

Preparedness Wargaming for Critical Infrastructure Resilience: Taiwan Digital Blockade Wargame

Jason Vogt*, Nina Kollars, Michael Poznansky

US Naval War College, Newport, RI, USA

For any developed country, the stable conduct of life for citizens, economies, and militaries—and the capacity to govern—depends on regular access to data and communications. This reliance makes communications and data flows a strategic target, not only for criminals but also for adversaries seeking geopolitical advantage. Defending against such threats is difficult because communication infrastructures are complex, interdependent systems with no single point of control. Addressing this challenge requires militaries, governments, and the private sector to coordinate and plan for attacks and conflict in the cyber domain. This article presents the Taiwan Digital Blockade Wargame, a scenario-based exercise designed to explore ways to improve the resilience of Taiwan’s information and communications technology (ICT) infrastructure in the event of a conflict with the People’s Republic of China (PRC). The wargame intends to identify overlapping opportunities that militaries, industry, and policymakers could jointly implement to enhance cyber defense and societal resilience during conflict. Methodologically, the paper contributes to the emerging practice of “preparedness wargaming,” a form of critical infrastructure game that moves beyond diagnosing weaknesses to generating actionable solutions for resilience and defense. By framing wargaming as a generative research method, we show how structured gameplay and facilitated dialogue can surface novel, cross-sectoral strategies not apparent to any single actor. The article reports on the game design, process, and key recommendations, and argues that such generative wargames offer a promising tool for anticipating and mitigating complex, interdependent cyber disruptions in an era of increasing geopolitical tension.

Keywords: Taiwan, cybersecurity, People’s Republic of China, cyber defense strategy, wargaming, cyber resilience

* Corresponding author: jason.vogt@usnwc.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof. 2025. This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.*

INTRODUCTION

In the event of a conflict between the People’s Republic of China (PRC) and Taiwan, it is reasonable to expect that Taiwan’s information and communications technology (ICT) infrastructure would experience severe disruptions. These disruptions could significantly limit Taiwan’s ability to communicate internally with its population and externally with the international community. The Department of War (DoW) needs to better understand the critical vulnerabilities of Taiwan’s ICT infrastructure, along with the key capabilities and technologies that could be used to mitigate threats and restore functionality during conflict. A gap exists in our knowledge about how to enhance defense and resilience, whether through policy or technology.

This problem is not unique to Taiwan. Data and internet access are integral to any developed society. Yet the landscape of stakeholders, managers, and maintainers of what constitutes data and internet connectivity for nations is by no means simple. Complex interdependencies leave nations vulnerable to disruption across all aspects of national security, affecting citizens’ daily lives, economic stability, military coordination, and even the ability to govern effectively (Jansen et al. 2023). Effective defense therefore requires militaries, national governments, and the private sector to coordinate and plan jointly for attacks on the internet and its enabling infrastructures. In prior work, we offered early theoretical insights into the concept of “digital denial”, which we define as an adversary’s actions to isolate a population from connectivity to data and communications for operational or strategic gain. In that study, we examined lessons on cyber resilience drawn from Ukraine’s efforts to maintain communications amid the 2022 Russian invasion (Vogt, Kollars, and Poznansky 2024). However, the value of the so-called “Zelensky Playbook” did not translate well to Taiwan’s vastly different communications architecture and geopolitical situation.

As we concluded that Taiwan was much more vulnerable to digital denial operations, we turned to wargaming to better understand what could be done to better prepare Taiwan for potential conflict with China. Why a wargame? Wargamers widely agree that wargames are useful tools for exploring and understanding complex decisions in complex environments (Haggman 2019). The wargaming community of practice designs games for multiple purposes but often distinguishes between experiential/educational and analytical approaches—though this division is contested, with many authors arguing that both objectives can coexist within a single game construct (Elg 2018). Since our goal was to generate forward-looking solutions, we turned to critical infrastructure games, a growing subset of wargames focused on problems related to critical infrastructure defense (Badea et al. 2018). We refer to these types of games as “preparedness wargaming”. Typically, preparedness games are focused on improving internal coordination and response processes, which can strengthen the cyber-defense posture of governments or private entities.

The difference between these types of games and our own lies in purpose. In most cases, critical infrastructure games aim to expose where stakeholders fall short of established standard. Cyberattack games serve a diagnostic function, identifying weak or incomplete security practices that already exist. For the Taiwan Digital Blockade Wargame, we modified this model by shifting the focus from diagnosing internal defense processes to generating investment solutions.

The purpose of this article is twofold. First, it provides an overview of the Taiwan Digital Blockade wargame and the recommendations it produced, with the aim of informing policy-makers, cyber defenders, and other stakeholders preparing for potential conflict. Second, it offers a contribution to the scholarly understanding of wargaming by demonstrating how such exercises can function as generative tools—capable of eliciting insights from participants beyond the typical stakeholder set. While traditional wargames often include outside experts to inspire new ideas, it is uncommon for this generative intent to serve as the primary driver of game design.

BACKGROUND

Game Setting: The Complexity of the Problem

Taiwan is one of the most digitally connected countries in Asia, with more than 90% of its population online (CIA World Fact Book 2025). This access is underpinned by a robust ICT infrastructure supported by multiple on-island telecommunications providers, an international network of undersea communications cables, and Taiwan's power industry, which is modernizing parts of its legacy energy grid with renewable and smart micro-grid technologies. Taiwan's government actively promotes these efforts through the Ministry of Digital Affairs (MODA), which is responsible for communications and cybersecurity policy, and the Ministry of Economic Affairs Energy Administration. However, ongoing disagreements between the ruling Democratic Progressive Party (DPP) and the Kuomintang (KMT)-controlled legislature on funding threaten the viability of several government-funded resilience programs.

Taiwan's domestic ICT infrastructure is supported by three major on-island telecoms providers offering mobile and fiber access (TaiwaneSim 2025). Chunghwa Telecom, the largest provider, manages several on-island data centers that support both government communications and digital civilian economy. Taiwan remains at the forefront of mobile technology deployment. Chunghwa Telcom has partnered with several multinational corporations to establish a Centralized Radio Access Network (C-RAN) architecture that enables 5G services for private users and businesses. Unlike legacy mobile networks that depend on robust base-station infrastructure, C-RAN consolidates data processing through centralized towers and facilities, improving efficiency and reducing energy costs (Ericsson 2025). These systems are underpinned by a dense network of fiber-optic cabling. Reducing energy consumption is a

major driver of Taiwan's ICT modernization, as the island's legacy energy infrastructure has struggled to meet the nation's growing power demands.

Taiwan currently relies on fifteen undersea fiber-optic cables to connect to the global internet (Mok and Huang 2024). These cables have been inadvertently or deliberately severed at least 27 times, demonstrating their vulnerability during conflict (Wu and Lai 2023). Several cables route directly through China, increasing exposure to exploitation (TeleGeography 2025). Learning from the war in Ukraine, Taiwan's leaders recognize the need to harden the island's digital infrastructure and have launched initiatives to defend against communications isolation. Taiwan's largest telecom company has signed an agreement with EutelSat OneWeb, which operates a satellite constellation similar to Starlink, to make its mobile network more resilient (EUTELSAT/ONEWEB 2025). These satellite systems are being integrated into current and planned communications architecture to help maintain connectivity to the global internet. Although they have proven resilient to signal jamming (i.e. intentional interference designed to block or degrade wireless communications), they provide only a fraction of the bandwidth available through undersea cables.

Established in 2022, the Ministry of Digital Affairs oversees national communications and cybersecurity policy. It promotes Taiwan's digital development, enhances government efficiency, develops plans for communications resilience and improves Taiwan's cybersecurity posture. In response to repeated undersea cable-cutting incidents, MODA approved the expansion of microwave relays to connect islands isolated by cable disruption (MODA 2025b). The Ministry also developed and tested a high-altitude communications balloon for use in emergency situations (MODA 2025c). MODA has also sought to improve the nation's cybersecurity posture, reduce online fraud and counter PRC disinformation campaigns (MODA 2025a).

Power generation and distribution are managed by the Taiwan Power Company (Taipower), under the Ministry of Economic Affairs' Energy Administration. Roughly 80% of Taiwan's power comes from coal, oil, and liquified natural gas, nearly all imported via maritime routes, leaving supply chains vulnerable to disruption (International Energy Agency 2025). Major power outages have occurred regularly over the past decade, with some blackouts affecting over five million customers, approximately one-quarter of the population (BBC 2025). These outages have had serious implications for Taiwan's industries, especially the power-intensive semiconductor sector, which has lost hundreds of millions of dollars due to power outages. To address these challenges, Taipower and government authorities plan to invest \$29 billion in smart-grid and renewable energy infrastructure upgrades by 2030 (U.S. Department of State 2025). These efforts are focused on solar and wind generation and are supported by major investments in smart-meters and on-island cloud infrastructure.

Taiwan's political landscape is dominated by the Democratic Progressive Party (DPP) and the Kuomintang (KMT), which have alternated control of the national government over the

last 25 years, leading to substantial shifts in security and defense policies towards the PRC. As of early 2025, the DPP controlled the executive branch, while the legislature was led by a KMT led coalition with the Taiwan People's Party (TPP) (The Economist 2025). To curb DPP initiatives, the KMT and TPP have sought to cut funding to government agencies, including MODA, by more than 40% (Hioe 2025). Consequently, Taiwan's communication- resilience programs face reduced budgets and delays in implementing already-funded equipment.

Despite these challenges, Taiwan is maintaining its efforts to prepare its civilian population for potential conflict. In 2024, Taiwan established a Whole-of-Society Defense Resilience Committee to strengthen civilian defense capacity in several areas, including critical infrastructure protection (Kepe and Harold 2025). The updated National Cybersecurity Strategy acknowledges that government resources alone will likely be insufficient during crisis and seeks to augment that capacity with civilian expertise. It calls for expanding domestic technology and cybersecurity industries to cultivate skilled professionals on-island who could serve in a cyber-reserve force (Waligora 2025). A more mature and diverse tech sector is viewed as an enabler to strengthen digital resilience across society.

Although the Taiwan Digital Blockade Wargame did not explicitly examine the implications of Taiwan's current political dynamics, it remains critical for U.S. policymakers to understand that Taiwan's government and population are not unified in their approach to the PRC. This means that funding for security initiatives is potentially prone to volatility, which may necessitate future shifts in infrastructure investment priorities and strategies over the coming years. External funding sources, therefore, may provide the stability required to enhance Taiwan's ICT infrastructure resilience.

Wargaming to Generate New Solutions

Wargames have long been used by the military to train officers, evaluate war plans and examine new operational approaches (Curry 2012). According to wargaming expert Peter Perla, a wargame is defined as a "model involving people making decisions in a synthetic environment of competition or conflict, in which they see the effects of their decisions on that environment and then get to react to those changes" (Perla 2022, 200). Although wargames include inputs from operations research and other quantitative methods, it is the focus on human decision-making and their ability to provide an immersive experience, which make them distinct from other forms of analysis.

Over the past decades, wargames have been adapted to simulate organizational responses to real-world problems, including cyber-attacks, natural disasters and public health emergencies. These "preparedness" games frequently bring together stakeholders across government and industry to test strategies and coordination mechanics, while simultaneously building trust among the people and organizations that must work together to effectively respond to a crisis (Fedina and Lucas 2025). For example, the North American Electric Reliability

Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC) developed a wargame called *GRIDEX*, which enables utility providers and government agencies to practice their response and recovery actions in response to cyberattacks (Duncan 2023). There are numerous examples, but a key feature of these preparedness games is that they are typically focused on internal stakeholders and organizational processes required to respond to incidents.

As the threats to Taiwan have intensified in recent years, researchers have increasingly used wargames to help them understand different aspects of the conflict. Researchers at the Center for Strategic and International Studies have conducted two wargames examining Taiwan, one of which is focused on military responses to a major attack and another which examines economic factors that would likely result from a prolonged blockade of key resources, which can affect electrical power and other infrastructure (Cancian, Cancian, and Heginbotham 2023, 2025). Earlier this year, researchers at Syracuse placed players in the role of the PRC's government and military to study whether the role reversal would generate valuable insights for U.S. planning (Michaels and Williams 2025).

The difference between conventional, cyber and critical infrastructure games lies in purpose. In most cases, critical infrastructure games aim to expose where stakeholders fall short of established standard. Cyberattack games serve a diagnostic function, identifying weak or incomplete security practices that already exist. More conventional wargames look for opportunities or weaknesses in military approaches to a problem. For the Taiwan Digital Blockade Wargame, we used a blended approach to the scenario, which included elements of conventional warfare, cyberattacks, electromagnetic warfare and covert sabotage of critical infrastructure. Instead of focusing on internal defense processes, we used the game to generate investment solutions.

The practical value of wargaming as a mechanism to interrogate complex contexts and discover potential solutions is well-established (Hirst 2020). Wargaming as a solution generation tool is not unique, but it is seldom explicitly articulated as such in the literature. As in much of the wargaming community, the generative function tends to be embedded in tacitly applied techniques¹. In this sense, playing the game allows players (while they may also be learning) and facilitators (while they may be collecting data for sentiment analysis) to move through an abstraction of reality that stimulates the creation of solutions not previously known to any individual party prior to game play. In so doing, wargames can produce new insights and strategies that provide clarity under conditions of complexity and uncertainty (Perla 2022).

1. While we do not elaborate here on the structure and function of communities of practice (COPs), there is a robust literature on the nature of practice and the knowledge they produce. See for example: (Wenger-Trayner and Wenger-Trayner 2015)

TAIWAN DIGITAL BLOCKADE WARGAME: GAME DESIGN, SCENARIO AND PLAY

The Taiwan Digital Blockade Wargame's overarching objective is to improve the defense of Taiwan's critical infrastructure, by bringing in outside perspectives who could potentially help generate novel solutions to the problems facing Taiwan. This section provides an overview of the game design. Further details are available in the full game report (Vogt and Kollars 2024).

Participants

In August 2024, we organized game sessions at DEFCON (<https://defcon.org>) and Blackhat (www.blackhat.com), two of world's largest multi-day cybersecurity conventions, which took place in Las Vegas, Nevada (USA). We recruited 27 players with backgrounds in cybersecurity, industrial control systems, data center operations, threat intelligence, subsea cabling systems and other areas. Players were identified and selected in the months preceding the game via outreach through trusted networks and some social media outreach. Players were invited to apply for a slot in the game, and the research team selected the participants based on their technical skill set. Two teams of players were selected and notified prior to the event.

The first iteration of the game was executed in a private conference suite during Blackhat and included 12 players, whereas the second was executed on the open DEFCON conference floor and involved 15 players. Each session lasted about 3 hours in total. In each game, players were placed on three teams, with the goal of having a mix of skills and backgrounds on each team. For example, there were many players with backgrounds in cyber threat intelligence, but fewer with direct experience with Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, so the game team ensured that at least one person with that expertise was assigned to each team.

Game Overview

The game placed players into the role of advisors to the government of Taiwan. Players were divided into advisory councils and presented with two conflict vignettes depicting a PRC invasion of Taiwan in 2030. In the first vignette, the PRC refrained from conventional military attacks, relying instead on cyber operations, electronic warfare, and sabotage to disrupt civilian communications and power infrastructure. In the second vignette, the PRC launched a full-scale kinetic attack, including against critical infrastructure. The PRC's overarching goal in both cases was to isolate the Taiwanese government in Taipei from its domestic population and the international community.

At the start of each round, advisory councils were briefed on the degraded state of Taiwan's infrastructure. Teams then discussed what investments Taiwan should make in the coming

years to mitigate the damage anticipated in 2030. Players then voted for the team whose recommendations they believe were most effective.

Players' recommendations were categorized into three investment domains: infrastructure, cybersecurity, and recovery. Infrastructure investments referred to the purchase of physical equipment that forms part of the ICT or energy infrastructure. Cybersecurity investments encompassed software-based solutions or industry best practices aimed at enhancing cyber resilience. Recovery investments focused on post-attack measures to restore damaged or inoperable infrastructure. Players were not provided with budgetary constraints and were encouraged to propose ideas freely.

Game Schedule

The full game session, including the introduction and two gameplay moves, lasted approximately three hours (Table 1).

Table 1. Overview of Game Activities and Scenario Play Structure

Activity	Duration	Description
Introduction	30 min	Players were divided into advisory councils (teams). The game team and participants introduced themselves, highlighting their expertise. A briefing followed, outlining the game's purpose, Taiwan's ICT and power context, gameplay mechanics, desired outcomes, and logistics. Players had time for questions before starting.
Move 1 – Scenario Play	1 h 15 min	<p>The first vignette was presented, describing the initial phase of conflict. The move was structured as follows:</p> <ul style="list-style-type: none"> • Red Action (10 min): Facilitators presented hostile actions and situational changes. • Team Planning (30 min): Teams discussed mitigation and investment options in infrastructure, cybersecurity, and recovery. • Team Presentations – Infrastructure (10 min) followed by Voting (5 min). • Team Presentations – Cybersecurity (10 min) followed by Voting (5 min). • Team Presentations – Recovery (10 min) followed by Voting (5 min). <p>Facilitators recorded discussion points and outcomes.</p>
Move 2 – Scenario Play	1 h 15 min	The second vignette introduced a full-scale kinetic attack. The same cycle was followed: brief overview (<i>Red Action</i> , 10 min), 30 min team planning, presentations of recommendations across the three investment categories (10 min each), and individual voting after each round (5 min each).

Scenario Overview

The scenario presented to players was set on August 6, 2030. Relations between the PRC and Taiwan had deteriorated to the breaking point due to the re-election of a liberal, pro-independence party. Rhetoric towards independence was at an all-time high, and several government representatives had openly called for UN recognition of Taiwan as an independent state. The Central Committee of the Communist Party (CCCP) deemed the risk of Taiwan declaring independence high enough to warrant military intervention and began preparations for invasion.

With little chance of surprise, the PRC sought to disrupt Taiwan's military and civilian communications prior to the assault. To avoid a direct intervention by the U.S., the PRC initially decided to limit kinetic attacks on the island prior to the launching of amphibious forces. However, they were willing to conduct operations using cyber, electronic warfare and clandestine sabotage prior to the invasion. The Taiwanese government, aware of the impending attack, had decided to prioritize maintaining government and civilian communications at peak levels to enable military coordination with allies and show resolve in the face of PRC aggression.

Vignette 1: Non-Kinetic Attacks. The first vignette presented to players depicted a non-kinetic campaign preceding conventional military strikes on the island. To justify their actions with the goal of disrupting civilian infrastructure to support the war effort, PRC accused Taiwan of illegally using high bandwidth communications to import and export proprietary (Chinese) materials. Multiple submarine fiber-optic cables connecting Taiwan to the global internet were physically severed; while cyberattacks targeted cable landing stations, further disrupting the flow of international internet traffic to the island. The remaining undersea cables running directly to the PRC mainland remained operational but were monitored by PRC authorities.

In this scenario, the PRC also employed airborne electronic warfare platforms to disrupt GPS signals and commercial satellite ground stations integrated with civilian ICT infrastructure. These disruptions were described as episodic, varying according to platform location. Additionally, data centers hosting email servers for several major internet providers were targeted with ransomware. While commercial mobile networks remained largely functional, service degradation occurred in areas suffering electrical power outages.

For each game, players were briefed on the first vignette and shown a map of degraded ICT infrastructure across Taiwan. Teams then discussed mitigation strategies. Once discussions were complete, each team presented their recommendations to the other teams and voted. The winning teams often proposed lower cost, easily distributed systems that could be rapidly deployed across multiple regions.

Vignette 2: Kinetic Attacks. The second vignette presented to players simulated the opening phase of a conventional attack on Taiwan's infrastructure prior to the invasion. The PRC conducted missile strikes to suppress Taiwan's air power, close airfields, and ensure that no aircraft could operate within Taiwanese airspace. Missile strikes also targeted Taiwan's power transmission infrastructure but spared power production facilities. Taiwan's national command-and-control systems and data centers, including associated power systems, were hit directly.

Data centers supporting microgrid electrical power distribution were infected with malware that encrypted data related to customer smart-meter identification and usage. Engineering

workstations managing industrial control systems responsible for microgrid operations lost visibility of routers and sensors monitoring power fluctuations. As a safety measure, all renewable power generation systems connected to microgrids were shut down, reducing Taiwan's energy capacity by 20%. Power outages rippled across manufacturing sectors, forcing most semiconductor manufacturing facilities offline. Malicious cyber actors also targeted security and traffic control systems taking some offline and causing malfunction in others, which led to confusion and traffic jams in several urban areas. Meanwhile, PRC forces also engaged in jamming all remaining microwave and satellite backbone.

Despite the escalation to large-scale conventional attacks in the second vignette, most teams did not fundamentally alter their strategies or recommendations. Stockpiling communications equipment and spare electrical-grid components have utility across multiple scenarios, including those unrelated to inter-state conflict, such as earthquakes or other natural disasters. This dual-use framing suggests a politically viable pathway for governments to justify certain expenditures as part of general disaster preparedness rather than explicit war planning.

WARGAME OUTCOMES: PLAYER-DERIVED SOLUTIONS FOR CRITICAL INFRASTRUCTURE RESILIENCE

Overview of Player Recommendations

Across the two wargames, players generated 65 recommendations aimed at improving Taiwan's critical infrastructure resilience. Approximately 70% focused on infrastructure investments, including communications systems, power generation and storage, and data backup and distribution capabilities. Another 20% of recommendations addressed recovery, emphasizing the stockpiling of critical spare parts and the development of technical skills among civilians. The remaining 10% centered on cybersecurity, primarily through cryptography and related methods to enhance communications security.

Players were not provided with budgetary constraints and were instructed not to constrain their recommendations based on finances.

In post-game analysis, all recommendations were evaluated and categorized by estimated cost (high, moderate, low) and implementation timeline (short-term, 1-2 years; medium-term, 2-4 years; long-term, 4+ years). Taken individually, two-thirds of the recommendations were judged to be low- to moderate cost and executable within one to four years—feasible under a 2030 conflict scenario. The remaining third were deemed high-cost, long-term or both, making it unlikely they would be available in a 2030 invasion scenario. Included in the high-cost group were several recommendations related to the use of modular nuclear reactors, which were also deemed to be politically unfeasible at this time. These high-cost/long-term recommendations were excluded from subsequent analysis due to limited practicality.

Thematic Areas of Recommendation

Communications infrastructure and cybersecurity. Recommendations related to communications infrastructure and cybersecurity were generally the least expensive and had the shortest implementation timelines. Many involved adapting or expanding existing technologies, including HAM radios, microwave relays, P-LEO satellite communications, long-range radio mesh networks, and drone- or balloon-based relays to maintain connectivity during disruption. Players also generated several novel concepts for enabling communications, such as using Bluetooth-based secure messaging services that function without mobile towers and implementing cryptographic protocols—including blockchain techniques—to verify message authenticity and ensure communications originated from trusted sources.

Power generation, data storage, and recovery. Recommendations involving power generation and storage, data backup and distribution, and stockpiling critical spares were judged to be more costly and potentially more difficult to implement. Players called for the expanded use of renewable power generation (wind, solar, and hydro), the establishment of distributed containerized data centers to provide reliable data backups, and options for stockpiling critical spares for power generation and network operations. The costs associated with stockpiling critical spares could vary greatly depending on type, quantity and means of storage implemented.

Civilian preparedness and skills development. Preparing the civilian population for conflict was another area discussed extensively by the participants. The amount of training and resources dedicated to these efforts could range from basic cybersecurity training programs to the creation of an elite civilian cyber corps. The costs could vary significantly depending on scale, scope, and depth of programs implemented.

EMERGENT STRATEGIC APPROACHES

Three overarching strategic approaches to enhancing Taiwan's ICT resilience strategies emerged during gameplay (Table 2):

- (1) **the decentralized strategy** would distribute lower cost assets across the population centers, saturating the environment and complicating the PRC's ability to target critical nodes
- (2) **the centralized strategy** would concentrate critical infrastructure near targets the PRC is unwilling to strike
- (3) **the interior strategy** would focus on building infrastructure and stockpiling critical spares in mountainous areas and the eastern side of the island to enable communications during a protracted conflict.

Each strategy requires prioritizing different types of investments to achieve optimal results.

Table 2. Strategic Approaches: Technologies, Benefits, and Drawbacks

Strategic Approach	Critical Technologies	Benefits	Drawbacks
Decentralized - distribute infrastructure throughout neighborhoods and towns	Solar power, P-LEO SATCOM, HAM, LoRa, distributed data, battery and repair parts	Maximizes civilian connectivity and self-sufficiency	High cost; requires civilian training and willingness to fight
Centralized - concentrate infrastructure around key manufacturing sites	Larger scale wind/solar power plants paired with data centers, large-scale battery back-ups	Requires smaller workforce to operate or maintain	Limited number of locations, population must relocate to sites
Interior - stockpile equipment in mountainous regions and the Eastern side	Solar power, microwave relays, ariel comms balloons/drones, P-LEO SATCOM, HAM, LoRa	Maximizes protection from attacks	Requires the infrastructure to be operated in difficult terrain

Decentralized Systems: Too Many Targets

A decentralized strategy favors the distribution of infrastructure to avoid the pitfalls of concentrating too many critical assets in one location. This approach can rely on many types of technologies, including many low-cost off-the-shelf technologies such as HAM radios and Long Range Radio Access (LoRa) systems. These solutions were among the most frequently suggested by players and most favorably received during voting sessions.

To be successful, the government would need to prioritize solar power generation, which can be widely dispersed, and connect it to existing mobile infrastructure. This would enable communications if large power stations and transformers go offline. The mobile infrastructure would also need to be locally connected to P-LEO satellite base stations to enable off-island internet communications. Low-cost communications devices, such as HAM and LoRa radio systems, could serve as backups if mobile infrastructure is rendered inoperable.

The government would need to invest significant time and resources to train civilians to operate and repair these systems, as well as stockpiling batteries, repair parts and replacement systems throughout the country. Well-executed, a decentralized strategy could maximize the number of civilians able to maintain communications during conflict.

High cost and the willingness of the population to participate in a decentralized strategy are the primary barriers to its execution. The government could potentially incentivize the expanded use of solar power through subsidies, but it is likely that much of the equipment would need to be purchased and distributed with government funds. Training the population would also require significant resources, without which much of the equipment would be useless. Taiwan’s military or government could establish civilian training programs or even establish a civilian cyber corps to help operate the systems, but unless participation was made compulsory there is a risk that the numbers that receive training would be insufficient.

Centralized Systems: Targeting May Be Unappealing to Adversaries

A centralized strategy assumes that the PRC may be reluctant to target key manufacturing sites and certain cultural artifacts, creating safe zones where civilian power and communications infrastructure could be concentrated. The sites identified by the players included areas dedicated to the production of semiconductors, along with museums and institutions housing important Chinese cultural artifacts. The idea builds on the “silicon shield” concept, which suggests that China would avoid destroying or disrupting industries vital to its own economy, such as semiconductor imports, which could entice a response from the U.S. who is also dependent on them (Institute for Security and Development Policy 2025). In this case, China is still willing to invade Taiwan, but would be unwilling to target key manufacturing areas with conventional attacks, thereby limiting damage to critical infrastructure located in these areas. Players advocating for this strategy recommended building up renewable power infrastructure, data centers, and communications nodes within these zones. This would create safe zones where civilian refugees could maintain communication and shelter during conflict.

A centralized strategy has several advantages, not least the fact that Taiwan’s government is already prioritizing renewable power investments, particularly wind and solar projects located near key manufacturing sites. This approach aligns well with existing national energy initiatives and could be further strengthened by integrating data centers into these zones, along with the capability to connect to one or more P-LEO satellite constellations. Such an integration would allow segments of the population to maintain communications with the outside world at a relatively low cost. Because the number of locations would be limited, the infrastructure could be managed by the government or trained private-sector professionals, reducing the need for large-scale civilian training.

The drawbacks of a centralized strategy include the restricted number of sites available, meaning that large portions of the population are unlikely to benefit from their existence. Located primarily along urban coastal areas, these sites would also remain especially vulnerable to electronic warfare, potentially leading to temporary disruptions to services. Moreover, because these locations are already deemed to be of high value to the PRC, the development of additional infrastructure could incentivize the PRC to seize these areas earlier in the conflict than it would otherwise. Lastly, in the event of a protracted conflict, there is no guarantee the PRC will limit its conventional strikes on these areas, particularly if it decides to prioritize the destruction of civilian infrastructure as a key objective of its military campaign.

Interior Shelters: Using Geography as a Strength

The interior strategy leverages Taiwan’s geography by positioning power and communications infrastructure within its mountainous eastern regions, away from its vulnerable western coastline. This strategy prioritizes building and stockpiling equipment in forests, mountainous regions, and coastal areas on the eastern side of the island. Stockpiling and pre-positioning

are central to this strategy, and players who advocated for it often described using mountain caves and other natural formations to shield systems from attack. These systems could be positioned in such a way that it maximizes their protection against conventional attacks and disruptions from electronic warfare systems.

The development of solar power infrastructure would need to be prioritized, complemented by hydroelectrical systems already operating in some mountainous areas. Mobile networks could be established using balloons or aerial drones, while microwave relays spanning across the mountain ranges could transmit data over long distances. Satellite ground stations could be hidden throughout the mountains to enable off-island communications, and HAM radios could serve as an additional backup layer.

The interior strategy could pair well with the establishment of a small cadre of technically trained civilians, capable of operating and maintaining the systems throughout the conflict. Should the conflict become protracted, this strategy would likely sustain communications for a longer period than either the decentralized or centralized strategies, as most infrastructure would be located in areas difficult for the PRC to reach. The principal drawback to the interior strategy, however, lies in the logistical and financial challenges of building and operating systems in rugged terrain. Although fewer installations would be required than in a decentralized strategy, the approach remains costly. Civilians would also have to relocate away from coastal areas to take advantage of the services, which may not be possible for much of the population.

IMPLICATIONS FOR FUTURE PLANNING

The full implementation of civilian training programs, energy resilience measures, and communications systems hardening is beyond the current capacity of Taiwan's government. In this context, strategic planning, and targeted international cooperation will be key. Future planning should carefully consider three key factors: the cost of each system, the technical expertise required to operate and maintain it, and its utility within an overarching national resilience strategy. Further research in these areas is highly recommended.

Many of the technologies and initiatives recommended by the players involve significant start-up and sustainment costs, which must be weighed against their operational value in a conflict scenario. Some technologies, such as P-LEO satellite terminals, are versatile enough to be useful in multiple scenarios, but planners still need to avoid overinvesting in any single platform, particularly if their chosen strategy is not overly dependent on it. Other systems - particularly those that come with higher costs - need to be considered carefully before committing to them. For example, establishing a network of containerized data centers may be an effective way to ensure the integrity of the government information systems on-island, but may prove more expensive than offshoring data to a friendly nation. Conversely, if those

data centers are also used to sustain the island's internal internet connectivity, then prioritizing investments in those systems may be of greater importance. Opportunities for private sector subsidization by U.S. federal grant funding could significantly reduce the costs to speed up the implementation of either of these solutions.

The success of many of these programs will also heavily depend on the population's willingness and capacity to participate in training and operational support. In general, the broader and more distributed the systems are, the larger the number of trained participants required. If a technology is already familiar to the population and easy to use, such as mobile phone applications, then the burden of training the population to use the system is relatively low. However, if the technology requires specialized hands-on training, like HAM radios, the burden can be substantially higher and limit scalability. Tying these investments to non-military goals, such as natural disaster preparedness, may improve the population's willingness to participate in the programs. Ultimately, the government's ability to entice or compel the population to dedicate time to learning how to operate and repair certain systems will be critical to the success of any resilience plan.

The results of the game should be considered within the construct of Taiwan's National Cybersecurity Strategy. The strategy outlines plans for whole-of-society resilience programs and critical infrastructure defense that match well with game findings pointing to the importance of civilian training and preparedness for keeping Taiwan connected during a sustained conflict. The strategy places significant emphasis on building up Taiwan's domestic cybersecurity industry to help maintain internet connectivity during a crisis (Taiwan National Security Council 2025). While budget shortfalls may stymie the progress of some of these initiatives in the short-term, the game findings suggest that anything the government can do to train and educate civilians on cybersecurity practices and basic communications technology could yield substantial benefits during a conflict.

While this game was focused on the resilience of civilian communications infrastructure, we should not overlook the direct military applications of these approaches, which is the focus of most other literature on this topic. Robust, distributed civilian communications, will likely enhance the Taiwanese military's capacity to coordinate actions against a PRC invasion and provide alternatives if military communications are disrupted or destroyed. Furthermore, the investment strategies referenced above can also be paired with different military approaches, such as those that call for decentralized command & control or asymmetric tactics should the PRC gain a foothold on the island (Rodriguez 2025).

Finally, while the solutions and insights generated by the wargame offer valuable guidance for cyber resilience planning, the process of conducting the game itself also produced important outcomes. Bringing together experts from across ICT security firms helped solidify the professional networks through which responders can communicate and plan. In several instances, former players attended post-game briefings to hear feedback from others. Notably,

members of Taiwan's Ministry of Digital Affairs observed one of the game sessions, and invited the game team to conduct a follow-on exercise in Taiwan in 2025, demonstrating how playing the game has itself helped strengthen the network.

CONCLUSION

The Taiwan Digital Blockade Wargame was designed to elicit ideas from the private sector on how Taiwan's government could invest to strengthen its ICT infrastructure. The significant variation in recommendations and strategies generated by the players underscores that there is no single approach to the challenge of enduring digital resilience. This diversity of perspectives highlights the need for Taiwan's government to adopt a comprehensive and flexible strategy, one that integrates selected ideas such as those presented here, to guide future investment and preparedness decisions.

Taiwan must ultimately balance its financial capacity with the level of civil-military preparedness its population is willing to embrace. Both factors are likely to evolve over time, requiring policymakers engaged in preparedness planning to capitalize on favorable moments for investments while being ready to defend expenditures when budget is under greater scrutiny. In the end, the willingness of the civilian population to take an active role in safeguarding their nation's ICT infrastructure may prove to be the most critical determinant of its overall resilience.

ABOUT THE AUTHORS

Jason Vogt is an assistant professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. Vogt previously worked for the Defense Intelligence Agency and served on active duty as an Army officer. He specializes in cyber and wargaming.

Dr. Nina Kollars is an associate professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. Kollars advises on issues of military modernization and emerging technology. In her free time, she manages a community of White hat, hackers who focus on maritime vulnerabilities. Her primary areas of research are in emerging technologies, cybersecurity, and military innovation.

Dr. Michael Poznansky is an associate professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. He is the author of *Great Power, Great Responsibility: How the Liberal International Order Shapes US Foreign Policy* (Oxford University Press, 2025) and *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (Oxford University Press, 2020).

ACKNOWLEDGMENTS

The authors thank Dan Grobarcik, Ed McGrady, and Frank Smith for their assistance in game development and feedback. The authors also thank participants at Blackhat and DEFCON for contributing their time and insights, as well as the ICS Hacking Village for hosting us at DEFCON. This project underwent IRB review (NWC.2024.0008-DD-N).

REFERENCES

- Badea, Dorel, Marin Marian Coman, Dumitru Iancu, and Olga Bucovești. 2018. "Critical Infrastructure Protection in the Knowledge Society: Increasing the Safety Level by Use of Learning Based on Wargaming Expertise." *BRAIN. Broad Research in Artificial Intelligence and Neuroscience* 9 (4): 38–48.
- BBC. 2025. *Taiwan: Massive Power Outage Affects Five Million Households*. March 2, 2025. <https://www.bbc.com/news/world-asia-60598234>.
- Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 2023. *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*. Center for Strategic / International Studies. <https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan>.
- Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 2025. *Lights Out: Wargaming a Chinese Blockade of Taiwan*. Center for Strategic / International Studies. <https://www.csis.org/analysis/lights-out-wargaming-chinese-blockade-taiwan>.
- CIA World Fact Book. 2025. *Field Listing – Internet Users*. <https://www.cia.gov/the-world-factbook/field/internet-users/>.
- Curry, John. 2012. *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists*. History of Wargaming Project.
- Duncan, Matthew. 2023. "The Evolution of the North American Electrical Reliability Corporation's Grid Security Exercise." In *Cyber Wargaming*, edited by F. Smith, N. Kollars, and B. Schechter, 137–138. Washington, DC: Georgetown University Press.
- Elg, Johan. 2018. "Wargaming in Military Education for Army Officers and Officer Cadets." PhD diss., King's College London. <https://kclpure.kcl.ac.uk/portal/en/studentTheses/wargaming-in-military-education-for-army-officers-and-officer-cad/>.
- Ericsson. 2025. *Chunghwa Telecom Shows the Way Forward*. <https://www.ericsson.com/en/cases/2022/chunghwa-telecom-and-ericsson>.
- EUTELSAT/ONEWEB. 2025. *Chunghwa Telecom Selects Eutelsat OneWeb for Low Earth Orbit (LEO) Satellite Services*. November 15, 2025. <https://oneweb.net/resources/chunghwa-telecom-selects-eutelsat-oneweb-low-earth-orbit-leo-satellite-services>.
- Fedina, Katja, and Rebecca Lucas. 2025. *Building Societal Resilience Through Wargaming*. RAND Corporation (April 2025). <https://www.rand.org/pubs/commentary/2025/04/building-societal-resilience-through-wargaming.html>.
- Haggman, Andreas. 2019. "Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education." PhD diss., Royal Holloway, University of London.
- Hioe, Brian. 2025. *Amid KMT Budget Cuts, Taiwan's DPP Proposes Raising Defense Spending*. The Diplomat (February 18, 2025). <https://thediplomat.com/2025/02/amid-kmt-budget-cuts-taiwans-dpp-proposes-raising-defense-spending>.
- Hirst, Aggie. 2020. "States of Play: Evaluating the Renaissance in US Military Wargaming." *Critical Military Studies* 8 (1): 1–21. <https://doi.org/10.1080/23337486.2019.1707497>.
- Institute for Security and Development Policy. 2025. *The Silicon Shield Erosion: Fortifying Taiwan Against Geopolitical Shocks*. <https://www.isdp.eu/the-silicon-shield-erosion-fortifying-taiwan-against-geopolitical-shocks/>.
- International Energy Agency. 2025. *Chinese Taipei*. <https://www.iea.org/countries/chinese-taipei>.
- Jansen, Bernardus, Natalia Kadenko, Dennis Broeders, Michel van Eeten, Kevin Borgolte, and Tobias Fiebig. 2023. "Pushing Boundaries: An Empirical View on the Digital Sovereignty of Six Governments in the Midst of Geopolitical Tensions." *Government Information Quarterly* 40 (4): 101862.
- Kepe, Marta, and Scott W. Harold. 2025. *Building Taiwan's Resilience: Insights into Taiwan's Civilian Resilience Against Acts of War*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR3388-1.html.
- Michaels, Jeffery, and Michael Williams. 2025. *A Wargame to Take Taiwan, from China's Perspective*. War on the Rocks (October 7, 2025). <https://warontherocks.com/2025/10/a-wargame-to-take-taiwan-from-chinas-perspective/>.
- MODA (Ministry of Digital Affairs). 2025a. *Deputy Minister Herming Chiueh Attends International Cybersecurity Conference, Sharing Taiwan's Experience in Cybersecurity and Communication Resilience*. <https://moda.gov.tw/en/press/press-releases/13324>.

Preparedness Wargaming for Critical Infrastructure Resilience: Taiwan Digital Blockade Wargame

- MODA (Ministry of Digital Affairs). 2025b. *Response of Ministry of Digital Affairs to Chunghwa Telecom's Subsea Cable Disruption on January 3, 2025*. January 3, 2025. <https://moda.gov.tw/en/press/press-releases/14990>.
- MODA (Ministry of Digital Affairs). 2025c. *The Ministry of Digital Affairs Demonstrates High-Altitude Communication Platform to Strengthen Taiwan's Communication Resilience*. <https://moda.gov.tw/en/press/press-releases/14322>.
- Mok, Charles, and Kenny Huang. 2024. *The Most Critical Resilience Questions of Them All: Taiwan's Undersea Cables*. University of Nottingham Taiwan Research Hub (October 2, 2024). <https://taiwaninsight.org/2024/10/02/the-most-critical-resilience-questions-of-them-all-taiwans-undersea-cables/>.
- Perla, Peter. 2022. "Wargaming and the Cycle of Research and Learning." *Scandinavian Journal of Military Studies* 5 (1): 197–208. <https://doi.org/10.31374/sjms.124>.
- Rodriguez, Tyler. 2025. "The Inevitable Invasion is Over, Now What? Resistance in a Post-Invasion Taiwan." *Small Wars Journal* (August 18, 2025). <https://smallwarsjournal.com/2025/08/18/the-inevitable-invasion-is-over-now-what-resistance-in-a-post-invasion-taiwan/>.
- Taiwan National Security Council. 2025. *National Cybersecurity Strategy 2025*. National Information and Security Office.
- TaiwaneSim. 2025. *Taiwan Mobile Operators: Which One Is the Best?* <https://taiwanesim.com/mobile-operators/>.
- TeleGeography. 2025. *Submarine Cable Map*. <https://www.submarinecablemap.com/submarine-cable/flag-north-asia-loopreach-north-asia-loop>.
- The Economist. 2025. *Taiwan's Political Drama Is Paralysing Its Government*. January 23, 2025. <https://www.economist.com/asia/2025/01/23/taiwans-political-drama-is-paralysing-its-government>.
- U.S. Department of State. 2025. *2024 Investment Climate Statements: Taiwan*. Technical report. <https://www.state.gov/reports/2024-investment-climate-statements/taiwan/>.
- Vogt, Jason, and Nina Kollars. 2024. *Taiwan Digital Blockade Wargame Report*. U.S. Naval War College. https://usnwc.edu/_images/portals/0/NWCDepartments/Cyber--Innovation-Policy-Institute/CIPI-Taiwan-Digital-Blockade-Distro-A2900.pdf.
- Vogt, Jason, Nina Kollars, and Michael Poznansky. 2024. "Should Taiwan Attempt to Replicate the Zelensky Playbook." *War on the Rocks*, May 15, 2024. <https://warontherocks.com/2024/05/should-taiwan-attempt-to-replicate-the-zelensky-playbook/>.
- Waligora, Erik. 2025. *Advancing Cyber Resilience: Taiwan's Strategic Shift in the Seventh Phase of Its National Cybersecurity Program*. Global Taiwan Brief 10, no. 14 (July 2025). <https://globaltaiwan.org/2025/07/advancing-cyber-resilience-taiwans-strategic-shift/>.
- Wenger-Trayner, Etienne, and Beverly Wenger-Trayner. 2015. *Introduction to Communities of Practice: A Brief Overview of the Concept and Its Uses*. <https://wenger-trayner.com/introduction-to-communities-of-practice/>.
- Wu, Huizhong, and Johnson Lai. 2023. *Taiwan Suspects Chinese Ships Cut Islands' Internet Cables*. Associated Press (April 18, 2023). <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366>.

Received 8 March 2025; Revised 20 October 2025; Accepted 5 November 2025