subversion, not at their own government, should the electricity fail or another problem develop.[45] At times, a "name-and-shame" approach may make an adversary less likely to act: for example, the legal process can highlight the hostility of a potential adversary even if its operatives do not show up in court.

## Civil Defenses

A resilient population prepares for a conflict and must be involved in designated services that increase resilience in society as a whole. For example, individuals might store batteries and water at home to better manage disruptions. They also might be assigned emergency roles, such as medical and rescue services. Many might serve as auxiliaries to an underground resistance, assisting with procurement, recruitment, early warning, media distribution, intelligence collection, and other vital roles. Both the government and voluntary organizations can organize some of this in advance of a conflict.[46]

Citizens need places to shelter in case of attack and must be able to receive important medical and other services. It is also vital for municipalities and civil society organizations to be prepared to evacuate the elderly, the sick, and other vulnerable populations.[47] During the Cold War, the Swiss prepared fighting positions at key locations, such as near or at bridges, tunnels, or hillsides to increase the effectiveness of small units in case of an invasion.[48] Swiss efforts were part of a concept of "total defense," which involved a whole-of-society approach to defending the country.[49]

Finland uses the Local Forces—or reservists who volunteer for additional exercises and duties and are called up in the case of natural disasters—to bolster preparedness. It also has plans to evacuate the civilian population from certain areas where fighting will likely be intense.[50] The country is also prepared for bombing. By law, all large buildings must have bomb shelters. Car parks, swimming pools, and other facilities can also be converted into bomb shelters.[51] Jarmo Lindberg, the former chief of defense, says underground Helsinki "is like Swiss cheese," with tunnels throughout, and all military headquarters are under "30–40 meters of granite."[52] Many of the large shelters are important civic spaces in peacetime, hosting sports facilities, parking, and school sports games and activities, or otherwise serving dual purposes, ensuring they are regularly used. All of Helsinki can shelter in an attack, and Finland has 45,000 civil defense shelters, which can accommodate more than half its population.[53]

Finland has also prepared border areas for attack. These include creating limited defenses to slow attacking forces, thus giving the local population more time to evacuate. In addition, by working with local communities in peacetime, the Finnish government has developed extensive evacuation plans.[54]

## Critical Infrastructure

Morale and well-being depend on continued electricity, communications, energy, healthcare, and other essential services. These types of critical infrastructure require general hardening to make disruption more difficult and improve redundancy and rapid repair capacity in case disruption occurs due to cyberattacks, physical damage, or occupation. Strengthening critical infrastructure also requires vetting foreign investment to ensure it is not subject to hostile foreign exploitation in a crisis.[55] In many cases, partial failure of initial defenses is expected, and the focus is on repair and resilience in dealing with limited services.[56] Examples of critical infrastructure include the following sectors:

- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- Information technology
- Transportation systems
- Water and wastewater

During the Cold War, much of the critical infrastructure of Western countries was in government hands, but now much of it is outside government control, with key industries such as transportation, internet services, and satellite communications mostly in private hands.[57] Many companies, unsurprisingly, are focused on profits, not national security. In addition, many large companies are global in their workforce, have some degree of foreign ownership, depend on foreign parts or labor for some of their supply chains, or otherwise are not fully national.

Some degree of national and personal stockpiling is important. The Baltic states have laws in place requiring reserves of vital goods. The European Union also requires member countries to have minimum crude oil stocks equal to 90 days of daily imports or 61 days of consumption, whichever is greater.[58]

Cyber threats are a constant concern. Countries at risk of attack are constantly probed by potential adversaries and near-constant threats from criminal networks or other malicious actors. Key personnel may also face risks to their physical security. Beginning in 2014, Russia conducted an aggressive cyber campaign against Ukrainian critical infrastructure, from the power grid to the banking system, in response to the departure of pro-Russian president Viktor Yanukovych and deepening Ukrainian ties with the West.[59]

Ensuring diverse means of communication is also vital. The standard ways people communicate, such as email and cell phone, are highly vulnerable to disruption and monitoring. Resistance forces may use a wide range of radios, so having large numbers of cheap and expendable devices will be valuable.[60]

During the Cold War, Switzerland prepared every major road, bridge, and other type of key infrastructure for rapid demolition. To do this, the Swiss rigged bridges and tunnels with explosives or kept stockpiles nearby in case of a Soviet invasion.[61]

In Finland, ensuring the continued functioning of critical infrastructure is a top priority. The National Emergency Supply Agency (NESA), which operates under the Ministry of Economic Affairs and Employment, is responsible for the resilience of the economy, infrastructure, and supply and is a key body for engaging industry and the private sector and maintaining critical stockpiles and security of supply. NESA helps coordinate government action and works with around 1,500 companies involved in supply security, with corporate representatives often playing a leading role.[62]

NESA divides its tasks into seven sectors: health, transportation and logistics, finance and insurance, industry, food supply, energy, and a catch-all other category. Each sector, in turn, has numerous subsectors. These subsectors are coordinated by a pool committee with its own budget. Pools comprise representatives from the most important companies, an overall industry representative, a NESA representative, a representative from the relevant ministry (e.g., transportation for the rail network), and a representative of the armed forces. The pools are often the key bodies for critical infrastructure resilience. They provide a venue for the most important actors to meet, build trust, train and exercise, make proposals for improvement, and strengthen sharing of critical information and best practices.[63]

Private companies play an important role in the process (and at times assume leadership roles), with infrastructure operators assessing their own networks. Companies provide information on their limits and vulnerabilities, contributing to a common threat and risk picture and enabling more comprehensive action. For example, hundreds of companies might exchange threat information related to cyber threats.

NESA has agreements with various Finnish companies responsible for the supply of grain, oil, pharmaceuticals, and other critical stocks. It also has arrangements with grocery stores to ensure sufficient supplies of food in case of a major cyberattack or disruption to the electricity grid. The most important requirements are set by law. Energy, for example, is necessary for defense production and thus requires high standards to ensure its supply in a crisis.[64] Finland has stockpiles of at least several months of fuel, grain, critical spare parts, and imported pharmaceuticals, among other necessities, with the level of legal and state contracting roles and the size of the stockpile varying by its perceived importance.

Some industries are expected to ramp up production if they produce goods such as weapons or medical supplies. Select companies may move to a more secure location, including within a Finnish Defense Forces (FDF) facility, while others may receive physical and cyber protection from the government. The government also has authority to allocate the power supply, which will affect production.[65]

In most instances, pool participation is voluntary, though in some areas there are legal requirements and, in general, companies must provide the information NESA requires on issues such as production levels and supply chains.[66] Shirking is possible, but there are limits and it is relatively rare. In Finland, companies must work with the government to create a list of critical employees who cannot be called for service during wartime. In addition, they have contracts with the military and government, which shirking would jeopardize. Perhaps most important in a small country are reputation and personal connections. Small com-

panies that work for the prime contractors, however, are harder to influence.[67]

Finnish officials regularly test the system for speed and quality of response, as it is too late after a crisis starts. Some testing involves tabletop exercises. Officials working on cybersecurity test their defenses through quarterly exercises in a simulated environment, but they also use real-world situations (e.g., a natural disaster that leads electricity to fail) to evaluate various systems.[68] At times, they will cut off electricity to one city or otherwise simulate a major crisis. The Covid-19 crisis and the supply disruptions that occurred after the 2022 Russian invasion of Ukraine revealed supply chain vulnerabilities in the system; poor supervision of some medical stockpiles, such as face masks; and the limits of NESA when procuring personal protective equipment. Finland treated all of these as learning experiences.[69]

Foreign companies that do business in Finland are also expected to participate in pools or otherwise protect critical infrastructure, either directly or through subsidiaries. All are subject to Finnish law, but voluntary participation is also encouraged. In some sensitive areas, such as the arms pool, Chinese and Russian companies are not allowed.[70] Weapons system manufacturers must ensure that a Finnish company or Finnish subsidiary can perform the maintenance, repair, and overhaul. [71]

Finland mandates that its military operate, maintain, and repair all critical defense systems, and industry take the lead on maintenance and repair for many systems.[72] Similarly, U.S. companies such as Mandiant and FireEye are often critical for cyber defense, and they have partnerships in Finland.[73]

Clearances, or at least access to classified information, are often vital so private actors in business and NGOs can see the broader threat picture and access the full range of possible responses. Finland also has developed security clearance procedures so the individuals responsible for critical infrastructure can receive secret information.[74] A digital platform allows them to share classified information, so to be in certain critical pools (e.g., weapons production), clearance is necessary.

Security can be a challenge for companies. They may fear espionage or threats against key workers from a foreign power. To reduce this danger, Finnish companies publish less information on personnel than before and encourage personnel to reveal less on social media.[75]

## Will to Fight

An important aspect of resilience is the will to fight: When a country is attacked, will the population participate in and support the armed forces and engage in resistance? The will to fight includes the willingness of a population—or key parts of the population—to resist an adversary and fight.[76] It is perhaps best captured in British prime minister Winston Churchill's speech before the House of Commons in June 1940, when Britain was facing a likely German invasion: "We shall defend our Island, whatever the cost may be, we shall fight on the beaches, we shall fight on the landing grounds, we shall fight in the fields and in the streets, we shall fight in the hills; we shall never surrender."[77]

Will to fight is difficult to predict in advance, though several analysts have made progress on this knotty question.[78] Russia disastrously assumed Ukrainians would not fight Russian invaders in 2022. Governments must inculcate a will to fight and, just as importantly, convey that determination to potential invaders to enhance deterrence. In the Baltics, defense and other officials speak to schools about resistance and otherwise incorporate security into the education system.[79]

Several factors generally increase the will to fight among individuals, units, and even societies: high stakes, including national survival; ideology, particularly a deep commitment to a cause or belief system; financial incentives; social or group identity; strong allies; and the capability and cohesion of individuals and units, which can be affected by training, education, leadership, and other factors.[80]

To undermine a will to fight, hostile governments will try to exploit fissures in a society through information operations or subversive activity in advance of a crisis and divide-and-rule methods when they occupy territory. A more atomized society is less likely to put up effective resistance.[81] The withdrawal of outside assistance can also undermine the will to fight.

In Afghanistan, for example, the will to fight of the Afghan National Army and Afghan National Police collapsed following the decision by the United States and NATO to withdraw all military forces and the failed leadership of President Ashraf Ghani, contributing to the Taliban overthrow of the Afghan government in 2021.[82] The same was true in South Vietnam under General Nguyen Van Thieu, including after the withdrawal of U.S. forces.[83]

Developing civic support leagues, national services, or other means to bring people together can build patriotic sentiment, as can ensuring that all communities identify strongly with the homeland.[84] Such efforts must avoid any hint of partisanship. Resilience emphasizes the country, not the government in power at a given moment, and it must transcend party politics.[85]

In Finland, there is a strong sense throughout society that independence cannot be taken for granted.[86] Although the government takes the lead on many aspects of resilience, much of the emphasis is on the individual level. One senior government official remarked, "The people must know they are *the* key actors. They must feel they can count on themselves rather than rely on others to take action. If individuals will act, many of the other functions become easier."[87]

Individual citizens are also meant to have some degree of self-reliance. The government encourages citizens to retain sufficient stockpiles of food, water, and other essentials for 72 hours at least. These include duct tape, which in Finland is casually referred to as "Jesus tape" because it performs miracles.[88]

Finland enjoys some of the highest levels of social trust in the world. The country also has made a robust effort to counter Russian narratives and otherwise build its resistance to adversary propaganda and disinformation, with the hope of bolstering psychological resilience.[89] Many of these efforts begin at an early age; even kindergarten students receive some training, while for 16- and 17-year-olds, schools organize a security day to introduce students to key concepts.[90] Finland also regularly makes citizens aware of potential threats and tries to inculcate the idea that they have some degree of agency by participating in resilience activities.

Finland appears to have a high will to fight. Before the invasion of Ukraine, opinion polls showed that over three-quarters of the population said they were willing to fight to defend their country—even when the question stressed "even if the outcome is uncertain"—the highest percentage in Europe.[91] Interviews suggest a high degree of confidence in the Finnish population's willingness to fight, with many noting that the invasion of Ukraine produced a surge in support for activities related to resistance as well as joining NATO and even assisting NATO with missions outside of Finland.[92]

Interviews suggest several reasons for this strong will to fight in Finland. First, Finland's history as a victim of Russian aggression during World War II and subsequent Soviet threats created a strong culture of self-reliance and concern about a Russian enemy.[93] Second, Finland has a strong sense of a Finnish way of life—including political and economic elements, such as democracy and the welfare state, and cultural ones, such as the sauna, social equality, and nature—all of which are seen as worth defending. Third, Finland has a strong sense of social trust and trust in government, which strengthens social bonds.[94] In addition, the national defense courses bring a wide range of elites into the national security system, giving them a sense of common purpose and understanding of the threat.

Conscription has also aided Finland's will to fight, according to interviews, and polling suggests strong support for conscription.[95] Finland maintains conscription to mobilize its population in a crisis and maintains a large network of reservists. As a result, much of Finnish society has been trained to fight, and they feel they have a stake in defense and some level of agency—or "active citizenship," as one study phrases it.[96] Conscription also creates bonds and understanding among citizens from different social classes, backgrounds, and parts of the country.[97] Over 700,000 men and women are part of the FDG reserves (out of a total population of less than 6 million), and most families have one or more citizen-soldiers.[98]

## Nonviolent Resistance and Stay-Behind Networks

To set the stage for the transition from resilience to resistance, some military and intelligence assets should

be designated to stay behind in the event of an occupation to help resist the enemy and organize local intelligence networks. Stay-behind networks might include those focused on logistics, intelligence, messaging, education, transportation, sabotage, or medical support.[99] In addition, the government may want to develop cache sites with weapons and ammunition, communication and medical equipment, and other essentials.

Ideally, leaders could be identified in advance to reduce the risk to those recruited to lead and participate in resistance and allow for a longer vetting and training period.[100] For financial reasons, networks will not be fully staffed, so core groups should be identified and developed.

The government will also want to give basic instructions to the population on how to collect intelligence that is useful to the resistance and external military forces. For example, instructing the population that an enemy might demolish bridges and telephone wires when they plan to leave is an example of how the local population might collect important indicators of enemy movements.[101] It is also important to document adversary human rights abuses and other forms of repression to generate international sympathy.[102]

Much of the goal will be nonviolent resistance, at least some of which can be taught in advance. There are many activities that can confound an adversary, ranging from marches and protests to mock elections, leaflets, boycotts, refusing to rent to occupiers, displays of flags and other symbols, and many other means.[103] If successful, this weakens the adversary's control and decreases its legitimacy, both of which make an occupation more costly. In addition, it may attract external sympathy and thus greater support for eventual liberation.[104]

Finland incorporates the possibility of conflict into its infrastructure design. All major bridges have hooks on them for hanging explosives in order to destroy the bridge as enemy troops advance. Some highways are hardened and widened to serve as alternative runways for combat aircraft.[105]

## Integration with Partners and Allies

For most small countries trying to build resilience, long-term survival in the event of a conflict may depend on external supporters. Thus, the country must build diplomatic and military relationships with external protectors and supporters, using them to bolster resilience during a crisis.[106] Short of a military campaign to reconquer lost territory, the support of outside powers is vital for continuity of government, supporting aspects of critical infrastructure, bolstering public morale, and other aspects of resilience.

Diasporas are an important audience as well. Because of their family ties, shared language and heritage, and other connections, diasporas are often highly engaged and aware of conditions in their home countries. They can publicize abuses, lobby host governments, and otherwise aid the struggle for liberation.

Foreign help can be a mixed blessing. In some ways, the promise of foreign assistance can be an excuse for inaction, with governments relying on others, not their own people, in the event of a crisis. At the same time, support from the United States and its allies is often vital to encourage people not to surrender or otherwise collapse.[107]

Baltic countries have developed regional cooperation in the event of a foreign invasion, including policy coordination, exercises, training, and professional military education, including military exchanges.[108] For Finland, NATO is an important source of advanced weapons and assistance in a crisis. But NATO membership is about more than warfighting or military assistance; it can also help with raw material gaps and supply chain dependency. There is also the possibility of joint stockpiling with neighbors such as Sweden.[109] Entities like NESA work with neighboring states to coordinate energy supplies in case of a crisis.[110]

Although Finland, of course, is not an island, it effectively becomes one if Baltic trade is cut off, as the amount of overland trade via other Scandinavian countries is limited. Around 80 percent of the country's trade comes over the sea, and it relies heavily on imported energy. Thus, it is relatively easy for a powerful foe like Russia to cut off reliable imports in a crisis. In addition, the ports freeze in winter, making it even easier to isolate, while the land connections to Norway and Sweden are limited, with the railroad gauge being on the Russian system.[111]

## The Necessity of Budgeting

Budgeting is an unglamorous but vital part of developing resilience. Indeed, it is essential for most, perhaps even all, of the above factors. Countries must invest in critical infrastructure, supplies, training, surge capacity for weapons, and other capacities of resilience, but this is difficult to justify because many of the capabilities will not be used on a day-to-day basis. Ideally, resilience should overlap with disaster preparedness. Some redundancy is necessary as power stations can be destroyed by either sabotage or massive storms, but often that linkage is limited. Because the private sector is so important, budgeting must help compensate private entities for losses but in a way that avoids playing favorites in the market.

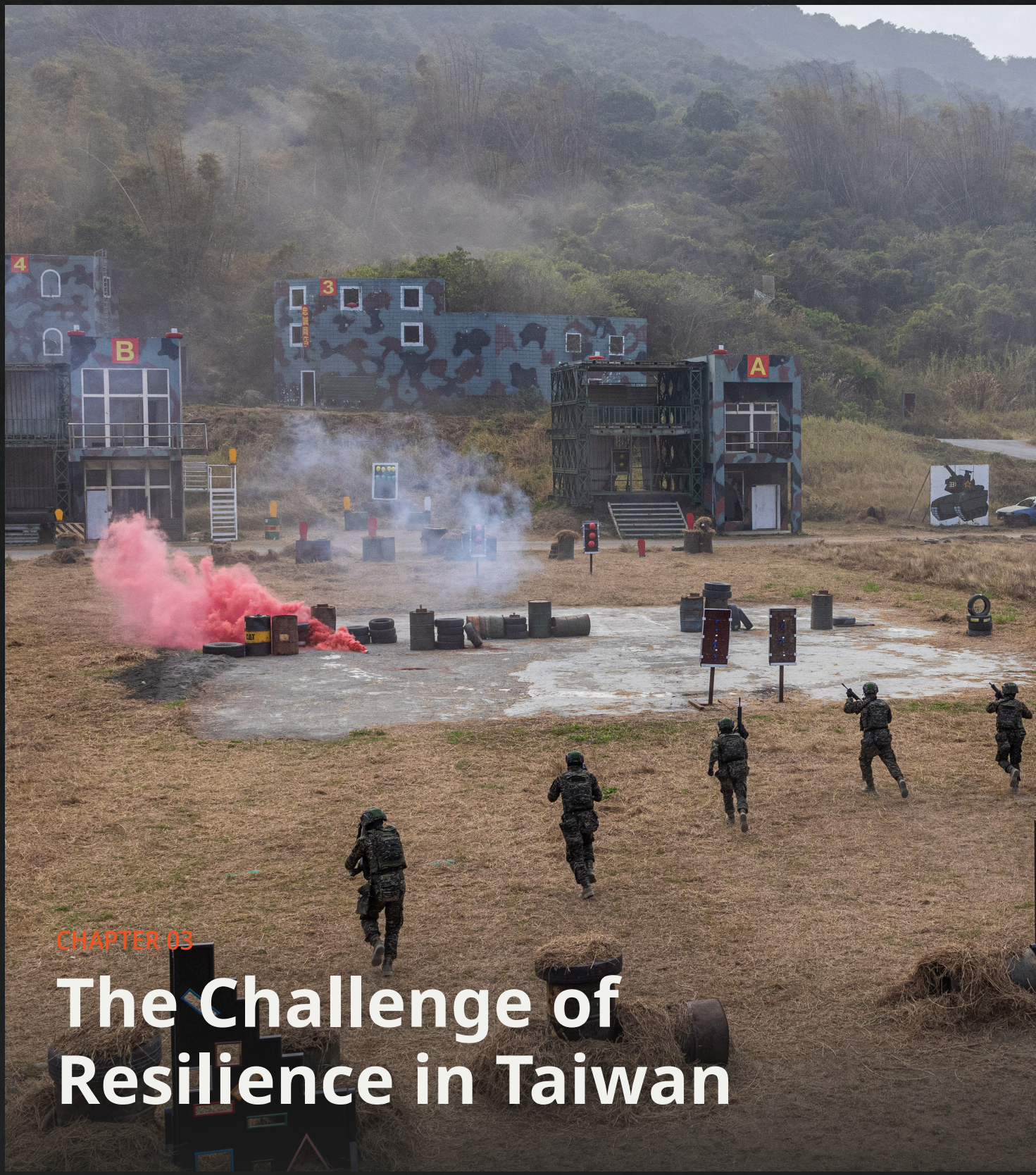
In Finland, for example, NESA works with over 1,000 companies and has a multi-billion-dollar budget to maintain strategic supplies.[112] NESA controls the National Emergency Supply Fund, which, in turn, is funded outside the budget by tax-like contributions on electricity, coal, natural gas, and other energy, generating about €38 million a year. NESA also has the authority to borrow around €200 million as state loans and receives funding from allocations derived from the national power grid.[113]

Finland uses this money in several ways to ensure the functioning of critical infrastructure. It may provide companies with partial compensation for the cost of an extra production line or a larger stockpile. NESA also owns a mothballed coal-fired power plant as a backup power source and has contracted with Black Sea transport to ensure the flow of oil. Because NESA controls its own budget, it can also fund surge capacity, new stockpiles, or other needs rapidly, avoiding potentially disastrous delays.[114]

In Finland, the government also offers financial protections for those affected by emergencies that fall outside normal insurance situations, such as damage resulting from the action of a hostile foreign power. Chapter 19 of the Emergency Powers Act outlines the legal requirements for compensation and protections for persons who have suffered damages because of the rights and obligations authorized under exceptional circumstances.[115]

## Conclusion

This chapter identifies eight key components of resilience: (1) strategic design and command structures, (2) legal authorities, (3) strategic communications and educating the population, (4) civil defenses, (5) critical infrastructure, (6) will to fight, (7) nonviolent resistance and stay-behind networks, and (8) integration with partners and allies. Each country, of course, is different, and there are no easy solutions to increase resilience. Nevertheless, this historical assessment of Finland and other cases suggests that strengthening a country in these categories—from legal authorities to critical infrastructure and will to fight—may have a compound effect by improving a country's overall resilience and increasing deterrence. As a NATO study concludes, "Resilience is therefore an important aspect of deterrence by denial: persuading an adversary not to attack by convincing it that an attack will not achieve its intended objectives."[116]




CHAPTER 03

# The Challenge of Resilience in Taiwan


**Taiwan's armed forces hold two days of routine drills to show combat readiness at a military base on January 12, 2023, in Kaohsiung, Taiwan.**
ANNABELLE CHIH/GETTY IMAGES

**This chapter examines the current and evolving threat to Taiwan, particularly from China**. Building on the framework outlined in chapter 2, this chapter examines Taiwan's activity in such areas as strategic design and command structure, legal authorities, strategic communications, civil defenses, critical infrastructure (including such areas as cyber defense, energy, communications infrastructure, food security, and government-private sector relations), will to fight, and integration with allies and partners.

## Threats to Taiwan's Resilience

Since 1949, Taiwan has faced a range of direct threats from the PRC, including a possible full-scale invasion. After U.S. president Harry Truman ruled out the use of the U.S. military in the Taiwan Strait in early 1950, Chinese leader Mao Zedong positioned nearly half a million Chinese troops on the coastline directly across from Taiwan. The beginning of the Korean War that June, however, brought the U.S. Seventh Fleet into the waters off Taiwan to stop the war's spread, and Mao had to shelve the idea of an invasion. Yet, in 1954 and again in 1958, Mao bombarded Taiwan's outer islands with artillery attacks and mobilized the People's Liberation Army (PLA) for an assault, only to be deterred by the prospect of U.S. intervention on behalf of Taiwan.[1]

In the late 1970s, Beijing adjusted its formal guidance from "liberate Taiwan" to "unify Taiwan," signaling a policy of increased flexibility on how the Chi-

nese leadership sought annexation. But the threat of a direct assault returned in the mid-1990s after Beijing conducted a series of missile tests in the waters off Taiwan, and again in 2004 when the PRC National People's Congress passed the Anti-Secession Law, which enshrined the use of "non-peaceful means and other necessary measures to protect China's sovereignty and territorial integrity."[2]

Over the past several decades, Taiwan has also faced a growing number of nonmilitary threats that pose significant risks to its security and stability. These range from economic pressure and cyberattacks to disinformation campaigns and diplomatic isolation. China's use of coercive tactics, including formal and informal trade restrictions and the poaching of Taiwan's diplomatic allies, has placed increasing stress on the island's economy and international standing. Additionally, Beijing has developed an increasingly sophisticated and comprehensive tool kit of gray zone tactics that allows it to probe Taiwan's defenses and the solidity of the U.S.-Taiwan relationship in ways that complicate a corresponding response by Taipei and Washington.[3] This gray zone "sliding scale" allows Beijing to rachet up political and military pressure to place significant stress on the Taiwan leadership and its people without crossing a threshold of kinetic conflict with Taiwan or the United States. Indeed, perhaps fearing that a direct assault on Taiwan would lead to U.S. and allied condemnation and perhaps retaliation, Beijing has conducted military exercises that demonstrate the capability and possible intention to blockade or quarantine Taiwan but in a way that Beijing believes will not prompt a direct U.S. response.[4]

For example, China conducted military exercises in August 2022 in the wake of then U.S. House speaker Nancy Pelosi's visit to Taiwan and again in May 2024 after the inauguration of President Lai Ching-te to demonstrate that Beijing is growing more creative and confident in its design and execution of gray zone tactics aimed at pressuring Taiwan. In the case of the May 2024 PLA exercises in response to President Lai's speech (dubbed Joint Sword–2024A), the operations blended conventional PLA forces with other nonmilitary actors, including the Chinese coast guard, highlighting the growing role of law enforcement actors and "lawfare" in conventional operations with the military. This strategy of "salami slicing" allows Beijing to exert continuous pressure without crossing the threshold of outright conflict, complicating Taiwan's defense posture and the international community's response.[5]

As Beijing works to create an impression of isolation and impotence in the waters and airspace surrounding Taiwan, it also strives to probe and stress Taiwan's defenses internally. One focal area for Beijing has been Taiwan's cyber defenses, which face an escalating volume of cyber incursions and attacks frequently linked to Chinese state actors. By some accounts, the island faces around 30 million cyberattacks and probes each month, targeting both government institutions and private enterprises.[6] These attacks aim to steal sensitive information, disrupt critical infrastructure, and undermine public trust in Taiwan's government. Notable incidents include the 2020 cyberattack on Taiwan's state-owned oil company, CPC Corporation, which disrupted its operations and highlighted vulnerabilities in the island's critical infrastructure. In a more recent example directly linked to China, the hacking group APT41 infiltrated an unnamed Taiwanese research institute that potentially gave the group access to "proprietary and sensitive technologies," according to a summary report by Cisco.[7]

Disinformation campaigns pose yet another serious nonmilitary threat to Taiwan, with efforts designed to manipulate public sentiment, leverage partisan frictions, and influence election outcomes. In nearly all of Taiwan's recent national elections, Chinese-linked actors have been present in the online and offline media and information ecosystem. These efforts include fabricated stories about political candidates, such as claims of corruption, as well as misinformation regarding government policies. Although such meddling has not compromised the integrity of Taiwan's elections, these efforts certainly affected the information environment for voters.[8] In the lead-up to the 2020 presidential election, for example, false narratives about candidates' personal lives and distorted policy claims circulated heavily on social media platforms. Aggravating the impact of PRC-originated disinformation efforts is the rabidly partisan nature of Taiwan's democracy, with the two major parties—the KMT and the DPP—often stoking their own disinformation campaigns or otherwise taking advantage of disinformation regardless of its source.[9]

Direct political meddling constitutes another layer of nonmilitary threats Taiwan faces. These activities often involve attempts to influence Taiwan's domestic politics through financial support for pro-Beijing politicians, espionage activities, and exertion of economic pressure. In July, National Security Bureau director-general Tsai Ming-yen warned the lawmakers in the Legislative Yuan, "The Chinese Communist Party's infiltration activities are increasingly rampant in Taiwan, posing a severe challenge to national security work. . . . They also recruit retired national security personnel and infiltrate political parties and government departments."[10] According to one tally by Reuters, the Taiwanese government has discovered 21 active or retired military officers at or above the rank of captain who have been actively spying for Beijing.[11] This interference aims to sway Taiwan's political direction in favor of unification with China, undermining the island's democratic governance and political autonomy. The openness and pluralism of Taiwan's political institutions, media environment, and wider society undoubtedly serve as the foundation of the island's long-term strength but in the short term leave it vulnerable to Chinese-linked and Beijing-backed actors looking to shape internal political discussions and outcomes.

Additionally, Beijing has sought to leverage its economic might to pressure Taiwan into capitulation, as well as to further isolate Taiwan diplomatically and economically. One tried and tested approach is to threaten the operations of Taiwan companies in the PRC. For example, in the lead-up to the January 2024 presidential elections, Chinese authorities launched a tax and land-use investigation into the electronics contract manufacturer Foxconn. Many saw this as an attempt to exert pressure on the company and Terry Gou, who was contemplating a presidential run in Taiwan.[12] Similarly, Beijing uses the lure of market access, preferential access, and development finance to ensure only a handful of countries diplomatically recognize Taiwan. Finally, Beijing has begun innovative efforts to treat Taiwan residents and entrepreneurs as de facto PRC citizens through efforts like the Fuzhou Province's "integrated development" plan.[13]

These nonmilitary threats—cyberattacks, disinformation, direct political meddling, and economic pressure—form a comprehensive and evolving strategy aimed at weakening Taiwan's political stability, economic resilience, and international standing. Based on these threats, the rest of this chapter turns to Taiwan's actions in the major areas of resilience, beginning with strategic design and command structure.

## Strategic Design and Command Structure

As the discussion of Finland and other countries indicates, a critical piece of national resilience is ensuring the requisite administrative structures are in place well before a crisis emerges. In the case of Taiwan, the picture today looks vastly better than several years ago, but significant gaps and areas of potential discoordination remain.

At a high level, Taiwan now delineates functional oversight of civil defense between the Ministry of the Interior (MOI) during peacetime and the Ministry of National Defense (MND), through its All-Out Defense Mobilization Agency (ADMA), during times of war. This division of responsibilities was formalized with the passage of the Civil Defense Act (CDA) in 2021.[14] Before the CDA, civil defense efforts were fragmented, involving a loosely coordinated network of administrative bodies and bureaucratic actors. These entities often worked in isolation, and while there were instances of cooperation, the overall structure lacked clarity and coordination. The CDA was a critical development as it established a clear chain of command for civil defense matters, creating a streamlined approach for peacetime and wartime situations.

The most significant issue with the current framework is that the distinction between peacetime and wartime responsibilities is, in many ways, artificial. In reality, the planning, coordination, and preparedness required for civil defense in peacetime overlap with those needed in wartime, especially in the context of China's ongoing gray zone activities targeting Taiwan. These activities, which blur the lines between peace and conflict, necessitate constant readiness and swift coordination between civilian and military agencies. The rigid separation of responsibilities could hinder the flexibility needed to respond effectively to such unconventional threats.

Moreover, both the MND and MOI are large bureaucratic entities with their own interests, priorities, and internal dynamics. This creates the risk of turf battles, with each ministry potentially guarding its domain rather than collaborating efficiently. In such a high-stakes environment, Taiwan cannot afford to let bureaucratic competition undermine its national security efforts. The challenges that China's hybrid warfare tactics pose require seamless interagency cooperation, and any misalignment between the MOI and MND could lead to delays or inefficiencies that weaken Taiwan's ability to respond to crises.

Another significant challenge lies in better integration of planning and decisionmaking between Taiwan's central government and subnational governments. As Taiwan moves toward centralizing civil defense planning under the MOI and MND, it will be crucial to actively engage with and incorporate local initiatives developed by mayors, city planners, and regional authorities across the island. The 2021 CDA makes an important first step by delineating authority between the central, municipal, and district governments, creating a clearer chain of command. However, a more fully integrated structure is needed to ensure that when a stress test of the system is conducted—whether in the event of a conflict or crisis—it will function as intended.

Key questions remain about how well Taiwan's civil defense apparatus will operate under actual strain. For example, how will resources and personnel be mobilized across the island in an emergency? What contingency plans are in place if critical communication lines between central and local governments are severed? Moreover, how will decisionmaking be coordinated between localities if contact with the central government is disrupted? These vital concerns must be addressed through joint planning, scenario-based exercises, and development of robust communication and logistics frameworks.

These concerns are not lost on the government. As one government official told the Financial Times, "We are discussing revising our disaster management mechanisms in order to build a clearer command chain and have one system that can work across peacetime and wartime."[15] One such effort was unveiled in June 2024. President Lai announced the creation of a National Whole-of-Society Defense Resilience Committee to be led by Lai, with Vice President Bi-khim Hsiao, National Security Council secretary-general Joseph Wu, and secretary-general to the president Pan Men-an serving as committee deputies. This potentially serves as an umbrella organization across government, civil society, and the private sector.

Resilience is a holistic effort, and as Lai said in a speech announcing the committee's creation, "We need to conduct a comprehensive review and propose solutions to problems, strengthening our resilience in national defense, economic livelihoods, disaster prevention, and democracy."[16] Signs emerging from the committee's inaugural meeting are positive, with a focus on running unscripted civilian defense exercises, involving all relevant actors in society, and finding better means of coordination across the government, especially with local governments. National Security Council deputy secretary-general Hsu Szu-chien, who briefed the committee, stressed,

> The traditional way is for Taiwan's government and military to take charge, issuing orders to civilians during natural disasters and emergencies. . . . Now we have to adjust this thinking to bolster civilian participation during contingencies, for people to know that "we can take the initiative to save lives."[17]

## Legal Authorities

The last decade has seen significant progress in building the necessary legal authorities and legislative tool kit to deal with the proliferation of threats to Taiwan's overall resilience. Notable examples include the following:

- The Cybersecurity Management Act (2018) targets government agencies and specific NGOs considered providers of critical infrastructure. It mandates they create and implement comprehensive cybersecurity plans.[18]
- The Anti-infiltration Act, enacted in early 2020, criminalizes foreign interference in Taiwan's political processes, including disseminating

false information intended to influence elections.[19] This legislation imposes strict penalties on individuals and organizations found guilty of spreading false information to meddle in Taiwan's democratic processes.

- The CDA (2021), discussed above, clarifies the division of responsibilities for civil defense between the MOI during peacetime and the MND during wartime.[20]
- The National Security Act, as amended in 2022, expands the scope of protections against espionage and infiltration, specifically the leakage of critical technologies and trade secrets to foreign powers.

One glaring weak spot for Taiwan's legal and administrative framework is the vital issue of leadership succession. As it stands, Article 49 of the Constitution of the Republic of China is the only public articulation of the presidential line of succession. It clarifies the transfer of power for two offices only: the vice president and the president of the Executive Yuan. Clarifying and codifying a more robust chain of command is an essential task for Taiwan, given the threat of a possible decapitation strike by the PLA.

## Strategic Communications

In response to the pervasive threat of disinformation, the Taiwanese government has adopted a comprehensive approach that includes public education, regulatory measures, and collaboration with technology companies. Recognizing the importance of an informed public, Taiwan has launched numerous media literacy programs aimed at educating citizens about the dangers of fake news, misinformation, and disinformation, as well as building the capability to identify reliable sources of news and information.[21] These programs cut across all demographics, including students, senior citizens, and rural communities, to ensure a broad reach. Additionally, the government has integrated media literacy into school curricula, teaching young students critical thinking skills and how to discern credible information sources from misleading ones.

To bolster these educational efforts, Taiwan collaborates with NGOs and civil society groups that specialize in media literacy. These organizations play a crucial role in grassroots education, conducting community outreach and providing resources to help citizens navigate the information landscape. For example, the Taiwan FactCheck Center works with schools and community groups to teach fact-checking techniques and promote skepticism toward unverified or suspicious information online. Such efforts can inoculate against disinformation created by external powers as well as false or misleading information created by partisan political and commercial interests.

Additionally, the government works closely with social media platforms like Facebook and LINE to identify and remove false content. These companies have established fact-checking partnerships with local organizations to help monitor and curb the spread of disinformation. For instance, Facebook collaborates with the Taiwan FactCheck Center to verify the authenticity of viral content, flagging and taking down posts deemed false. This partnership also extends to sharing data on disinformation trends, allowing the government and civil society to stay ahead of evolving tactics used by malicious actors.

International cooperation is another key component of Taiwan's strategy against disinformation. Taiwan participates in global forums and collaborates with other democracies to share best practices and develop joint responses to information threats. The country's participation in initiatives like the Global Cooperation and Training Framework (GCTF) allows it to benefit from the expertise of international partners and contribute to the collective defense against disinformation.

## Civil Defenses

One of the most notable developments in Taiwan since Russia's invasion of Ukraine in 2022 is the proliferation of NGOs focused on civil defense and whole-of-society resilience. Notable examples include the following:

- **Kuma Academy**, founded with a $32 million donation from entrepreneur Robert Tsao, runs all-day courses on combat skills, medical training, and general disaster response.

- **Camp 66**, an airsoft shooting range, seeks to improve the weapons capabilities of the general population.
- **Taichung Self-Training Group** focuses on disaster response and medical training.
- **Forward Alliance**, according to founder Enoch Wu, seeks to "teach citizens how to respond in an emergency. In peacetime, this means disaster response. In wartime, the same skills form the backbone of civil defense."[22]

Dozens more organizations blanket the island, most of which are not more than a few years old.

Despite this good work, however, the government and military have, to a large extent, ignored or evinced skepticism about these efforts. Indeed, former defense minister Chiu Kuo-cheng once dismissed the Kuma Academy as little more than a paintball club.[23] Yet this bottom-up surge of grassroots enthusiasm and organization is arguably one of the most promising channels the Taiwanese government has for bolstering functional capabilities in disaster preparedness and strengthening the population's will to fight.[24] The key question is how to channel and coordinate their efforts with those of the new Lai government and the military.

Thus, while the unofficial nature of these organizations is arguably their most important attribute, the government should take greater steps to work with and coordinate these resilience-focused civil society organizations, including regular convenings with organization leaders and the newly formed Whole-of-Society Defense Resilience Committee.[25] It should also include more formally integrating these groups into the MND's Wan An and Han Kuang combat exercises, as well as the Wanan air defense drill.

Within the government and military, there have been notable signs of progress, including the creation of the AODMA, established under the MND in 2021 as part of the All-Out Defense Mobilization Readiness Act. AODMA's primary goal is to coordinate the mobilization of the island's reserve force in the face of a conflict or disaster, which, prior to AODMA's creation, had been managed by the All-Out Defense Mobilization Office and the Armed Forces Reserve Command.

In the spring of 2022, the MND issued its first-ever civil defense handbook, which included QR codes that could direct individuals to one of Taiwan's 89,405 air raid shelters, information on how to locate medical clinics and "daily necessities allocation stations," and images to help distinguish between Taiwan's military and the PLA.[26] Of course, the handbook's distribution is a welcome but fairly minor step in the right direction. More important is the internationalization of the information contained in the pamphlet. As some critics have noted, relying on QR codes to find air raid shelters in a time of war is problematic as access to reliable cell phone service during a Chinese attack is far from guaranteed.[27] Indeed, the known operations to sever Taiwan's undersea cables, likely at Beijing's direction, clearly indicate that telecommunications access might be the first casualty of a prospective Chinese attack.[28] As discussed, countries like Finland mandate all large buildings have shelters. They have also turned many of the shelters into social spaces that community members incorporate into their daily lives during peacetime, ensuring citizens are not scrambling to determine the location of the nearest shelter in the event of a surprise attack.

At the end of 2022, then president Tsai Ing-wen gave a speech at the Presidential Office in which she unveiled a plan for important changes to Taiwan's national defense, including the lengthening of conscription from four months to a full year.[29] She also called for upgrading Taiwan's civil defense system, with better integration of central and local governments, the military, law enforcement, and the private sector across disaster relief, public health, and public security. Her speech was light on details, but it signaled at the highest level that Taiwan's existing civil defense framework and capabilities were insufficient to meet the current and future challenges.

Despite this progress, roadblocks exist. Perhaps the most notable is the issue of a possible Chinese attack, which is deeply political, with the two main parties—the Kuomintang (KMT) and the Democratic Progressive Party (DPP)—engaging in intense disputes about the nature of the threat and the correct measures for responding. The KMT tends to advocate for closer ties to mainland China, arguing that maintaining peaceful cross-strait relations is the best way to avoid conflict.


**FIGURE 1** Cover of MND's 2023 Civil Defense Handbook

**SOURCE** Taiwan Ministry of National Defense.

DPP leaders, including President Lai, have pushed for increased defense spending and stronger relations with the United States and other democratic nations to counter the military threat from China. This divide is evident in election campaigns, with the KMT accusing the DPP of unnecessarily provoking Beijing, while the DPP accuses the KMT of being too willing to appease China, risking Taiwan's future security. Thus, instead of a core national political consensus on the nature of the threat and the road map to addressing it, including defense mobilization and civil defense preparedness, key partisan divisions remain, thwarting progress.

The second clear roadblock is the lack of effective coordination across the growing ecosystem of government, private sector, and NGO stakeholders working directly on or adjacent to civil defense. Although absolute coordination is neither achievable nor desirable, Taiwan's small population and limited resources, coupled with the existential risk of a possible Chinese attack, means there is little room for duplicative or ineffective efforts. This fragmentation hinders the pooling of resources and limits the strategic alignment needed for an integrated civil defense strategy. Relatedly, without more central coordination and national-level standards on civil defense and all its related domains, the Taiwanese government cannot ensure consistency and quality within the growing network of civil defense actors. The new Whole-of-Society Defense Resilience Committee, discussed above, is an important step in the right direction, but much depends on how the committee operates, how inclusive it is, and whether or not it is geared toward substance reforms.

# Critical Infrastructure

Taiwan has made progress on protecting its critical infrastructure, but significant vulnerabilities remain. This section addresses four areas: cyber defense, energy, communications, and food security. It then examines the broader issue of relations with the private sector.

## Cyber Defense

For decades, Taiwan has been under constant cyber assault from the PRC. Indeed, these attacks date to the late 1990s, when a large-scale web defacement attack targeted government websites in the wake of comments by then president Lee Teng-hui asserting Taiwan's distinct sovereignty from China.[30] Since then, the scale and intensity of these efforts have increased in tandem with China's strengthening assertion of sovereignty over Taiwan and its proliferating cyber capabilities, including through hybrid and proxy actors.[31]

Successive leaders in Taiwan have taken aggressive steps to address the threat. In 2013, the government established a cybersecurity office under the Executive Yuan, which was later upgraded to a department in 2016. The department seeks to coordinate national cybersecurity efforts, including the formulation and im-

plementation of all national-level cybersecurity laws and regulations.[32] It also works closely with other government agencies, such as the MND, the Ministry of Economic Affairs, and the National Communications Commission, in an attempt to create a unified front against cyber threats.

In 2017, MND established the Information, Communication, and Electronic Force Command (ICEF), which is tasked with defending military networks and conducting offensive cyber operations and thus is similar in function to the U.S. Cyber Command. ICEF was the first effort by the Taiwanese government and military to cohere electronic warfare, cyber warfare, and communication warfare into a single entity.

Taiwan's approach to cybersecurity—and indeed its approach to digital governance—took a major step forward with the creation of the Ministry of Digital Affairs (MODA) in August 2022. From the outset, MODA was tasked with improving Taiwan's approach to cyber resilience, and the Department of Communications and Cyber Resilience was tasked with looking across the island's telecommunications and digital infrastructure to ensure it is effective, advanced, protected, and coordinated. The ministry's inaugural leader, Audrey Tang, had already built a reputation for creativity and an unconventional approach to technology while serving as the minister without portfolio of digital affairs. Tang has shown a distinct willingness to partner with civil society, including the island's robust hacking community, to improve the government's capabilities, transparency, and service offerings to the public. Tang's successor at MODA, Huang Yen-nun, recently unveiled a new strategy to increase the resilience of Taiwan's communications system, including the maintenance of internet access during natural disasters through investments to ensure internet access during natural disasters, cyberattacks, and other threats.[33]

International cooperation is another cornerstone of Taiwan's cybersecurity strategy. The Department of Cybersecurity collaborates with international partners to share threat intelligence, best practices, and technological advancements. Taiwan has also signed cybersecurity memoranda of understanding (MOUs) with several countries, including the United States, Japan, and Australia. For example, Taiwan and the United States conduct annual cybersecurity drills known as the Cyber Offensive and Defensive Exercises (CODE), which simulate real-world cyberattacks and defenses to test and improve their respective cybersecurity capabilities.[34]

Furthermore, Taiwan participates in global cybersecurity forums and initiatives, such as the Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response and Security Teams (FIRST). While these memberships allow Taiwan to collaborate with international cybersecurity experts, share insights on threat trends, and contribute to the development of global cybersecurity standards, Taiwan's lack of diplomatic status with nearly all its partner nations continues to constrain the depth and breadth of these cooperative engagements.

The Taiwanese government's investment in cybersecurity technologies and workforce development, while noteworthy, still demands additional effort given the enormity of the challenges faced. In interviews with government officials and cybersecurity experts in Taiwan, a consistent concern was the limited talent development pipeline due to Taiwan's relatively small population size and the challenges of attracting key talent away from commercial technology firms or tech start-ups. The government has attempted to address this through educational and training programs. However, questions remain about the adequacy of these programs in meeting the growing complexity of cyber threats. Universities and technical colleges offer specialized courses, but as of yet, there is no evidence that these programs can produce a sufficiently large or skilled workforce to address Taiwan's urgent needs, especially in light of the enormous challenge from Beijing. Government-sponsored certifications and continuous learning opportunities, while beneficial, may lack the depth required for tackling increasingly sophisticated cyberattacks, let alone for dealing with the types of attacks that prefigure an all-out invasion.

## Energy

Taiwan's basic energy equation puts it in a strategic bind. For geographic and policy reasons, it overwhelmingly depends on the importation of energy resources, the vast majority of which are traditional hydrocarbons. In 2023, Taiwan imported 97 percent

of its energy, most of which came from oil and petroleum (44 percent), coal (29 percent), and natural gas (20 percent). Indigenously derived power is split between nuclear (4 percent), biomass (1.3 percent), solar (1 percent), and wind and hydro (0.8 percent).[35]

Yet for political and policy reasons, many of which are sensible, the Taiwanese government has outlined ambitious goals to decarbonize, seeking net-zero emissions by 2050. While further expansion of the island's nuclear power program could enable such an effort, the ruling DPP, for political and environmental reasons, has moved aggressively to eradicate nuclear power as a possible energy source by 2025, despite the fact that nuclear power remains the single largest domestically produced power source.

Today wind and solar alone have insufficient capacity to power Taiwan's economy during noncrisis periods or during a possible crisis. Adding to the challenge is the problematic nature of Taiwan's power grid. According to a report by the American Chamber of Commerce in Taiwan, the grid is "both isolated and relentlessly centralized, with heavy reliance on larger plants," including the three vital voltage substations of Lunchi, Longtan, and Zhong Liao.[36] A problem in any one plant would ripple out across the entire grid, causing "an electrical heart attack" for the island and its economy.[37] The impacts of these deficiencies have been put front and center in the political conversation after a series of significant island-wide blackouts over the past several years. The 303 blackout—named for the date of the outage, March 3, 2022—affected nearly 5.5 million residents, most notably in southern Taiwan, where the blackout lasted more than half a day. Because one firm, Taipower, structures and oversees Taiwan's power grid, the issues that arise in one part of the grid are likely to spread nationwide.

Addressing all the above challenges will be vital for Taiwan, not only in a major geopolitical crisis but also in nonmilitary scenarios that are more likely to affect the island, including typhoons, earthquakes, and—in the case of the 303 blackout—human error. Addressing Taiwan's reliance on imported energy will not be easy or quick. While it is notable and laudable that the administrations of Presidents Tsai and Lai set out ambitious climate goals, these must be weighed against the growing geopolitical threats Taiwan currently faces. Taking steps to build a more resilient power supply need not mean completely abandoning the vital objective of greening Taiwan's energy future, but tough political choices must be made.

## Communications Infrastructure

In early 2023, two undersea communication cables connecting Taiwan's main island with the Matsu Islands were severed, temporarily disrupting internet communications for the 14,000 inhabitants of the outer islands Taiwan governs. Taipei did not formally accuse the PRC of sabotage, but credible rumors point toward Chinese ships causing the disruption.

While Beijing might have been sending a subtle warning to Taipei, the incident highlighted the vulnerability of Taiwan's communications infrastructure. A mere 15 submarine cables link Taiwan to the rest of the world. According to the *New York Times*, these undersea fiber optic cables have experienced nearly 30 ruptures since 2017, in most cases because of dragged ship anchors.[38] These incidents underscore the island's precarious position, with its global connectivity largely hinging on undersea cables that could be easily targeted in a conflict scenario. It is also worth noting that rupturing Taiwan's undersea cables would have knock-on effects for countries on its periphery, including South Korea and Japan.[39] Furthermore, the infrastructure enabling domestic communications is also highly vulnerable to potential disruption, whether by physical attack or natural disaster. Indeed, a 7.2-magnitude earthquake that rocked Taiwan's eastern coast early in 2024 damaged nearly 200 cellular base stations.[40] Irrespective of the origin of disruption, incapacitation of the macro cell tower network that connects Taiwan's residents to each other and the government through their cell phones would significantly hamper the ability to coordinate in a crisis. Even lower-tech communication media, such as wireless radio and television networks, depend on physical infrastructure that would be a tempting target for an invading force. As one researcher from the Institute for National Defense and Security Research told Reuters, "Strategic communications, internally and externally, is what keeps us up at night, particularly in the aftermath of Ukraine."[41]

Taiwan is vulnerable not just to physical attacks on its infrastructure but also to cyberattacks that disrupt its communications and military command systems. In fact, Taiwan's cybersecurity agencies have reported a significant increase in cyberattacks over the past few years, with Chinese state-sponsored groups being the primary perpetrators. According to a report from the cybersecurity firm Cloudflare, Taiwan saw a staggering 3,370 percent year-on-year increase in distributed denial-of-service (DDoS) attacks during the final three months of 2023.[42] The major utility Chunghwa Telecom, discussed above, was hacked in early 2024, with vast troves of sensitive information and data exfiltrated onto the dark web. While the identity of the perpetrator has not yet been confirmed, the attack demonstrates the vulnerability of Taiwan's critical infrastructure. As a recent report by Microsoft reveals, PRC-led hacking efforts across the Asia-Pacific region, including against Taiwan, frequently attack the telecommunications sector, "often leading to many downstream effects."[43] Taiwan Semiconductor Manufacturing Company (TSMC), arguably Taiwan's most strategically important firm, reported a ransomware hack last summer that, while limited in its actual damage, again demonstrates just how vulnerable Taiwan's vital actors are to such attacks.[44]

Yet another warning for Taiwan comes from the ongoing war in Ukraine, both because Russia's assault on the country's telecommunications infrastructure hints at a possible playbook for Beijing and because of the Ukrainian military's reliance on the Starlink network to communicate and coordinate across the battlefield and with Kyiv. For Ukraine's extraordinarily effective drone army, the reliance on Starlink's network of 6,000 low Earth orbit (LEO) satellites has been especially stark. Starlink's owner, Elon Musk, has been reluctant to support the Taiwan market, in part because of joint-venture requirements that Taipei would mandate. Even assuming Musk sees Taiwan as a potential partner, some have raised concerns that his other business interests, most notably Tesla's deep integration into the Chinese marketplace, potentially add variables beyond Taipei's control that are too uncertain to accept.[45]

Under the pioneering leadership of Tang, who led the MODA from 2022 through May 2024, Taipei has made important strides in recent years to address the island's vulnerabilities. The umbrella effort aims to enhance Taiwan's overall telecommunications resilience through a better mix of land-based, maritime, and communications systems that, taken together, ensure Taiwan's "government command structure, disaster relief units, and the general populace can maintain essential and secure communication even in extreme circumstances."[46]

In January 2023, MODA established the National Institute of Cyber Security (NICS) with the goal of advancing "the application, competence and R&D of Taiwan's cyber security technology."[47] Among other goals, NICS strives to create a talent pipeline that can assist the government and private sector to help Taiwan confront a range of current and future cyber threats. As mentioned, these efforts have not clearly yielded strategic dividends, but recognizing the deficiencies in the talent pipeline is an important first step.

MODA also selected the Telecom Technology Center to lead an effort focused on "response or wartime applications of new technology to strengthen digital communications resilience," including the use of non-geostationary satellite orbit (NGSO) in instances where traditional means of communication, including mobile and landline phones, become unavailable.[48] Under its Program for the Digital Resilience Validation of Emerging Technologies for Contingency or Wartime Applications, the government seeks to enhance connectivity to Taiwan's outer islands and remote areas through an expansion of satellite hot spots and cellular base stations.[49] This summer, MODA announced it had launched a new medium Earth orbit (MEO) satellite to bolster the connectivity of Taiping Island, which sits in the Nansha (Spratly) Islands and is contested by the PRC, Vietnam, and the Philippines.[50]

In 2023, Chunghwa Telecom, one of Taiwan's largest telecommunications providers, signed a deal with London-based Eutelsat OneWeb to bring its satellite network coverage to Taiwan. Around the same time, MODA partnered with the Luxembourg-based satellite firm SES to implement an MEO satellite network covering all of Taiwan. According to industry reports, conversations are also ongoing with Amazon's Project Kuiper and the Canadian firm Telesat.[51] These concur-

rent efforts with multiple satellite firms are an effort to avoid any single point of failure in Taiwan's telecommunications network.

While these efforts are to be applauded, Taiwan's ability to insulate its telecommunications infrastructure from intentional attacks or disasters stemming from natural disasters, as discussed below, has limitations. If Beijing is intent on attacking the island, knocking out its communications network will be a top priority. Therefore, cooperation with international companies and governments is essential.

## Food and Water Security

In addition to importing the vast majority of its energy requirements, Taiwan relies heavily on global supply chains to source food. Statistics from 2021 show that nearly 70 percent of Taiwan's annual caloric intake comes from overseas.[52] According to an analysis by Taiwan's Ministry of Agriculture, the island's food self-sufficiency ratio stood at 31 percent in 2022, the lowest in a decade, well below the target of 40 percent by 2020 set by the Ma Ying-jeou administration in 2011. Analysis by the USDA concludes that the problem might be even worse than the official self-sufficiency ratio indicates, as "domestic poultry and hog production which are shown to have high self-sufficiency ratios rely on imported grains and feed to maintain production."[53] Further, Taiwan relies on fertilizer imports, which, in turn, sustain its domestically grown vegetable and fruit crops. In the event of a Chinese blockade or invasion that partially or completely disrupts global supply chains, access to imported grains and fertilizers would be significantly affected, to the great detriment of Taiwan's domestic food production.

While one government official stated publicly in 2022 that Taiwan had sufficient food stockpiles to sustain for one year in the event of a direct attack by China, there is no full public accounting to verify these claims.[54] In other venues, senior officials have been more cagey on the precise inventories and the planning scenarios used to formulate these supply targets. Former deputy economy minister Chen Chern-chyi would only clarify, "We want to ensure that we have a certain period's worth stockpiled in Taiwan, including food, including critical supplies, minerals, chemicals and energy of course."[55] During the Covid-19 pandemic, U.S. government experts assessed that Taiwan had sufficient food stocks to last six months. While the assessment does not contravene Taiwanese government estimates, it highlights the need for more robust data reporting on the current stockpile levels.[56]

While public reports indicate that Taiwan has sufficient reserves of rice to last one year (1.26 million metric tons), the stockpiles of other staples are less certain. Relatedly, a significant and prolonged power outage would call into question the electrical cooling systems needed to store food supplies, even the national reserves of rice, which require storage in low-temperature silos.

During a crisis, a key logistical challenge is the rationing and distribution of food and water. This is no easy task, especially in the instance of a military attack or, more probably, a severe earthquake. Relatedly, in the instance of a prolonged crisis, a key issue for the Taiwanese government and its military planners would be the issue of food resupply. As discussed below, this is an area of potentially enhanced U.S.-Taiwanese cooperation.

Taiwan is also wrestling with growing challenges in water security and water resource management. Taiwan's 2021 drought, the worst in 56 years, severely affected its semiconductor industry, which accounts for more than 60 percent of the global supply of microchips and 90 percent of the globe's most advanced chips.[57] TSMC, a vital player in this sector, faced significant production slowdowns during the drought, as it was forced to truck in water to meet its needs. This example highlights the stark nature of Taiwan's vulnerability, as the high-tech industry is water intensive and crucial to both Taiwan's economy and the global supply chain. Indeed, one estimate shows that a typical semiconductor firm on Taiwan uses roughly 20,000 tons of water per day and that TSMC's demand for municipal water increased 71 percent between 2015 and 2019.[58]

## Government-Private Sector Relations

Coordination between the public and private sectors is challenging in almost all market democracies, owing to the de jure and de facto independence of private firms, as well as concerns about corruption stemming from overly cozy relations between policymakers and prof-

it-making firms. Moreover, many bureaucrats have little incentive to deepen discussions and relations with the private sector, as such efforts are not, in themselves, rewarded. Yet a mature discussion on societal resilience and whole-of-society defense is impossible without deep planning and coordination interlinkages between the private sector and the government. As the case of Finland demonstrates, some governments that face a serious external threat have significantly deepened their relationship with the private sector.

Such efforts are underway in Taiwan, though they are largely piecemeal and event driven. While many workshops and conferences focus on how supply chains, telecommunications, and cybersecurity resilience affect Taiwan's economy, there are few formal frameworks and channels for bolstering coordination between the private sector and the government or between private sector actors. During a recent trip to Taipei, representatives from several global technology companies with large footprints in Taiwan told one of the authors of this report they had no active ongoing conversations with the government on the issue of resilience and whole-of-society defense. Taipei must find ways to bolster communication and coordination with the private sector directly, as well as to support efforts for horizontal coordination among companies in key sectors like telecommunications, energy, transportation, and food.

One recent positive sign was the inclusion of private sector executives in the inaugural convening of the Whole-of-Society Defense Resilience Committee on September 27, 2024. According to press reporting, external attendees included representatives from Google, the cybersecurity firm Trend Micro, and the supermarket chain Pxmart Co.[59]

## Will to Fight

As the ongoing war in Ukraine decisively indicates, the will to resist is vital for the ability to repel and resist an invading force. A 2018 RAND study concludes, "Argu ably, will to fight is the single most important factor in war."[60]

There are vexing questions, however, about Taiwan's will to fight. Some polls, such as a 2021 poll conducted by the Taiwan Foundation for Democracy, show that more than 70 percent of respondents would resist a Chinese invasion; this number drops by 10 percent if the attack comes after Taiwan declares independence. In a separate poll conducted by *Global Views Monthly* in 2022, just over 40 percent stated they would be willing to fight for Taiwan. Still another poll from the same year reports that 61 percent of survey respondents would fight for Taiwan if the PLA attacked.[61]

Because the threat of an attack on Taiwan currently feels distant to many on the island, and because Beijing's gray zone actions have to some extent become normalized to many Taiwan inhabitants, both assessing and galvanizing public resolve are challenging. Polling data are an imperfect measure for the will to fight, as they necessarily omit variables that would be key to determining how many in society actually resist. For example, what expectations do the Taiwanese people have about their leadership's competence and resolve? What expectations do they have of the United States and the dependability of its quasi-security commitment as outlined in the Taiwan Relations Act? Recent polling by the think tank Academia Sinica shows that views of the United States are mixed, with just over 40 percent of respondents agreeing the United States is a "credible country."[62] The connection between the will to fight and U.S. credibility matters greatly, as there is understandably a blunted incentive to resist the PLA if the expectation is that the United States will sit on the sideline. For all Taiwan can and should do to provide for its own defenses, it probably could not defeat a Chinese invasion absent significant support from the United States.[63]

Further, successive governments on Taiwan have faced the dilemma of how to sufficiently raise the threat awareness of a possible attack or blockade to facilitate the difficult investments or sacrifices Taiwan must make without unduly panicking the island's small population, creating a brain drain, or redirecting much-needed foreign direct investments to safer locations. Several senior Taiwanese government officials have privately stated their deep frustration with Western media coverage that frames Taiwan as "the most dangerous place on earth," as this narrative potentially drives away investment precisely at the time Taipei is seeking to build Taiwan into a global technology powerhouse in sectors extending beyond semiconductors.[64] In addition, taking a more overt stance in publicizing

Chinese aggression toward Taiwan could, in itself, provoke more such actions by Beijing as punishment.

## Integration with Allies

Taiwan's small population, combined with its geographic and diplomatic isolation, means resilience will demand active international collaboration. Despite these severe limitations, successive governments on Taiwan have built out substantive partnerships for a wide array of issues critical to its prosperity and security. These include areas from trade and trade diversification, such as the 2016 New Southbound Policy, to technology, where Taipei has been building unique partnerships leveraging the singular advantage it has in its cutting-edge semiconductor industry. Taiwan has also leveraged world-leading public health capabilities to expand cooperation on pandemic preparedness.

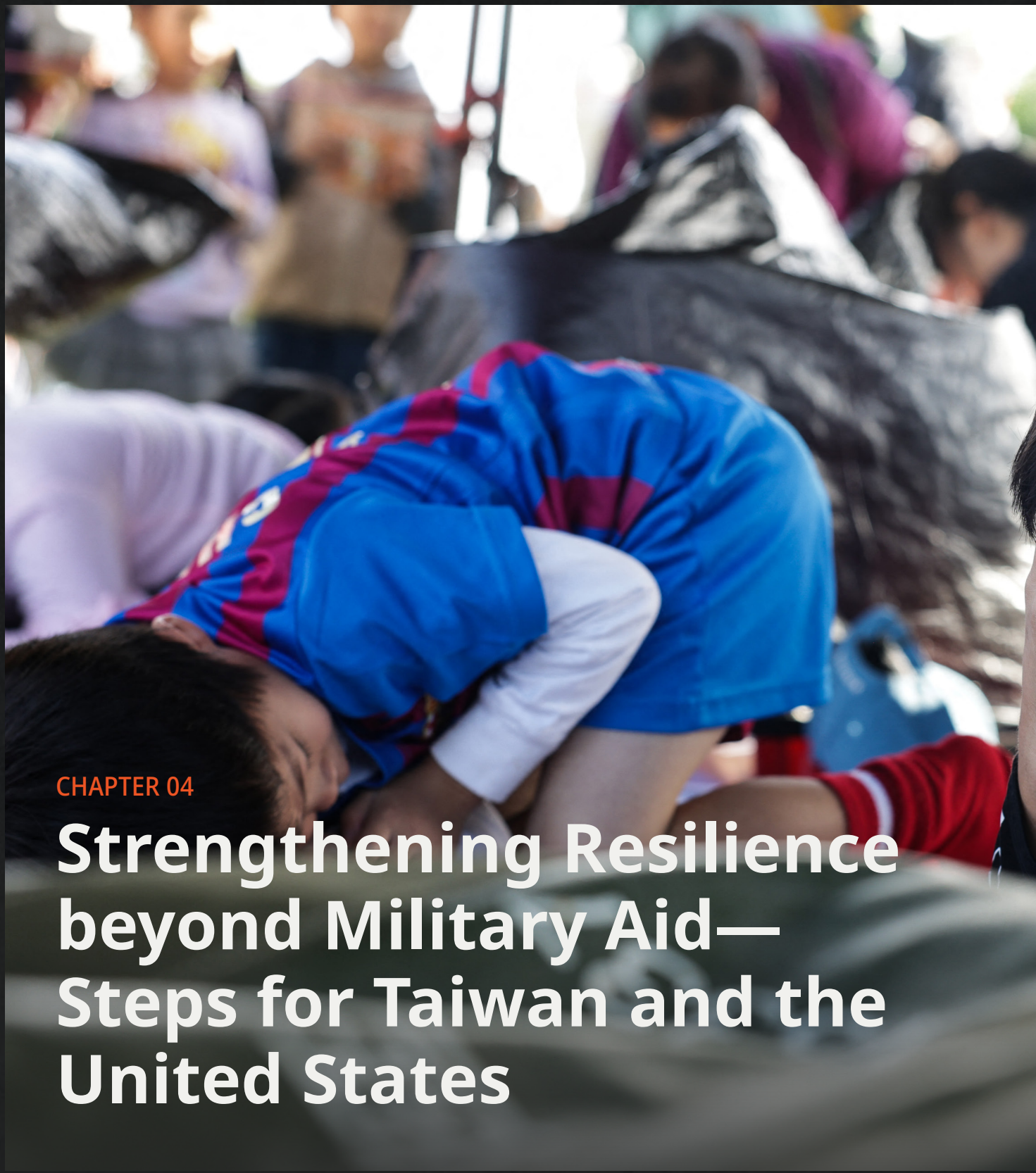
Related to overall societal resilience, Taiwan's efforts have been more mixed. One notable success is the GCTF, formed in 2015 in partnership with Japan, the United States, and Australia to facilitate discussions and cooperation between Taiwan and a range of international stakeholders on issues ranging from digital crimes to media literacy. The GCTF has also provided a platform for deeper discussion and partnership on issues that directly affect Taiwan's resilience, including supply chain security, trade diversification, telecommunication resilience, and combatting disinformation.[65] Although the GCTF demonstrates that creative organization structures can help Taiwan participate more fully in critical global conversations, it is still unclear how many of the workshops and discussions it has facilitated have translated into concrete or meaningful action that is changing the facts on the ground.

Taiwan has also done well in finding discrete areas for bilateral cooperation on issues including cybersecurity, food security, public health, and disaster preparedness. Highlights include the following:

- In 2021, the United States and Taiwan launched the U.S.-Taiwan Technology, Trade and Investment Collaboration (TTIC) to strengthen dialogue on supply chain security and resiliency. After convenings in 2021 and 2022, however, the TTIC went dark.[66]
- Taipei has signed a range of MOUs focusing on public health with foreign partners including the United States, Canada, the United Kingdom, and the Czech Republic. Not all of these, however, focus on strengthening Taiwan's capabilities and resilience. The agreement with the Czech Republic, for example, targets the rebuilding of Ukraine's shattered primary healthcare system.[67] Thus, many of Taiwan's external partnerships have a dual nature: they attempt to thread a needle of being substantive but also normalizing and expanding Taiwan's international space.
- NICS signed an MOU with Lithuania's Innovation Agency to bolster digital resilience. Tang, then head of MODA, stated that Lithuania, "value-wise, is the closest to Taiwan in the world" and that the partnership gave Taiwan the ability to draw on the Lithuanian government's experience combatting cyberattacks and disinformation.[68]

## Conclusion

As this chapter argues, Taiwan has taken some laudatory steps to strengthen resilience, but its efforts thus far are inadequate. For example, there is limited evidence of a coordinated and effective civilian readiness program that addresses economic and social disruptions. This is a critical gap, especially in light of current and future Chinese activities to target Taiwan's financial systems, electricity grid, telecommunications network, or other areas. In addition, the readiness and resolve of Taiwan's civilian population to resist in the event of foreign aggression also remains concerning. To help resolve these and other issues, the next chapter turns to recommendations.



CHAPTER 04

# Strengthening Resilience beyond Military Aid—Steps for Taiwan and the United States

**Children take shelter when hearing air raid sirens during an event in New Taipei City on November 18, 2023.**
I-HWA CHENG/AFP VIA GETTY IMAGES

**The geopolitical importance of Taiwan in the Indo-Pacific region has made it a focal point for U.S. strategic interests**, particularly in the context of countering Chinese influence and aggression. However, while the United States has invested significantly in bolstering Taiwan's military capabilities, there has been a notable lack of attention to enhancing the resilience of Taiwanese society. A robust societal resilience strategy is essential not just for immediate military deterrence but also for the long-term survival and thriving of Taiwan in the face of potential Chinese aggression.

Despite also highlighting the importance of developing asymmetric capabilities, U.S. strategy toward Taiwan has nonetheless heavily emphasized providing advanced military hardware, such as F-16 fighter jets, M1 Abrams tanks, HIMARS rocket launchers, Harpoon coastal defense systems, and Javelin antitank missiles. These systems are indeed crucial for Taiwan to maintain a credible defense posture against a conventional invasion by China. Moreover, the training provided to Taiwan's military, including joint exercises and instruction on the use of advanced systems, is designed to enhance Taiwan's ability to respond effectively in a high-intensity conflict.

However, the focus on military assistance overlooks several critical factors. First, while advanced weaponry can serve as a deterrent, it does not address the broad spectrum of challenges Taiwan would face in a protract-

ed conflict with China or increased gray zone activities. These challenges include not just military confrontations but also economic warfare, cyberattacks, disinformation campaigns, and attempts at political subversion. In these areas, Taiwan's societal resilience—its ability to withstand and recover from various forms of coercion—is as important as its military strength.

Second, historical examples highlight the limitations of relying solely on military aid without concurrent efforts to build societal resilience. In numerous conflicts, from Vietnam to Afghanistan, the failure to develop a society's internal strength and cohesion has led to the collapse of resistance, even in the presence of superior military technology. Taiwan's situation, while unique, shares some parallels with these cases, particularly in terms of the asymmetric nature of the threat it faces from China.

The remainder of this chapter is divided into three sections. The first discusses steps the Taiwanese government could take to improve its resilience. The second section provides an overview of steps the United States and other international actors can take to aid Taiwan. The third section offers a summary of the main conclusions and recommendations.

## Steps for the Taiwanese Government to Take on Its Own

This section focuses on recommendations in four areas: raising threat awareness, improving ties to the private sector, bolstering energy infrastructure, and stockpiling food and energy.

### Raising Threat Awareness among the People of Taiwan

The Taiwanese government understandably fears stoking panic among its population by highlighting the extent of the PRC threat. Yet at the same time, hesitancy creates an artificial barrier to galvanizing public support for the necessary and potentially costly reforms Taiwan must undertake to ensure its free and democratic future.

> **A robust societal resilience strategy is essential not just for immediate military deterrence but also for the long-term survival and thriving of Taiwan in the face of potential Chinese aggression.**

This tension is important for several reasons. First, *perceptions* of resolve are important for shaping Beijing's calculus. If PLA planners assume a passive population, this increases the likelihood of a possible attack or miscalculation. Second, there is an inextricable link between U.S. perceptions of Taiwan's will to fight and the willingness of Americans to expend significant financial resources and lives in defense of Taiwan. No political leader in the United States will advocate for sacrificing Americans' blood and treasure to protect Taiwan if there is a widespread perception that the Taiwanese people themselves are not willing to fight for their freedom. Of course, many Taiwanese leaders understand this; as Joseph Wu, the secretary-general of the Taiwan National Security Commission, stated bluntly, "We have no right to ask others to help us if we are not prepared to defend ourselves."[1] Finally, many of the reforms outlined in this report require significant political and financial sacrifice, which becomes more difficult if the population does not have sufficient grasp of the enormity of the challenge China presents today and tomorrow.

One starting point is greater transparency throughout the spectrum of Chinese gray zone and military actions. In private, Taiwanese government officials have reported being vexed that the Japanese military first disclosed on Twitter that the Chinese had fired missiles over Taiwan in the wake of Speaker Pelosi's trip to the island in August 2022. Understandably, Taipei did not want to panic the population. Yet through a higher tempo of controlled disclosures, Taipei could

better educate its population about the threat and galvanize public support for preparing for a range of crisis scenarios.

Taiwan should establish a dedicated public communication platform that regularly updates citizens and the global public on Chinese intimidation tactics, including disinformation campaigns, cyberattacks, and military maneuvers. An objective data-driven platform would not only help foster a public dialogue but also give citizens tools to discern between actual threats and misinformation. In parallel, Taiwan needs to force better coordination and public messaging strategies across the Office of President, MND, MOFA, MODA, and MOI to ensure that consistent messages about the growing threat level are being communicated to the Taiwanese people.

## Improving Ties to the Private Sector

It is critical for Taipei to strengthen links with the private sector. In addition to the efforts that are beginning to take shape, Taiwan might consider two ideas. First, Taipei should create a private sector "Resilience Advisory Board" comprising senior leaders from key private sector firms and industries that can convene under the auspices of the Whole-of-Society Defense Resilience Committee, thereby engaging directly with President Lai and his senior leadership team. The board would not only coordinate between the private sector and the Taiwanese government but also serve as a critical node for driving more substantive and strategic discussions among private sector firms about how they are building internal resilience, sector-specific resilience, and resilience across the entire economy.

Second, the Taiwanese government should consider establishing an annual Taiwan economic security forum to drive conversations between the government and private sector and allow third countries and their respective private sector firms to deepen their relationships with Taiwan. In the comparative cases discussed in chapter 2, governments developed strong relations with foreign companies, including large multinational companies, to strengthen resilience. The reality is that there is a global conversation about Taiwan's importance for global innovation, yet Taiwan companies and actors often are not at the table, given the sensitivity of discussing Taiwan in many foreign capitals. Having this conversation would be both prudent and likely effective for Taipei.

Finally, borrowing from the Finnish model, the Taiwan Ministry of Defense, in conjunction with the newly established Whole-of-Society Defense Resilience Committee, should run invitation-only, regional training courses for media organizations, religious leaders, and private sector representatives in order to better understand the challenges these actors would face in the event of a crisis, but also to help build bridges between the government and external actors.

## Bolstering the Energy Infrastructure

Taiwan must take several steps to boost its energy infrastructure and strengthen resilience. First, and most politically challenging, the importance of nuclear power to Taiwan's overall resiliency cannot be avoided. As Taiwan seeks to secure its energy future amid growing threats, nuclear energy offers a reliable carbon-neutral source of electricity that does not rely on volatile fuel imports. Currently, Taiwan's three nuclear power plants contribute approximately 10–15 percent of the island's total electricity generation. However, with plans to phase out nuclear energy by 2025, Taiwan faces the difficult decision of balancing energy security with public concerns over nuclear safety.

To enhance its resilience, Taiwan could reconsider extending the lifespan of its existing nuclear plants or even constructing new, safer reactors. For example, maintaining the current nuclear capacity would require an extension of the operating licenses for these plants, potentially adding another 5–10 years of service. Alternatively, constructing new advanced reactors, such as small modular reactors (SMRs), could provide a safer and more flexible nuclear option, potentially contributing up to 20 percent of Taiwan's energy mix by 2035. While politically challenging, ensuring a stable nuclear energy supply could significantly reduce Taiwan's vulnerability to external energy pressures and contribute to a more resilient and self-sufficient energy system.

Second, recent efforts to decentralize and upgrade the island's power grid must be accelerated. Taiwan's power grid is the backbone of its economic and societal functions, yet it remains vulnerable to both natural

disasters and potential military strikes. Decentralizing the grid by increasing the number of microgrids and local power generation units would reduce the risk of widespread blackouts and enhance the system's resilience to targeted attacks or natural calamities. Currently, Taiwan relies heavily on centralized power generation facilities, with nearly 80 percent of electricity produced by just a few large plants. To mitigate risks, Taiwan should aim to decentralize at least 30–40 percent of its power generation within the next decade, with a focus on renewable energy sources like solar and wind, which are more adaptable to decentralized systems.

Moreover, upgrading the grid with advanced technologies such as smart grids, which allow for real-time monitoring and rapid response to disruptions, is crucial. In September 2022, Taiwan's utility monopoly, Taiwan Power Company (known as Taipower), announced the Grid Resilience Strengthening Construction Plan, which pledged $17.7 billion over 10 years to "comprehensively upgrade the national electrical grid system" to make it more resilient in the face of growing power outages.[2] However, experts recommend doubling this investment to accelerate progress and ensure the grid can withstand both environmental and geopolitical threats.

## Food, Energy, and Water Stockpiling

Taipei can take several steps to address these issues, many of which are beyond the scope of this report. These include investments in agricultural yield-enhancing technologies, efforts to boost urban microfarming and smart farming, and steps to enhance resiliency along the food supply chain.

Given these are all long-term investments and Taiwan is a small island with limited arable land (and many competing uses for it), there is a ceiling to how much it can do to alleviate its basic reliance on imports. Thus, increased stockpiling is the necessary foundation of its food security efforts insofar as they relate to a possible national disaster or, more extreme, a direct attack by the PLA or prolonged blockade of the island. Significantly increasing strategic reserves of staples (rice, grains, and essential nonperishables) and strengthening cold storage capacity for vegetables, fruits, dairy, and meat products will be essential. Additionally, Taipei must make investments in the resiliency of the electricity infrastructure that can maintain these food supplies.

Next, the current stockpiles of hydrocarbons must be dramatically increased. Taiwan's strategic energy reserves are crucial not only for sustaining its economy during peacetime but also for ensuring resilience in times of crisis. The island's vulnerability to natural disasters, such as typhoons and earthquakes, can severely disrupt supply chains, making it imperative to have substantial reserves to mitigate these risks. Furthermore, in the context of growing Chinese aggression, Taiwan's energy security is intertwined with its national security. Currently, Taiwan's government mandates a 90-day reserve of crude oil, yet experts suggest expanding this to at least 180 days to ensure sufficient coverage in the event of a prolonged crisis. Doing so would require increasing reserves from approximately 36 million barrels to 72 million barrels.

Additionally, Taiwan's natural gas reserves, which currently stand at around 10–15 days of supply, need to be bolstered to at least 60 days, necessitating the construction of additional storage facilities capable of holding an estimated 7.2 million cubic meters of liquefied natural gas (LNG). These increases would provide Taiwan with the necessary buffer to withstand potential blockades or disruptions to its energy imports, ensuring its military and civilian infrastructure remain operational. Therefore, building up these reserves is not merely a precaution but a strategic necessity that enhances Taiwan's ability to navigate an increasingly precarious geopolitical landscape, reinforcing its sovereignty and resilience against external pressures.

On the issue of water security, Taipei has attempted to mitigate these challenges by investing in water recycling, desalination, and reservoir management, but rapid industrial growth and urbanization continue to outpace these efforts. Without more aggressive conservation policies and infrastructure upgrades, Taiwan's ability to adapt to climate-induced water stress will be limited, threatening its overall resilience in maintaining economic growth, food security, and environmental sustainability.

In a crisis, such as a natural disaster or a potential Chinese invasion, Taiwan's potable water distribu-

tion plan would undergo profound stress. During the aforementioned 2021 drought and Typhoon Haikui in 2023, Taiwan relied on emergency measures such as water rationing and trucking in water to areas in critical need. Building on these experiences, Taiwan must establish decentralized water distribution networks to ensure access during infrastructure failures. For example, mobile desalination devices and plants could be deployed to coastal regions to convert seawater into potable water in emergency situations.[3]

Taiwan should also bolster its reserve of potable water. The government has started to build emergency reservoirs and underground water storage systems accessible in times of crisis. Prepositioning bottled water reserves and distributing portable filtration systems to households can further enhance readiness. Additionally, Taiwan could enhance its digital infrastructure for crisis management, using real-time data and artificial intelligence (AI) to prioritize water distribution to vulnerable areas and critical industries and ensure equitable access.

# Build on Existing Cooperation Mechanisms

This section highlights the need to reinforce several ongoing cooperation mechanisms that could be further developed to strengthen resilience.

## Roles for the United States

This research reveals a lack of established U.S. and international attention and effort to systematically assess Taiwan's resilience and develop a comprehensive assistance plan to improve resilience in Taiwan. The conversation is much more advanced than where it was just several years ago, but still, this must be an area of greater urgency across the U.S. government. Much of the U.S. military's focus has been on providing military assistance and training to help Taiwan resist a conventional invasion and gray zone activities. The United States has also engaged with Taiwan through initiatives like the EPPD, which includes some focus on technology and security.

However, U.S. efforts have not been sufficient to help Taipei meet the full spectrum of threats it faces or to prepare society to withstand external threats and coercion. As this report's review of historical cases suggests, a population that lacks resilience is in danger of external and internal aggression. A robust societal resilience strategy is essential not just for immediate deterrence but also for the long-term survival and thriving of Taiwan in the face of external threats. In addition, many of the efforts to enhance Taiwan's resilience could be applied to other allies and partners after being suitably modified for their situation. Thankfully, the United States and its partners can positively contribute to Taiwan's ongoing efforts to strengthen its societal resilience in several areas.

## U.S.-Taiwan Economic Prosperity Partnership Dialogue

The EPPD, launched in 2020, aims to strengthen economic ties and enhance cooperation between the United States and Taiwan. This dialogue addresses a broad spectrum of economic issues, including supply chain security, technology, energy, healthcare, and infrastructure. The EPPD functions as a forum for both nations to tackle common economic challenges and identify opportunities for collaboration, especially in key sectors like semiconductors and 5G technology, which are vital to the global economy.

To enhance the effectiveness of the EPPD in improving Taiwan's resilience, the United States should consider the following steps:

- **Broaden participation.** Include representatives from the private sector, civil society, and academia to provide diverse perspectives and expertise. This multistakeholder approach would ensure that the dialogue addresses the needs and concerns of all relevant parties.
- **Regional integration.** Encourage the inclusion of other Indo-Pacific nations—either directly or through representatives from the private sector—in specific discussions, fostering regional economic integration and cooperation. This would help Taiwan diversify its economic partnerships and strengthen its role in regional supply chains. However, these discussions must be held careful-

**“However, U.S. efforts have not been sufficient to help Taipei meet the full spectrum of threats it faces or to prepare society to withstand external threats and coercion.**

ly and not in public since many governments may be concerned about Beijing’s response.

- **Innovation and research and development collaboration.** Establish joint research and development (R&D) initiatives focused on emerging technologies, such as AI and green energy. This collaboration would not only drive economic growth but also ensure that both the United States and Taiwan remain competitive in global innovation.
- **Cybersecurity cooperation.** Deepen cooperation on cybersecurity within the EPPD framework, particularly in protecting critical infrastructure and securing digital economies, ensuring both economies withstand and respond to cyber threats effectively.

## Global Cooperation and Training Framework

The GCTF is an initiative Taiwan and the United States cofounded in 2015, with Japan later joining as a full partner and other countries, such as Australia, joining as partners or participants. The GCTF aims to enhance Taiwan’s participation in global issues and share Taiwan’s expertise with the international community. The framework facilitates training workshops and cooperative activities on a variety of topics, including public health, disaster relief, environmental protection, cybersecurity, and women’s empowerment. These events, often held in Taiwan, serve as platforms for government officials, experts, and NGOs from across the Asia-Pacific region and beyond to exchange knowledge, build capacity, and strengthen regional cooperation.

As it relates to resilience, the GCTF can expand along the following lines:

- **Broaden the scope of topics.** While the GCTF already covers a wide range of important areas, it could expand to include additional critical topics such as civil defense, legal reform, supply chain security, and economic resilience. Training sessions and workshops on these topics would help Taiwan and its partners better prepare for crises and strengthen their ability to respond to various challenges.
- **Increase participation from regional partners.** Expanding participation to more countries in the Indo-Pacific region would not only bolster regional collaboration but also increase Taiwan’s integration into international networks. This broader participation could help Taiwan develop stronger ties with neighboring countries, thereby enhancing its regional resilience.
- **Focus on technology and cybersecurity.** Given the increasing importance of cybersecurity and emerging technologies, the GCTF could introduce more specialized programs focused on protecting critical infrastructure and promoting technological innovation. This would help Taiwan and its partners stay ahead of cyber threats and technological challenges.
- **Promote public-private partnerships.** Engaging the private sector more deeply in GCTF activities could provide new resources and perspectives. Public-private partnerships could be fostered in areas such as disaster response, cybersecurity, and innovation, bringing in expertise and investment from leading industries; they could also be messaged to show the integration of Taiwan beyond the narrowing diplomatic domain.
- **Establish a permanent secretariat.** To enhance coordination and continuity, establishing a permanent GCTF secretariat could be beneficial, although admittedly difficult to achieve for bureaucratic reasons. This body could oversee the

planning and implementation of activities, ensure consistent communication between partners, and help secure funding for future initiatives.

## Cooperation between USDA's Foreign Agricultural Service and Taiwan's Ministry of Agriculture

On June 3, 2024, the American Institute in Taiwan, the de facto U.S. embassy in Taiwan, and the Taipei Economic and Cultural Representative Office signed an agreement to establish formal cooperation between the USDA Foreign Agricultural Service and the Taiwanese Ministry of Agriculture to expand "food security related cooperation and exchanges."[4] While not explicitly designed to deal with a possible invasion or blockade, the MOU nonetheless provides a solid foundation for expanding cooperation and coordination between the two sides on a range of issues related to both crisis and precrisis scenarios.

## Expanded U.S.-Taiwan Military Coordination

A number of areas under the current One China Policy framework that govern the unofficial U.S. relationship with Taiwan can be expanded to increase Taiwan's resilience and civil defense capabilities:

1. As the U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party outlines in its May 2023 *Ten for Taiwan* report, congruent with section 5503 of the 2023 National Defense Authorization Act (NDAA), the U.S. military should build an aggressive "regional contingency stockpile," as well as war reserve stocks for allies located on Taiwan.[5]
2. Also in congruence with the NDAA and the Taiwan Relations Act, the U.S. military, including and especially U.S. special operations forces, should increase collaboration with the ADMA to ensure more cohesion and coherence in scenarios where vast sections of Taiwanese society need to be mobilized for a crisis contingency.
3. The United States should expand International Military Education and Training (IMET) for Taiwan, particularly to improve civil defense and will to fight. IMET is a U.S. government-funded initiative aimed at enhancing the military capabilities of foreign nations by offering training to their military personnel in the United States. The program is administered by the U.S. Department of State and executed by the U.S. Department of Defense. Given the strategic importance of Taiwan in the Indo-Pacific region and the increasing tension across the Taiwan Strait, expanding IMET in relation to Taiwan could be a crucial element in enhancing Taiwan's defense capabilities and reinforcing U.S.-Taiwan relations. Possible areas for expanding the IMET program include the following:
    - Increase the number of IMET slots available to Taiwanese military personnel, allowing more Taiwanese officers to receive training in the United States, thereby expanding their skill sets and enhancing interoperability with U.S. forces.
    - Tailor IMET training to address Taiwan's unique security challenges, such as cyber defense, anti-submarine warfare, and coastal defense.
    - Offer more advanced and longer-term educational programs to deepen the expertise of Taiwan's military personnel. Programs at institutions like the U.S. Army War College and the Naval War College could provide strategic-level education to senior Taiwanese officers.
    - Integrate more joint exercises as part of IMET or incorporate simulation-based training that mirrors potential conflict scenarios in the Taiwan Strait. This could involve wargaming and strategic decisionmaking exercises that prepare Taiwanese officers for real-world contingencies, including analyzing the implications of strengthened resilience.
    - Provide training in civil-military relations, governance, and respect for international law, which could help further professionalize Taiwan's military, ensuring it aligns with democratic values and human rights.
4. The United States and other allies should consider a rapid reaction team focused on detecting and stopping cyberattacks.[6] Allies have varying capa-

bilities, and a devastating cyberattack could be a game changer. If classification is a hurdle, then a public-private consortium might be a work-around.

## Conclusion

There is an urgent need to strengthen resilience in Taiwan. This chapter concludes with some final thoughts about strengthening resilience.

First, resilience is only one part of deterrence. Countries and societies, including Taiwan, still need a strong military capable of resisting invasion and other coercive activity. In addition, a strong military requires developing the capabilities to conduct offensive actions, including offensive cyber operations.

Second, the steps highlighted in this chapter generally need to be set up *well in advance* of a crisis—ideally years in advance. It takes time and money to bolster strategic design and command structure, establish additional legal measures, enhance strategic communications and psychological resilience, strengthen civil defenses, improve the population's will to fight, reinforce nonviolent resistance networks, and increase integration with allies and partners. In Ukraine, Russia annexed Crimea in 2014 and proceeded to conduct a range of military and offensive cyber actions over the next several years—well before Russia's February 2022 full-scale invasion. This gave the Ukrainian government and the private sector—including such companies as Microsoft and Amazon Web Services (AWS)—years to increase resilience.

Third, strengthening resilience requires a careful balancing act. Too many high-profile actions can incite a potential adversary, worsen the security situation, and create a security dilemma—a situation in which actions taken by one side to increase its security can make others less secure and lead them to respond in kind. The result is a spiral of hostility that leaves neither side better off than before. Finland has built resilience over decades, even as its leadership has professed neutrality toward Moscow.

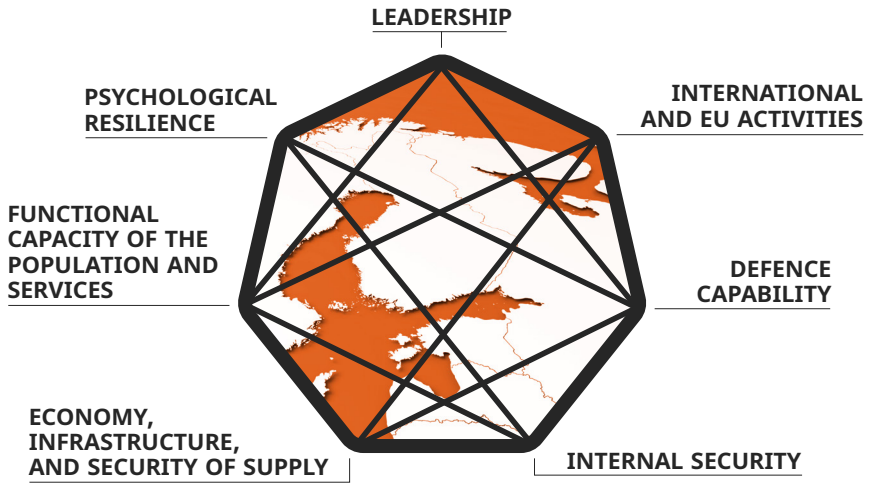
Overall, the steps outlined in this chapter are useful first steps to strengthen Taiwan's will and ability to resist external pressure, influence, and potential invasion. They would strengthen deterrence by raising the costs and risks for an aggressor weighing whether to employ conventional military or gray zone actions against Taiwan.

# Appendices

# Appendix A

## Finland's Diamond Model for Resilience

Comprehensive security is the cooperation model of Finnish preparedness, where authorities, businesses, NGOs, and citizens handle vital societal functions.[1] As highlighted in Figure A.1, vital societal functions include leadership; international and EU activities; defense capability; internal security; economy, infrastructure, and security of supply; functional capacity of the population and services; and psychological resilience.




▲ **FIGURE A.1** Finland's Diamond Model

**SOURCE** "Concept of Comprehensive Security – Building National Resilience in Finland," The Security Committee, Finland, https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/.

# Appendix B

## Finland's Security Concept for Society
## 57 Functions of Resilience

The following list includes the 57 vital functions in Finland's comprehensive security model.[1] Finland divides the functions into several key areas: leadership; international and EU activities; defense capability; internal security; economy, infrastructure, and security of supply; functional capacity of the population and services; and psychological resilience. This list also includes the ministry or ministries in charge.

### LEADERSHIP

1. Safeguarding the operating prerequisites of the state leadership
   *Ministry in charge: Prime Minister's Office*
2. Maintaining the situation picture of the state leadership
   *Ministry in charge: Prime Minister's Office*
3. Functioning of communications
   *Ministries in charge: Prime Minister's Office and all other ministries*

### INTERNATIONAL AND EU ACTIVITIES

4. Finland's role in the European Union ensuring that EU matters can be properly drafted and considered at national level and securing solidarity and mutual assistance
   *Ministries in charge: Prime Minister's Office and all other ministries*
5. Developing contacts and cooperation with foreign countries and key international actors
   *Ministries in charge: Ministry for Foreign Affairs and all other ministries in their own areas of responsibility*
6. International crisis management, humanitarian assistance, and international rescue operations
   *Ministries in charge: Ministry for Foreign Affairs, Ministry of Defence, Ministry of the Interior, Prime Minister's Office, Ministry of Social Affairs and Health, Ministry of Justice*
7. Providing Finnish citizens and foreigners permanently residing in Finland with protection and assistance outside Finland
   *Ministry in charge: Ministry for Foreign Affairs*
8. Ensuring a smooth flow of goods and services between Finland and other countries
   *Ministries in charge: Ministry for Foreign Affairs, Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry, Ministry of Transport and Communications, Ministry of Finance*

**DEFENSE CAPABILITY**

9. Finland's military defense
   *Ministry in charge: Ministry of Defence*

**INTERNAL SECURITY**

10. Ensuring legal protection
    *Ministry in charge: Ministry of Justice*

11. Holding elections and safeguarding the prerequisites of democracy
    *Ministry in charge: Ministry of Justice*

12. Maintaining public order and security
    *Ministry in charge: Ministry of the Interior*

13. Ensuring border security
    *Ministry in charge: Ministry of the Interior*

14. Ensuring the safety of supply chains and safety of goods
    *Ministry in charge: Ministry of Finance*

15. Civil defense
    *Ministry in charge: Ministry of the Interior*

16. Ensuring the maritime search and rescue capability
    *Ministry in charge: Ministry of the Interior*

17. Emergency response centers
    *Ministries in charge: Ministry of the Interior, Ministry of Social Affairs and Health*

18. Maintaining rescue services
    *Ministry in charge: Ministry of the Interior*

19. Immigration control
    *Ministries in charge: Ministry of the Interior, Ministry for Foreign Affairs, Ministry of Economic Affairs and Employment*

20. Management of large-scale immigration
    *Ministries in charge: Ministry of the Interior and Ministry of Economic Affairs and Employment*

21. Environmental emergency response
    *Ministries in charge: Ministry of the Environment, Ministry of Transport and Communications, Ministry of Economic Affairs and Employment, Ministry of the Interior, Ministry of Defence*

22. Preparedness for biological threats
    *Ministries in charge: Ministry of Social Affairs and Health, Ministry of Agriculture and Forestry, Ministry of Defence, Ministry for Foreign Affairs, Ministry of the Interior, Ministry of the Environment*

23. Preventing radiation hazards and preparing for them
    *Ministries in charge: Ministry of the Interior, Ministry of Social Affairs and Health, Ministry of Agriculture and Forestry, Ministry of the Environment, Ministry of Defence, Ministry of Economic Affairs and Employment*

24. Preparation for chemical threats
    *Ministries in charge: Ministry of Social Affairs and Health, Ministry of the Interior, Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry, Ministry of the Environment, Ministry of Defence*

### ECONOMY, INFRASTRUCTURE, AND SECURITY OF SUPPLY

25. Acquiring economic resources and focusing them, and safeguarding human resources
    *Ministry in charge: Ministry of Finance*

26. Ensuring the functioning of the financial system
    *Ministry in charge: Ministry of Finance*

27. Safeguarding public administration information and communications technology infrastructure and digital services
    *Ministries in charge: Ministry of Finance, Prime Minister's Office*

28. Ensuring availability of and access to electronic communications services
    *Ministry in charge: Ministry of Transport and Communications*

29. Safeguarding the continuation of insurance business
    *Ministry in charge: Ministry of Social Affairs and Health*

30. Securing the fuel supply
    *Ministries in charge: Ministry of Economic Affairs and Employment, Ministry of Transport and Communications, Ministry of Agriculture and Forestry*

31. Securing power supply
    *Ministry in charge: Ministry of Economic Affairs and Employment*

32. Ensuring weather, maritime, and circumstance services
    *Ministry in charge: Ministry of Transport and Communications*

33. Ensuring the availability and usability of transport services
    *Ministry in charge: Ministry of Transport and Communications*

34. Ensuring the security and operational reliability of transport and communications network
    *Ministry in charge: Ministry of Transport and Communications*

35. Ensuring the continuity of the transports essential for Finland's security of supply and foreign trade
    *Ministries in charge: Ministry of Transport and Communications, Ministry of Defence, Ministry of Economic Affairs and Employment*

36. Ensuring the functioning of the social welfare and healthcare information systems and the availability of critical supplies
    *Ministries in charge: Ministry of Social Affairs and Health, Ministry of Economic Affairs and Employment*

37. Detection and monitoring of changes taking place in the environment, adapting to the changes and combating the threats arising from them
    *Ministries in charge: Ministry of the Environment, Ministry of Agriculture and Forestry*

38. Ensuring waste management
    *Ministry in charge: Ministry of the Environment*

39. Securing resources for construction
    *Ministry in charge: Ministry of the Environment*

40. Ensuring proper housing
    *Ministry in charge: Ministry of the Environment*

41. Safeguarding the water supply
    *Ministries in charge: Ministry of Agriculture and Forestry, Ministry of Social Affairs and Health, Ministry of the Environment*

42. Flood risk management and supervision of dam safety
    *Ministry in charge: Ministry of Agriculture and Forestry*

43. Securing sufficient labor workforce
    *Ministry in charge: Ministry of Economic Affairs and Employment*

44. Maintaining the education, training, and research system
    *Ministry in charge: Ministry of Education and Culture*

45. Safeguarding vital industries and services
    *Ministry in charge: Ministry of Economic Affairs and Employment*

46. Safeguarding food supply
    *Ministries in charge: Ministry of Agriculture and Forestry, Ministry of Economic Affairs and Employment, Ministry of Transport and Communications, Ministry of Social Affairs and Health, Ministry for Foreign Affairs*

47. Ensuring the supply of daily consumer goods
    *Ministries in charge: Ministry of Economic Affairs and Employment, Ministry of Agriculture and Forestry*

### FUNCTIONAL CAPACITY OF THE POPULATION AND SERVICES

48. Ensuring the last-resort livelihood of the population
    *Ministries in charge: Ministry of Social Affairs and Health, Ministry of Finance*

49. Ensuring access to social welfare and healthcare services
    *Ministry in charge: Ministry of Social Affairs and Health*

50. Maintaining expertise and skills
    *Ministry in charge: Ministry of Education and Culture*

### PSYCHOLOGICAL RESILIENCE

51. Maintaining cultural services and protecting cultural heritage
    *Ministry in charge: Ministry of Education and Culture*

52. Ensuring the basis for religious activities
    *Ministry in charge: Ministry of Education and Culture*

53. Ensuring the continuation of youth work and activities as well as civic sports activities
    *Ministry in charge: Ministry of Education and Culture*

54. Communications
    *Ministries in charge: all ministries*

55. Combating social exclusion and inequality
    *Ministries in charge: Ministry of Social Affairs and Health, Ministry of Education and Culture, Ministry of Economic Affairs and Employment*

56. Promoting voluntary activities
    *Responsible actors: all administrative branches and organizations*

57. Recovery
    *Responsible actors: all administrative branches and organizations*

# About the Authors

**Daniel Byman** is the director of the Warfare, Irregular Threats, and Terrorism Program at CSIS. He is also a professor at Georgetown University's School of Foreign Service and director of the Security Studies Program. He is the foreign policy editor for *Lawfare* and a part-time senior adviser to the Department of State on the International Security Advisory Board. In addition to serving as the vice dean for the School of Foreign Service at Georgetown, he was a senior fellow at the Center for Middle East Policy at the Brookings Institution and a professional staff member with both the National Commission on Terrorist Attacks on the United States (9/11 Commission) and the Joint 9/11 Inquiry Staff of the House and Senate Intelligence Committees. He formerly served as research director of the Center for Middle East Public Policy at the RAND Corporation and as a Middle East analyst for the U.S. intelligence community. Dr. Byman is a leading researcher and has written widely on a range of topics related to terrorism, insurgency, intelligence, social media, artificial intelligence, and the Middle East. He is the author of nine books, including *Road Warriors: Foreign Fighters in the Armies of Jihad* (Oxford, 2019), *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs Know* (Oxford, 2015), and *A High Price: The Triumphs and Failures of Israeli Counterterrorism* (Oxford, 2011). He is the author or coauthor of almost 200 academic and policy articles, monographs, and book chapters as well as numerous opinion pieces in the *New York Times*, *Wall Street Journal*, *Washington Post*, and other leading journals. Dr. Byman is a graduate of Amherst College and received his PhD in political science from the Massachusetts Institute of Technology.

**Seth G. Jones** is president of the Defense and Security Department at CSIS. He focuses on defense strategy, military operations, force posture, and irregular warfare. He also teaches at Johns Hopkins University's School of Advanced International Studies (SAIS) and the Center for Homeland Defense and Security (CHDS) at the U.S. Naval Postgraduate School. Prior to joining CSIS, Dr. Jones was the director of the International Security and Defense Policy Center at the RAND Corporation. He also served as representative for the commander, U.S. Special Operations Command, to the assistant secretary of defense for special operations. Before that, he was a plans officer and adviser to the commanding general, U.S. Special Operations Forces, in Afghanistan (Combined Forces Special Operations Component Command–Afghanistan). He is the author of *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (W. W. Norton, 2021), *A Covert Action: Reagan, the CIA, and the Cold War Struggle in Poland* (W. W. Norton, 2018), *Waging Insurgent Warfare: Lessons from the Vietcong to the Islamic State* (Oxford University Press, 2016), *Hunting in the Shadows: The Pursuit of al Qa'ida since 9/11* (W. W. Norton, 2012), and *In the Graveyard of Empires: America's War in Afghanistan* (W.W. Norton, 2009). Dr. Jones has published articles in a range of journals, such as *Foreign Affairs*, *Foreign Policy*, and *International Security*, as well as newspapers and magazines like the *New York Times*, *Washington Post*, and *Wall Street Journal*. Dr. Jones is a graduate of Bowdoin College and received his MA and PhD from the University of Chicago.

**Jude Blanchette** was the Freeman Chair in China Studies at the Center for Strategic and International Studies (CSIS). Previously, he was engagement director at the Conference Board's China Center for Economics and Business in Beijing, where he researched China's political environment with a focus on the workings of the Communist Party of China and its impact on foreign companies and investors. Prior to working at the Conference Board, Blanchette was the assistant director of the 21st Century China Center at the University of California, San Diego. Blanchette has written for a range of publications, including *Foreign Affairs*, *Foreign Policy*, the *Wall Street Journal*, War on the Rocks, the *Financial Times*, and the *Washington Post*. His book *China's New Red Guards: The Return of Radicalism and the Rebirth of Mao Zedong* was published by Oxford University Press in 2019. Blanchette is a public intellectual fellow at the National Committee on U.S.-China Relations and serves on the board of the American Mandarin Society. He holds an MA in modern Chinese studies from the University of Oxford and a BA in economics from Loyola University in Maryland.

# Endnotes

## CHAPTER 1: INTRODUCTION

1 Yew Lun Tian and Ben Blanchard, "China Will Never Renounce Right to Use Force over Taiwan, Xi Says," Reuters, October 16, 2022, https://www.reuters.com/world/china/xi-china-will-never-renounce-right-use-force-over-taiwan-2022-10-16/.

2 "China-Backed Hackers Stepping up Attacks on Taiwan, Cybersecurity Firm Says," Al Jazeera, June 24, 2024, https://www.aljazeera.com/economy/2024/6/24/china-backed-hackers-stepping-up-attacks-on-taiwan-cybersecurity-firm-says.

3 See Jude Blanchette and Bonnie Glaser, "Taiwan's Most Pressing Challenge Is Strangulation, Not Invasion," War on the Rocks, November 9, 2023, https://warontherocks.com/2023/11/taiwans-most-pressing-challenge-is-strangulation-not-invasion/.

4 Anna M. Dowd and Cynthia R. Cook, *Bolstering Collective Resilience in Europe* (Washington, DC: CSIS, December 2022), 3, https://www.csis.org/analysis/bolstering-collective-resilience-europe.

5 Otto C. Fiala, *Resistance Operating Concept (ROC)* (MacDill Air Force Base, Florida: JSOU Press, 2020), xv.

6 Fiala, *Resistance Operating Concept*, 9.

7 Ben Connable et al., *Will to Fight: Analyzing, Modeling, and Simulating the Will to Fight of Military Units* (Santa Monica, CA: RAND, 2018).

8 Fiala, *Resistance Operating Concept*, xv. See also Robert S. Burrell and John Collison, "A Guide for Measuring Resiliency and Resistance," *Small Wars & Insurgencies* 35, no. 1 (2024): 147–72.

9 See, for example, Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (Fall 2021): 51–90.

10 Mikael Wigell, "Democratic Deterrence," *Washington Quarterly* 44, no. 1 (2021): 52–55, https://doi.org/10.1080/0163660X.2021.1893027.

11 Jyri Raitasalo, "Finnish Defense 'Left of Bang,'" *PRISM* 10, no. 2 (March 10, 2023): 86, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323915/finnish-defense-left-of-bang/.

12 On the Baltic states, see Tony Lawrence, "Estonia: Size Matters," *PRISM* 10, no. 2 (March 10, 2023), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323882/estonia-size-matters/; and Anika Binnendijk and Marta Kepe, *Civilian-Based Resistance in the Baltic States: Historical Precedents and Current Capabilities* (Santa Monica, CA: RAND, 2021), https://www.rand.org/pubs/research_reports/RRA198-3.html. On Norway and Sweden, see Fredrik Bertilsson, "The Swedish Defence Research Establishment (FOA) and the Influence of Historical Knowledge on Swedish Civil Resistance Policy," *Scandinavian Journal of History* 46, no. 1 (2021): 1–20, https://doi.org/10.1080/03468755.2021.1880474; and James Kenneth Wither, "Back to the Future? Nordic Total Defence Concepts," *Defence Studies* 20, no. 1 (2020): 61–81, https://doi.org/10.1080/14702436.2020.171849. On Switzerland, see Kevin D. Stringer, "Building a Stay-Behind Resistance Organization: The Case of Cold War Switzerland against the Soviet Union," *Joint Force Quarterly* 86 (2017): 109–14, https://ndupress.ndu.edu/Media/News/Article/1220620/.

13 Interview with Finnish government officials, May 2024, Helsinki.

14 "Resilience, Civil Preparedness and Article 3," NATO, August 2, 2023, https://www.nato.int/cps/en/natohq/topics_132722.htm.

15 Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," *International Affairs* 95, no. 2 (2019): 255–75, https://doi.org/10.1093/ia/iiz018.

## CHAPTER 2: BUILDING RESILIENCE

1 Interview with Finnish government officials, May 2024, Helsinki.

2 Interview with Finnish government officials, May 2024, Helsinki.

3 Binnendijk and Kepe, *Civilian-Based Resistance*, xi.

4 Fiala, *Resistance Operating Concept*, 14.

5 "Resilience, Civil Preparedness and Article 3"; and "Resilience Committee," NATO, October 7, 2022, https://www.nato.int/cps/en/natohq/topics_50093.htm.

6 Finnish Ministry of Defence Security Committee, *The Security Strategy for Society* (Helsinki: Government of Finland, 2017), https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

7 Fiala, *Resistance Operating Concept*, 11.

8 For those suggestions and others, see Fiala, *Resistance Operating Concept*, 76–79. For an excellent vision of labor by stage of the crisis, see Fiala, *Resistance Operating Concept*, appendix J.

9 Wither, "Back to the Future?"

10 Dowd and Cook, *Bolstering Collective Resilience in Europe*, 4.

11 Fiala, *Resistance Operating Concept*, 80; and "Resilience, Civil Preparedness and Article 3."

12 Finnish Ministry of Defence Security Committee, *The Security Strategy for Society*.

13 Interview with Finnish government official, May 2024, Helsinki.

14 Ibid.

15 Ibid.

16 Interview with Finnish government officials, May 2024, Helsinki.

17 Finnish Ministry of Defence Security Committee, *The Security Strategy for Society*.

18 Finnish Ministry of Defence Security Committee, *The Security Strategy for Society*; and Finnish Ministry of the Interior, *National Risk Assessment 2023* (Helsinki: Government of Finland, 2023), https://julkaisut.valtioneuvosto.fi/handle/10024/164629.

19 Interview with Finnish government official, May 2024, Helsinki.

20 Finland produced a risk assessment in 2015, with updates in 2018 and 2023. A working group was appointed to revise the national risk assessment (Finnish Ministry of the Interior, *National Risk Assessment 2023*).

21 OECD, "Critical Infrastructure Resilience Case-Study: Electricity Transmission and Distribution in Finland," in *Good Governance for Critical Infrastructure Resilience* (Paris: OECD Publishing, 2019), https://doi.org/10.1787/02f0e5a0-en.

22 Interview with Finnish nongovernment experts, May 2024, Helsinki.

23 Interview with Finnish government official.

24 "Resilience, Civil Preparedness and Article 3."

25 Fiala, *Resistance Operating Concept*, 12, 24.

26 Interview with Finnish nongovernment experts, May 2024, Helsinki.

27 As quoted in Richard Milne, "War with Russia? Finland Has a Plan for That," *Financial Times*, March 27, 2022, https://www.ft.com/content/c5e376f9-7351-40d3-b058-1873b2ef1924.

28 Author's translation. Valmiuslaki [Emergency powers act], 1552/2011, https://www.finlex.fi/fi/laki/ajantasa/2011/20111552.

29 Interview with Finnish government official, May 2024, Helsinki.

30 Robin Häggblom, "Finland Has a Plan for Russia's Little Green Men," *Foreign Policy*, August 15, 2020, https://foreignpolicy.com/2020/08/15/finland-army-russia-little-green-men/; and Milne, "War with Russia?"

31 Interview with Finnish nongovernment experts, May 2024, Helsinki.

32 Ibid.

33 Interview with Finnish government official, May 2024, Helsinki.

34 Essi Lehto, "Finland Plans to Ban Russians from Buying Property," Reuters, September 2, 2024, https://www.reuters.com/world/europe/finland-plans-ban-russians-buying-property-2024-09-02/.

35 Binnendijk and Kepe, *Civilian-Based Resistance*, 44.

36 Fiala, *Resistance Operating Concept*, 11–12, 63, 173, 198.

37 Ibid., 8, 31–33.

38 Lithuania Ministry of National Defence, *Prepare to Survive Emergencies and War: A Cheerful Take on Serious Recommendations* (Vilnius: Military Cartography Centre of the Lithuanian Armed Forces, 2015), https://lt72.lt/wp-content/uploads/2020/12/katurimez-inotipraktiniaipatarimaienel.pdf.

39 Swedish Civil Contingencies Agency, *If Crisis or War Comes* (Karlstad, Sweden: MSB), 7, https://rib.msb.se/filer/pdf/30307.pdf.

40 Häggblom, "Finland Has a Plan."

41 Milne, "War with Russia?"

42 Interview with Finnish government official.

43 Interview with Finnish nongovernment experts, May 2024, Helsinki.

44 Interview with Finnish government and nongovernment experts, May 2024, Helsinki.

45 Interview with Finnish nongovernment experts, May 2024, Helsinki.

46 Fiala, *Resistance Operating Concept*, 3, 27.

47 Binnendijk and Kepe, *Civilian-Based Resistance*, 106.

48 Jan Osburg, *Unconventional Options for the Defense of the Baltic State* (Santa Monica, CA: RAND, 2016), 4.

49 See, for example, *Bericht des Bundesrates über die Sicherheitspolitik der Schweiz* (Berne: Government of Switzerland, June 1973); Hans von Dach Bern, *Total Resistance: Swiss Army Guide to Guerilla Warfare and Underground Operations* (Boulder, CO: Paladin Press, 1992); and Fiala, *Resistance Operating Concept*, 171–75.

50 Häggblom, "Finland Has a Plan."

51 Finnish Ministry of the Interior, "Fact Sheet: Civil Defence and Civil Defence Shelters in Finland." Published document received in May 2024 in Helskini.

52 Milne, "War with Russia?"

53 Wither, "Back to the Future?"

54 Kalle Schoenberg, "Suomi varautuu mahdolliseen Venäjän uhkaan aivan eri tavalla kuin etelänaapurit—luottaa vanhaan kikkaan" [Finland prepares for a possible threat from Russia in a completely different way than its southern neighbors—it relies on an old gimmick], Yle, May 24, 2024, https://yle.fi/a/74-20089888.

55 Binnendijk and Kepe, *Civilian-Based Resistance*, 100.

56 Interview with Finnish government officials, May 2024, Helsinki.

57 "Resilience, Civil Preparedness and Article 3."

58 See Binnendijk and Kepe, *Civilian-Based Resistance*, 96, 107. For EU rules, see "Security of

Oil Supply," European Commission, https://energy.ec.europa.eu/topics/energy-security/eu-oil-stocks_en.

59 Maschmeyer, "The Subversive Trilemma."

60 Fiala, *Resistance Operating Concept*, 60.

61 Osburg, *Unconventional Options*, 4.

62 Interview with Finnish government officials, May 2024, Helsinki.

63 Aaro Toivonen, "National Emergency Supply Organisation and Healthcare Pool" (PowerPoint presentation, One Health Security Conference, Finnish Institute for Health and Welfare, Helsinki, October 14, 2019), slide 12, https://www.slideshare.net/slideshow/aaro-toivonen-national-emergency-supply-agency-finland/186277556.

64 Interview with Finnish government officials, May 2024, Helsinki.

65 Ibid.

66 Interview with Finnish government officials, May 2024, Helsinki.

67 Interview with Finnish government officials, May 2024, Helsinki.

68 Interview with Finnish government official, May 2024, Helsinki.

69 Interview with Finnish government officials, May 2024, Helsinki.

70 Interview with Finnish government officials, May 2024, Helsinki.

71 Interview with Finnish government officials, May 2024, Helsinki.

72 Ibid.

73 Interview with Finnish government official, May 2024, Helsinki.

74 Interview with Finnish government officials, May 2024, Helsinki.; and "Government to Improve Protection of Infrastructure Critical to Functioning of Society," Finnish government, January 19, 2024, https://valtioneuvosto.fi/en/-/1410869/government-to-improve-protection-of-infrastructure-critical-to-functioning-of-society.

75 Interview with Finnish government officials, May 2024, Helsinki.

76 On the definition of "will to fight," see, for example, Connable et al., *Will to Fight*.

77 Winston Churchill, "We Shall Fight on the Beaches," International Churchill Society, June 4, 1940, https://winstonchurchill.org/resources/speeches/1940-the-finest-hour/we-shall-fight-on-the-beaches/.

78 See Connable et al., *Will to Fight*; and Michael J. McNerney et al., *National Will to Fight: Why Some States Keep Fighting and Others Don't* (Santa Monica, CA: RAND, 2019).

79 Binnendijk and Kepe, *Civilian-Based Resistance*, 113.

80 Connable et al., *Will to Fight*, 33–112; and Mcnerney et al., *National Will to Fight*.

81 Isak Svensson and Mathilda Lindgren, "Community and Consent: Unarmed Insurrections in Non-democracies," *European Journal of International Relations* 17, no. 1 (2011): 97–120, https://doi.org/10.1177/1354066109350045.

82 On the collapse of the Afghan will to fight see, for example, "Remarks by President Biden on Afghanistan," White House, August 16, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/16/remarks-by-president-biden-on-afghanistan/.

83 Robert K. Brigham, *ARVN: Life and Death in the South Vietnamese Army* (Lawrence: University Press of Kansas, 2006); and Anthony James Joes, *The War for South Vietnam: 1954–1975* (Westport, CT: Praeger Publishers, 2001).

84 Fiala, *Resistance Operating Concept*, 8.

85 Fiala, *Resistance Operating Concept*, 7.

86 Interview with Finnish government officials, May 2024, Helsinki.

87 Interview with Finnish government official, May 2024, Helsinki.

88 Interview with Finnish government officials, May 2024, Helsinki.

89 Corneliu Bjola and Krysianna Papadakis, "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience," *Cambridge Review of International Affairs* 33, no. 5 (2020): 638–66, https://doi.org/10.1080/09557571.2019.1704221; and interview with Finnish government official, April 11, 2024.

90 Interview with Finnish government official, May 2024, Helsinki.

91 Milne, "War with Russia?"; and interview with Finnish government officials, May 2024, Helsinki.

92 Interview with Finnish government official, May 2024, Helsinki.

93 Interview with Finnish nongovernment experts, May 2024, Helsinki.

94 Interview with Finnish government officials, May 2024, Helsinki.

95 Advisory Board for Defence Information, *Finns' Opinions on Foreign and Security Policy, National Defense and Security* (Helsinki: Ministry of Defence, January 2024), https://www.defmin.fi/files/5893/ABDI_Finns_opinions_on_foreign_and_security_policy_national_defence_and_security_january_2024.pdf.

96 Interviews with Finnish government officials, May 2024, Helsinki; and Reetta Riikonen, Teemu Tallberg, Jarkko Kosonen, and Alisa Puustinen, "Vapaus, velvollisuus ja vastavuoroisuus—käsityksiä kansalaisen suhteesta valtioon ja maanpuolustukseen (vertaisarvioitu)," *Tiede ja ase* 2019, no. 1 (2019): 155–86, https://journal.fi/ta/article/view/88685.

97 Interview with Finnish government officials, May 2024, Helsinki.

98 Raitasalo, "Finnish Defense," 85.

99 Fiala, R*esistance Operating Concept*, 15, 41–43.

100 Ibid., 40.

101 Ibid., 49.

102 Binnendijk and Kepe, *Civilian-Based Resistance*, 24.

103 For a review, see Gene Sharp, *Waging Non-violent Struggle: 20th Century Practice and 21st Century Potential* (Manchester, NH: Extending Horizons Books, 2005), 51–64. See also Adam Roberts, *Civilian Resistance as a National Defense: Non-violent Action against Aggression* (Harrisburg, PA: Stackpole Books, 1967).

104 Binnendijk and Kepe, *Civilian-Based Resistance*, 19.

105 Interview with Finnish government officials, May 2024, Helsinki.

106 Fiala, *Resistance Operating Concept*, 9.

107 Interview with Finnish nongovernment experts, May 2024, Helsinki.

108 Stephen J. Flanagan et al., *Deterring Russian Aggression in the Baltic States through Resilience and Resistance* (Santa Monica, CA: RAND, 2019), 12–13.

109 Interview with Finnish government official, May 2024, Helsinki.

110 OECD, "Critical Infrastructure Resilience Case-Study."

111 Interview with Finnish government officials, May 2024, Helsinki.

112 Milne, "War with Russia?"

113 Interview with Finnish government officials, May 2024, Helsinki.

114 Ibid.

115 See Valmiuslaki, ch. 19.

116 "Deterrence and Defence," NATO, updated July 1, 2024, https://www.nato.int/cps/en/natohq/topics_133127.htm.

## CHAPTER 3: THE CHALLENGE OF RESILIENCE IN TAIWAN

1 Jian Chen, *Mao's China and the Cold War* (Chapel Hill: University of North Carolina Press, 2001), 163–204.

2 "Anti-secession Law," Embassy of the People's Republic of China in the United States, March 15, 2005, http://us.china-embassy.gov.cn/eng/zt/twwt/200503/t20050315_4912997.htm.

3 Bonny Lin et al., *Competition in the Gray Zone: Countering China's Coercion against U.S. Allies and Partners in the Indo-Pacific* (Santa Monica, CA: RAND, 2022).

4 See recent CSIS reports Bonny Lin et al., *How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios* (Washington, DC: CSIS, June 2024); and Bonny Lin et al., "How China Could Blockade Taiwan," CSIS, August 22, 2024, https://features.csis.org/chinapower/china-blockade-taiwan/.

5 For an in-depth discussion of salami slicing, see Richard W. Maass, "Salami Tactics: Faits accomplis and International Expansion in the Shadow of Major War," *Texas National Security Review* 5, no. 1 (Winter 2021–22): 33–54, https://tnsr.org/2021/11/salami-tactics-faits-accomplis-and-international-expansion-in-the-shadow-of-major-war/.

6 "Taiwan—Cybersecurity," International Trade Administration, January 10, 2024, https://www.trade.gov/country-commercial-guides/taiwan-cybersecurity.

7 Joey Chen, Ashley Shen, and Vitor Ventura, "APT41 Likely Compromised Taiwanese Government-Affiliated Research Institute with ShadowPad and Cobalt Strike," CISCO Talos Intelligence Group, August 1, 2024, https://blog.talosintelligence.com/chinese-hacking-group-apt41-compromised-taiwanese-government-affiliated-research-institute-with-shadowpad-and-cobaltstrike-2/.

8 Tai-Li Wang, "Does Fake News Matter to Election Outcomes?: The Case Study of Taiwan's 2018 Local Elections," *Asian Journal for Public Opinion Research* 8, no. 2 (May 31, 2020): 67–104, https://doi.org/10.15206/ajpor.2020.8.2.67.

9 Jude Blanchette, Scott Kennedy, Scott Livingston, and Bonnie S. Glaser, *Protecting Democracy in an Age of Disinformation: Lessons From Taiwan* (Washington, DC: CSIS, September 2024), https://www.csis.org/analysis/protecting-democracy-age-disinformation-lessons-taiwan.

10 Hsia Hsiao-hwa and Ray Chung, "Taiwan Spy Chief Warns of Sharp Rise in Chinese infiltration," Radio Free Asia, July 5, 2024, https://www.rfa.org/english/news/china/taiwan-spying-07052024135320.html.

11 Yimou Lee and David Lague, "Intrigue Island," Reuters, December 20, 2021, https://www.reuters.com/investigates/special-report/taiwan-china-espionage/.

12 Keith Bradsher, "Foxconn, Apple's Manufacturer in China, Is Said to Be under Tax Audit," *New York Times*, October 22, 2023, https://www.nytimes.com/2023/10/22/business/foxconn-china-tax-investigation.html.

13 John Dotson, "Beijing's New Plan for Fujian as a Model Zone for Economic Integration with Taiwan," Global Taiwan Institute, October 4, 2023, https://globaltaiwan.org/2023/10/beijings-new-plan-for-fujian-as-a-model-zone-for-economic-integration-with-taiwan/.

14 "Civil Defense Act," ROC (Taiwan) Ministry of Justice, updated January 20, 2021, https://

law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0080118.

15 Kathrin Hille, "Taiwan to Strengthen Civil Defence to Prepare against China Threat," *Financial Times*, July 10, 2024, https://www.ft.com/content/4c772bdb-e6e3-4272-a591-367695f1cc73.

16 ROC (Taiwan) Office of the President, "President Lai Holds Press Conference to Mark First Month in Office," press release, June 19, 2024, https://english.president.gov.tw/News/6768.

17 Chen Yun and Jason Pan, "First Whole-of-Society Meeting Held," *Taipei Times*, September 27, 2024, https://www.taipeitimes.com/News/front/archives/2024/09/27/2003824418.

18 A notable shortcoming of the legislation was that it did not cover any private sector actors.

19 "Anti-infiltration Act," ROC (Taiwan) Ministry of Justice, updated January 15, 2020, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030317.

20 "Civil Defense Act."

21 Huynh Tam Sang, Tong Thai Thien, and Le Thi Yen Nhi, "How Taiwan Fights the Disinformation War," Lowy Institute, June 20, 2024, https://www.lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war.

22 Russell Hsiao, "Taiwan's Bottom-Up Approach to Civil Defense Preparedness," Global Taiwan Institute, September 21, 2022, https://globaltaiwan.org/2022/09/taiwans-bottom-up-approach-to-civil-defense-preparedness/.

23 Calvin Chu, "Enhancing Taiwan's National Resilience," *Taipei Times*, July 26, 2024, https://www.taipeitimes.com/News/editorials/archives/2024/07/26/2003821318.

24 Hsiao, "Taiwan's Bottom-Up Approach."

25 At the time of writing, the committee had not formally met, but Taiwanese government officials stated in interviews that representatives from resilience NGOs would be included in the official committee proceedings.

26 All-Out Defense Mobilization Agency, *All-Out Defense Contingency Handbook* (Taipei: ROC [Taiwan] Ministry of National Defense, 2023), https://shorturl.at/gqA4L.

27 Yang Zhiqiang, "手冊不實用、演習變表演?" [As the manual is not practice, are exercises becoming a performance?], *The Reporter*, May 23, 2022, https://www.twreporter.org/a/national-defense-reform-civil-defense.

28 Alastair Gale, "Ukraine War Stokes Concerns in Taiwan over Its Fragile Internet Links," *Wall Street Journal*, April 18, 2022, https://www.wsj.com/articles/ukraine-war-stokes-concerns-in-taiwan-over-its-fragile-internet-links-11650285592.

29 ROC (Taiwan) Office of the President, "President Tsai Announces Military Force Realignment Plan," press release, December 27, 2022, https://english.president.gov.tw/NEWS/6417.

30 Michael Laris, "Chinese Web Warriors," *Washington Post*, September 11, 1999, https://www.washingtonpost.com/archive/politics/1999/09/11/chinese-web-warriors/bf004cfe-1e46-4013-a3f7-3b4dacf805e6/.

31 U.S.-China Economic and Security Review Commission, "Section 2: China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States," in *2022 Report to Congress* (Washington, DC: USCC, November 2022), 418–519, https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf.

32 "History," Administration for Cyber Security, updated September 3, 2022, https://moda.gov.tw/en/ACS/aboutus/history/608.

33 "MODA Minister Huang Unveils Digital Development Strategy," *Taiwan Today*, May 29, 2024, https://taiwanreview.nat.gov.tw/news.php?unit=10&post=253361&unitname=Society-Top-News&postname=MODA-Minister-Huang-unveils-digital-development-strategy.

34 Executive Yuan Department of Information Services, "Taiwan-US Joint Cyber Security Offensive and Defensive Exercise—First of Its Kind in International Collaboration on Cyber Security," press release, November 6, 2019, https://www.nchc.org.tw/Message/MessageView/3361?mid=92&page=1.

35 "Overview of Taiwan's Energy Supply," Taiwan Ministry of Economic Affairs, https://www.moeaea.gov.tw/ECW/populace/content/Content.aspx?menu_id=14435.

36 Angelica Oungon, "Fixing Taiwan's Grid Issues Requires Redistribution," Taiwan Business Topics, May 11, 2022, https://topics.amcham.com.tw/2022/05/fixing-taiwans-grid-issues-requires-redistribution/.

37 Ibid.

38 Meaghan Tobin and John Liu, "Why Taiwan Is Building a Satellite Network without Elon Musk," *New York Times*, updated March 15, 2024, https://www.nytimes.com/2024/03/14/business/taiwan-starlink-satellite.html.

39 "How China Could Choke Taiwan," *New York Times*, August 25, 2022, https://www.nytimes.com/interactive/2022/08/25/world/asia/china-taiwan-conflict-blockade.html.

40 Michael Nakhiengchanh, "Over 100 telecom base stations in Taiwan disrupted by quake," Taiwan News, April 3, 2024, https://www.taiwannews.com.tw/news/5135822.

41 Sarah Wu and Yimou Lee, "Fear of the Dark: Taiwan Sees Wartime Frailty in Communication Links with World," Reuters, March 15, 2023, https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/.

42 "DDoS Threat Report for 2023 Q4," *Cloudflare Blog*, September 1, 2024, https://blog.cloudflare.com/ddos-threat-report-2023-q4/.

43 "Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods," Microsoft Security Insider, April 4, 2024, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/east-asia-threat-actors-employ-unique-methods.

44 Filip Truță, "TSMC Refuses to Pay $70 Million Ransom after Lockbit Falsely Claims Its Affiliates Hacked the Giant Chipmaker," Bitdefender, July 3, 2023, https://www.bitdefender.com/blog/hotforsecurity/tsmc-refuses-to-pay-70-million-ransom-after-lockbit-falsely-claims-its-affiliates-hacked-the-giant-chipmaker.

45 Helen Davidson, "Taiwan Tells Elon Musk It Is 'Not for Sale' after Latest China Comments," *The Guardian*, September 14, 2023, https://www.theguardian.com/world/2023/sep/14/taiwan-elon-musk-china-comments-response-all-in-summit-los-angeles.

46 "Enhancing the Resilience of Communications Network," ROC (Taiwan) Ministry of Digital Affairs, updated March 15, 2024, https://moda.gov.tw/en/digital-affairs/communications-cyber-resilience/operations/310.

47 "About," National Institute of Cyber Security, https://www.nics.nat.gov.tw/en/about/introduction/.

48 Staff Writer, "TTC to Bolster Internet Against Disaster and War," *Taipei Times*, July 9, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/07/09/2003802925.

49 "Program for the Digital Resilience Validation of Emerging Technologies for Contingency or Wartime Applications," ROC (Taiwan) Ministry of Digital Affairs, updated March 27, 2024, https://moda.gov.tw/en/digital-affairs/communications-cyber-resilience/programs/4187.

50 ROC (Taiwan) Ministry of Digital Affairs, "Moda Has Officially Launched the Middle Orbit Satellite Signal for Taiping Island, Increasing Communication Efficiency by 3.9 Times," ROC (Taiwan) Overseas Community Affairs Council, April 24, 2024, https://ocacnews.net/article/367262.

51 Staff Writer, "Taiwan Teams up With SES to Boost Digital Resilience," *Taipei Times*, August

4, 2023, https://www.taipeitimes.com/News/front/archives/2023/08/04/2003804212.

52 Gustavo F. Ferreira and Jamie A. Critelli, "Taiwan's Food Resiliency—or Not—in a Conflict with China," *Parameters* 53, no. 2 (Summer 2023), https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3222&context=parameters.

53 Oscar Lin, *Taiwan Food Security Situation Overview* (Washington, DC: USDA, June 19, 2024), https://agriexchange.apeda.gov.in/marketreport/Reports/Taiwan%20Food%20Security%20Situation%20Overview_Taipei_Taiwan_TW2024-0030.pdf.

54 "Taiwan taking monthly energy, food inventories in case of China conflict," Reuters, October 5, 2022, https://www.reuters.com/world/asia-pacific/taiwan-taking-monthly-energy-food-inventories-case-china-conflict-2022-10-05/.

55 Lawrence Chung, "Taiwan Is Stockpiling Supplies to Prepare for Blockade or Attack, Official Says," *South China Morning Post*, October 5, 2022, https://www.scmp.com/news/china/politics/article/3194938/taiwan-stockpiling-supplies-prepare-blockade-or-attack-official.

56 Troy Lai and Lucas Blaustein, *Taiwan Confident in Food Stocks as COVID-19 Disrupts International Trade* (Washington, DC: USDA, April 13, 2020), https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=Taiwan%20Confident%20in%20Food%20Stocks%20as%20COVID-19%20Disrupts%20International%20Trade_Taipei_Taiwan_04-05-2020.

57 "Taiwan's Dominance of the Chip Industry Makes It More Important," *The Economist*, March 6, 2023, https://www.economist.com/special-report/2023/03/06/taiwans-dominance-of-the-chip-industry-makes-it-more-important.

58 Liliana Narvaez, Sally Janzen, Caitlyn Eberle, and Zita Sebesvari, *Taiwan Drought* (Bonn: United Nations University–Institute for Environment and Human Security, August 2022), https://doi.org/10.53324/UJZW5639.

59 "Lai Committee Aims to Enhance Civilian Component of Emergency Response," Focus Taiwan, September 26, 2024, https://focustaiwan.tw/politics/202409260019.

60 Connable et al., *Will to Fight*, 2.

61 Lin Chia-nan, "Poll says 72.5% of Taiwanese willing to fight against forced unification by China," *Taipei Times*, December 30, 2021, https://www.taipeitimes.com/News/front/archives/2021/12/30/2003770419; and Russel Hsiao, "New Opinion Polls Highlight Trends in Taiwan's Will to Fight and Its Partisan Divide," Global Times Institute, January 12, 2022, https://globaltaiwan.org/2022/01/new-opinion-polls-highlight-trends-in-taiwans-will-to-fight-and-its-partisan-divide.

62 "How does the Taiwan Public View the U.S. and China?" CSIS public event, July 18, 2024, https://www.csis.org/events/how-does-taiwan-public-view-us-and-china.

63 Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan* (Washington, DC: CSIS, January 2023), https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.

64 "The Most Dangerous Place on Earth," *The Economist*, May 1, 2021, https://www.economist.com/leaders/2021/05/01/the-most-dangerous-place-on-earth.

65 "News," GCTF, https://www.gctf.tw/en/news.htm.

66 "Technology, Trade and Investment Collaboration," American Institute in Taiwan, https://www.ait.org.tw/technology-trade-and-investment-collaboration/.

67 "Taiwan, Czechia Sign MOU on Ukraine Health Care Reconstruction Assistance," *Taiwan Today*, December 4, 2023, https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=245521.

68 "Interview with BNS," ROC (Taiwan) Ministry of Digital Affairs, updated January 25, 2023, https://moda.gov.tw/en/press/background-information/3637.

## CHAPTER 4: STRENGTHENING RESILIENCE BEYOND MILITARY AID

1 Margaret Simons, "Taiwanese Flock to Civil Defense Training Ahead of Potential Chinese Invasion," *Foreign Policy*, December 19, 2022, https://foreignpolicy.com/2022/12/19/taiwan-china-invasion-civil-defense-training/.

2 Chen Ping-hei, "Taipower Upgrades Pay Off in Earthquake," *Taipei Times*, April 7, 2024, https://www.taipeitimes.com/News/editorials/archives/2024/04/07/2003816049.

3 Adam Zewe, "From Seawater to Drinking Water, with the Push of a Button," MIT News, April 28, 2022, https://news.mit.edu/2022/portable-desalination-drinking-water-0428.

4 Lin, Taiwan Food Security; and "Taiwan, US Sign Food Security Pact," *Taiwan Today*, June 5, 2024, https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=253723.

5 Select Committee on the Chinese Communist Party, *Ten for Taiwan: Policy Recommendations to Preserve Peace and Stability in the Taiwan Strait* (Washington, DC: Select Committee on the Chinese Communist Party, May 2023), 14, https://selectcommitteeontheccp.house.gov/media/policy-recommendations/ten-taiwan-policy-recommendations-preserve-peace-and-stability-taiwan.

6 Dowd and Cook, *Bolstering Collective Resilience in Europe*, 5.

## APPENDIX A

1 "Comprehensive Security," Finnish Ministry of Defence Security Committee, https://turvallisuuskomitea.fi/en/comprehensive-security/.

## APPENDIX B

1 "The Security Strategy for Society," Finnish Ministry of Defence Security Committee, 2017, https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

**COVER PHOTO** SAM YEH VIA AFP/GETTY IMAGES

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | **www.rowman.com**

ISBN 978-1-5381-7090-8

9781538170908 90000