CYBER & INNOVATION
POLICY INSTITUTE
U.S. NAVAL WAR COLLEGE

Authored by: Jason Vogt & Nina Kollars

Edited by: Dan Grobarcik

Principal Investigators: Jason Vogt, Nina Kollars & Michael Poznansky

Additional Game Team Members: Ed McGrady, Tiffany Tat, Stephanie Helm, Nick Henderson, Erik Whitworth

U.S. Naval War College

Cyber & Innovation Policy Institute

The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

The Taiwan Digital Blockade Wargame Report

Authored by: Jason Vogt & Nina Kollars

Edited by: Dan Grobarcik

Principal Investigators: Jason Vogt, Nina Kollars & Michael Poznansky

Additional Game Team Members: Ed McGrady, Tiffany Tat, Stephanie Helm, Nick Henerson, Erik Whitworth

25-P-0004

Table of Contents

Taiwan Digital Blockade Wargame Report

I. Executive Summary

The Taiwan Digital Blockade Wargame explores ways to improve the resilience of Taiwan's information and communications technology (ICT) in the event of a conflict with the Peoples Republic of China (PRC). The wargame is part of The Taiwan Resilience Project, a research initiative conducted by the U.S. Naval War College's Cyber and Innovation Policy Institute (CIPI). The project is focused on understanding and improving Taiwan's ICT security and operations. The "Taiwan Digital Blockade Wargame," was designed to fill gaps in knowledge about the different capabilities that private sector and domestic critical infrastructure planners could employ in a Taiwan conflict scenario.

Two iterations of the game were played in Las Vegas, Nevada in August 2024, which coincided with two of the world's largest cybersecurity conventions, Blackhat and DEFCON. The game was played by twenty-seven players who were pre-recruited from conference attendees with backgrounds in cybersecurity, industrial control systems, data center operations, threat intelligence, subsea cabling systems and the government.

The wargame was designed to generate recommendations that could help improve Taiwan's ICT resilience in three areas: infrastructure, cybersecurity, and recovery. Overall, the players generated a series of solutions and overall strategic approaches. Note takers identified 65 recommendations, 70% of which related to purchasing or improving ICT or power infrastructure. Only 10% of the recommendations dealt exclusively with cybersecurity, which centered on using software and cryptography to enhance communications security. The remaining 20% of recommendations dealt with recovery, which focused on stockpiling "critical spares"—replacement components that keep systems running—and improving the technical skills of Taiwan's civilian population.

Solutions: Cost and Speed

Overall, recommendations that were the least expensive and had the shortest implementation timelines were those focused on bolstering communications infrastructure and cybersecurity. Recommendations related to power generation & storage infrastructure, data backup & distribution infrastructure, and stockpiling critical spares to aid recovery efforts were judged to be more expensive and more difficult to implement.

Workforce development and training also featured strongly during the game, but the effectiveness of those solutions was the least understood from both time and cost perspectives. Participants recommended that the government undertake civilian training and disaster preparation in anticipation of a conflict. Ideas ranged from establishing basic training programs in cybersecurity for the general population to the creation of an elite civilian cyber corps. The costs of implementing these recommendations could vary significantly depending on scale, scope and depth of programs. The success of these programs also hinges on the population's willingness to participate, a factor not evaluated during this wargame.

Strategic Approaches

Three different strategies emerged for improving Taiwan's ICT resilience during gameplay: centralized, decentralized and the interior strategy. A centralized strategy would concentrate critical infrastructure near targets the PRC is unwilling to strike. A decentralized strategy would distribute lower cost assets across the population centers, saturating the environment and complicating the PRC's ability to target critical nodes. An 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 possesses its own strengths and weaknesses, and each requires different types of investments to be prioritized to achieve optimal results. Taken together, the strategies and recommendations can be used to generate a framework that policymakers could use to evaluate the utility of their future investments.

II. Introduction & Background

Research Questions

1. What key investments and policies could be implemented to improve the resilience of the Taiwan's capacity to communicate with its people and the world leading up to and through conflict?
2. Are there new approaches and technologies that will be mature in a 5-year timeline that can make Taiwan's ICT infrastructure more resilient?
3. Are there strategic approaches to the positioning and acquisition of ICT and energy infrastructure that could deter or make the island more resilient?

Taiwan's ICT and Energy Trajectory

Taiwan is one of the most digitally connected countries in Asia with more than 90% of its population online. This access is enabled by a robust ICT infrastructure supported by three major on-island telecoms providing mobile and fiber network access. Chunghwa Telecom is the largest provider, accounting for 33% of the market share. Chunghwa has partnered with several multinational corporations to establish a modern Centralized Radio Access Network (C-RAN) communications architecture to enable 5G services for private users and businesses. Unlike traditional mobile architectures, which rely on robust base station infrastructure to function, C-RAN consolidates data processing and information exchange through centralized towers and data processing facilities, improving efficiency and reducing electricity costs. These systems are unpinned by a robust network of fiberoptic cabling.

Taiwan is currently reliant on undersea fiberoptic cables to connect to the global internet. The island is connected to ten undersea cable systems, which include 16 individual cables, with three additional systems planned in the coming years. Together, these cables carry approximately 97% of Taiwan's global internet traffic. Three of these systems route directly through China, making them highly vulnerable to exploitation during a potential conflict. Inadvertently or not, Taiwan's undersea cables have been severed at least 27 times, demonstrating their vulnerability to disruption during conflict.

Learning from the conflict in Ukraine, Taiwan's leaders recognize the need to harden the island's digital infrastructure and have embarked upon a campaign to defend against communications isolation. Taiwan's largest telecommunications company formally signed an agreement with EutelSat/OneWeb,

which operates a satellite constellation like Starlink, to make its mobile network more resilient. These systems will be integrated into existing and future planned communications architecture to help maintain connectivity to the global internet. While these systems have proven resilient to disruption from jamming, they provide only a fraction of the bandwidth that is currently available through undersea cables.

Power generation and distribution is controlled by the Taiwan Power Company (referred to as Taipower). 80% of Taiwan's power is generated by coal and liquified natural gas, most of which is imported via maritime routes. While the bulk of these resources are imported from the United States, Canada, and Australia, ensuring delivery of them during a conflict would be extremely challenging.

The Taiwanese are actively attempting to resolve their critical energy issues. Major power outages have occurred regularly over the last ten years, with some blackouts affecting 5-7 million customers. This has also had major implications for Taiwan's power-hungry semiconductor industry which has lost hundreds of millions of dollars due to the power outages. The semiconductor industry accounts for more than half of all industrial energy use, a demand that is expected to grow by 20% in the coming years.

To address these challenges, Taipower and the government are investing in a 17.5 billion decade long smart-grid and renewable energy infrastructure upgrade. These efforts are focused on solar and wind generation and are supported by major investments in smart-meters and cloud infrastructure located at newly built on-island data centers. Chunghwa Telecom has partnered with Taipower to install several hundred miles of additional fiberoptic cables to enable these smart grid technologies. Their goal is to increase Taiwan's renewable energy production to 20% of the total energy used by the island.

III. Gameplay

Game Overview

The game placed players into the role of advisors to the government of Taiwan. Players were divided into advisory councils presented with two conflict vignettes involving a PRC invasion of Taiwan to occur in 2030. During the first vignette, the PRC refrained from conducting conventional military attacks on Taiwan, and instead used cyber, electronic warfare and sabotage to disrupt civilian communications and power infrastructure. In the second vignette, the PRC launched a full-scale attack on Taiwan, including against critical infrastructure. The PRC's goal was to isolate the government in Taipei from the domestic population and the international community. At the start of each round, the advisory councils received information about the degraded state of Taiwan's civilian/government infrastructure. Teams then met to discuss what types of investments Taiwan should make in the coming years to mitigate the actions that occur in 2030. The advisory councils provided recommendations in three areas: infrastructure, cybersecurity and recovery. Players then voted for the team they believe had the best recommendation.

Scenario

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) decided that the risk of Taiwan declaring independence was high enough to warrant military intervention. They began preparations for an invasion.

With little chance of surprise, the PRC decided to do their utmost to disrupt Taiwan's military and civilian communications prior to the assault. Seeking to avoid a direct intervention by the U.S. in the first phase of their operation, the PRC decided to limit kinetic attacks on the island prior to the launching of amphibious forces. However, they were willing conduct operations using cyber, electronic warfare and clandestine sabotage prior to the invasion.

The Taiwanese government was aware of the impending attack and 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.

Schedule

Introductions/Game Brief: 30 min

Move X 2: (1 hour 15 min each)

- Red Action: 10 min
- Team Planning: 30 min
- Team Presentations: Infrastructure: 10 Min
- Voting: 5 minutes
- Team Presentations: Cybersecurity: 10 Min
- Voting: 5 minutes
- Team Presentations: Recovery: 10 Min
- Voting: 5 Min

Total: ~3 Hours

Game Activities

Introductions/Game Brief (30 Minutes): Players arrived and were separated into their advisory councils (teams). The game team and players then introduced themselves, highlighting their relevant expertise.

The game team provided players with an overview brief, which included the game purpose, an overview of Taiwan's ICT/power trajectory, mechanics of play, desired end state and logistical information. Players were then given an opportunity to ask questions before the game began.

Move overview (1:15 minutes)

At the start of each move, players were given a vignette overview and ~30 minutes to plan within their respective groups. Members of each group proposed potential investment solutions in three areas: infrastructure, cybersecurity, and recovery. Facilitators took notes on the discussion and helped answer questions.

Following the planning period, teams returned to the central map board. Each team presented a single investment recommendation for one of the investment areas. Other teams were able to ask clarifying questions or offer a rebuttal. After each team offered a recommendation, players

voted individually on which team's recommendation they thought was the best. Players could not vote for their own teams' proposal. Each investment area was discussed following this format. Once completed the game shifted to the second vignette.

Vignette 1: Pre-invasion

PRC Objective 1: Diminish the ability of civilian infrastructure to support the war effort

PRC declared that Taiwan is illegally using high bandwidth communications to import and export proprietary (Chinese) materials.

Multiple fiberoptic submarine cables connecting to Taiwan are physically severed; additionally cyberattacks are conducted on several cable landing stations, disrupting the flow of international internet traffic to the island. Cables running directly to the PRC mainland remain intact and are likely to be monitored by PRC authorities.

PRC leverages airborne electronic warfare platforms to disrupt GPS signals and commercial satellite ground stations operating with civilian ICT infrastructure. These disruptions are episodic based on the where the PRC electronic warfare platforms are operating.

Data centers housing email servers for several large internet providers are targeted by ransomware.

Commercial mobile infrastructure remains largely intact but is suffering degradations in areas with electrical power disruptions.

PRC Objective 2: Disrupt civilian critical infrastructure to support the war effort & increase stress on the civilian population

Data centers supporting microgrid electrical power distribution are targeted with malware that encrypts data related to customer smart-meter identification and usage. Furthermore, engineering workstations used to manage industrial control systems responsible for microgrid operations have lost all visibility of the routers and sensors used to monitor power fluctuations. As a safety precaution, all renewable power generation systems connected to microgrids have been shut down, reducing Taiwan's energy capacity by 20%.

Power outages are affecting multiple manufacturing sectors, including the production of semiconductors. Most semiconductor manufacturing facilities are currently offline.

Malicious cyber actors have also targeted Taiwan's security and traffic control systems. While some of these systems have been taken completely offline, others are operating improperly causing confusion and traffic jams in several urban areas. There is concern that the compromise of these systems indicates that PRC saboteurs are active on the island and that follow-on physical attacks are likely.

Vignette 2 Conventional Attack

PRC Objective 1: Degrade and destroy Taiwan's military fighting capabilities

PRC conducts strikes to suppress Taiwan's aircraft, close all its airfields, and ensure that nothing can fly in Taiwanese airspace.

Taiwan's air defense systems are targeted by missile attacks.

Bridges and key routes that can support beach defensive systems are destroyed.

Taiwanese vessels are targeted in the island area.

Taiwan's national command and control systems are targeted. This includes kinetic attacks against any long-range UHF/VHF/HF emitters and their control systems.

Objective 2: Further degrade civilian telecommunications and power infrastructure with kinetic attacks.

Missiles strike Taiwan's power transmission capability but leave power production facilities intact.

PRC engaged in jamming all backbone microwave and satellite communications that remain on island. This includes any point-to-point microwave communications relay towers.

PRC conducts missile strikes on data centers and their associated power systems.

Participants

Blackhat Game Execution August 8, 2024:

The first iteration of the game was executed in a private conference suite at the Cosmopolitan Hotel. The game included 12 players with backgrounds in government and industry cybersecurity, industrial control system cybersecurity, data center operations, and regional expertise.

DefCon Game Execution August 10, 2024:

The second iteration of the game was executed on the open DefCon conference floor. The game included 15 players with expertise in government and industry cybersecurity, threat intelligence, industrial control system cybersecurity and undersea cabling systems.

IV. Findings

Analysis of Player Recommendations

This wargame was designed to elicit player insights into infrastructure, cybersecurity, and recovery. Overall, the players generated 65 solutions or recommendations, 70% of which related to purchasing or improving infrastructure. These infrastructure recommendations can be further subdivided into the following categories: communications infrastructure, power generation & storage infrastructure, and data backup & distribution. Only 10% of the recommendations dealt with cybersecurity, which centered on using cryptography and related methods to enhance communications security. The remaining 20% of recommendations dealt with recovery, which focused on stockpiling critical spares and improving the technical skills of the civilian population.

During gameplay, players were not provided specific budgets to work within and were instructed not to constrain their recommendations based on finances. However, during the post-game analysis, recommendations were evaluated and categorized by cost (high, moderate, low) and the amount of time it would take to implement (short 1-2 years, medium 2-4 years, long-term 4+ years). Taken individually, two-thirds of the recommendations were judged to be low to moderate cost and capable of being executed in 1-4 years. The remaining recommendations 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. As a result, those high cost/long-term recommendations were excluded from the remainder of this analysis.

Recommendations focused on bolstering communications infrastructure and cybersecurity were the least expensive and had the shortest implementation timelines. This included several technologies that already exist today, including HAM radios, microwave relays, P-LEO satellite communications, long-range radio mesh networks, and communications networks augmented by drones or aerial ballons. The players also generated several novel concepts for enabling communications using Bluetooth to create secure messaging services that do not require a functioning mobile tower. They also suggested implementing cryptographic protocols using blockchain and other methods to ensure that messages originated from a trusted source.

Recommendations for power generation & storage, data backup & distribution, and stockpiling critical spares were judged to be more expensive and potentially more difficult to implement. These recommendations call for the expanded use of renewable power generation technologies (wind, solar, 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.

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 training programs in cybersecurity to the establishment of an elite civilian cyber corps. The costs of these recommendations could vary significantly depending on scale, scope and depth of programs implemented.

Planning Factors and Tradeoffs

Full implementation of civilian training, energy resilience measures, and communications systems hardening is well beyond the resources of Taiwan's government. It is here that planning, and carefully targeted international cooperation will be key. Due consideration in planning should be given to three factors: the cost of a system, the technical knowledge required to operate/maintain it, and the system's utility within an overarching resilience strategy. Follow-on research in these areas is highly recommended.

Many of the technologies and programs recommended by the players come with significant start-up and sustainment costs, which must be balanced against their utility in a conflict scenario. Some technologies are versatile enough to be useful in multiple scenarios, such as P-LEO satellite terminals, but planners still need to avoid overinvesting in a single platform, particularly if their strategy does not require it. Other systems - particularly those that come with higher costs - need to be considered carefully before committing to them. For example, establishing a system of containerized data centers may be an effective way to ensure the integrity of the government information systems on-island, but it is probably more costly than offshoring the data in a friendly nation. However, if those data centers are also going to be used to keep the island's internal internet functioning, then prioritizing investments on 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 also hinges on the population's willingness to participate in training to operate them. In general, the more systems the government purchases and the more distributed they are, the greater number of people will be needed to operate them. 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 that required to operate a HAM radio, then the burden can be substantially higher. Whether or not the government can entice or compel the population to dedicate time to learning how to operate and repair certain systems is critical to understanding a plan's chances of success.

The Three Strategies

Three different ICT resilience strategies emerged during gameplay: centralized, decentralized and the interior strategy. A centralized strategy would concentrate critical infrastructure near targets the PRC is unwilling to strike. A decentralized strategy would distribute lower cost assets across the population centers, saturating the environment and complicating the PRC's ability to target critical nodes. An 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 of these strategies require different types of investments to be prioritized to achieve optimal results.

Centralized Systems: Targeting May Be Unappealing to Adversaries

A centralized strategy hinges upon the idea that the PRC is likely unwilling to conventionally 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 other buildings housing important Chinese cultural artifacts. Players advocating for this strategy recommended building up renewable power infrastructure, data centers and concentrating communications infrastructure in these areas. This would create safe-zones where civilian refugees could congregate and maintain communication with the outside world.

A centralized strategy holds several advantages, not the least of which is the fact that Taiwan's government is already prioritizing renewable power investments, specifically wind and solar, around key manufacturing sites. Integrating data centers into this construct, along with the capability to connect to one or more P-LEO satellite constellations, could enable segments of the population to maintain communications with the outside world at a relatively low cost. Since the number of locations is limited, the infrastructure could be operated by the government or a professional private sector workforce and would not require extensive training for the civilian population writ large.

Drawbacks to the centralized strategy include the limited number of locations available, which means that large portions of the population are unlikely to benefit from their existence. Located along urban coastal areas, these sites would also remain vulnerable to electronic warfare and cyberattacks, which could cause temporary disruptions to services. Since these locations are already deemed to be of high value to the PRC, it is possible that the buildup of additional infrastructure could incentivize the PRC to seize these areas earlier in the conflict than they otherwise would. Lastly, in the event of a protracted conflict, there is no guarantee the PRC will limit their conventional strikes on these areas, particularly if

they decide to prioritize the destruction of civilian infrastructure as a key objective within its military campaign.

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. 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.

To be successful, the government would need to invest significant time and resources to train civilians to operate and repair these systems. The government would also need to purchase and distribute batteries, repair parts and replacement systems across the country. Well-executed, a decentralized strategy would likely maximize the number of civilians able to maintain communications throughout a 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.

Interior Shelters: Using Geography as a Strength

An interior strategy attempts to use Taiwan's geography to its advantage, establishing power and communications infrastructure away from its vulnerable western coastline. This strategy would prioritize building and stockpiling equipment in the forests and mountainous regions, along with coastal areas on the eastern side of the island. These systems could be positioned in such a way that maximizes their protection from conventional attacks and disruptions from electronic warfare systems. Should the conflict become protracted, this strategy would likely enable communications for a longer period than the other two strategies, as most of the infrastructure would be in areas that will be difficult for the PRC to reach.

Building solar power infrastructure would need to be prioritized, but this could be augmented by hydroelectrical systems that already exist in some mountain areas. Mobile networks could be established using ballons or aerial drones, and data could be transported over longer ranges using microwave relays established across the mountains. Satellite ground stations could be hidden throughout the mountains to enable off-island communications. HAM radios could be used to augment these systems. The interior strategy could pair well with the establishment of a small cadre of technically trained civilians, who could operate and maintain the systems throughout the conflict.

The principal drawback to this strategy is that it requires the infrastructure to be established and operated in difficult terrain. While fewer systems would be needed than those required in a

decentralized strategy, it is still likely to be 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.

V. Conclusion and Follow-on Research

The Taiwan Digital Blockade Wargame demonstrates the need for a comprehensive strategy to improve Taiwan's ICT resilience during a conflict with the PRC. The wargame identified three potential strategies: centralized, decentralized and interior, each with its own strengths and weaknesses. The next step for the research team is to explore how these strategies could be tested against different contingencies, potentially through a follow-on wargame. Additional research is also required to determine which of these strategies is achievable within Taiwan's current and projected fiscal and political environment.

VI. Annexes and Supplemental Data

Game Guide and Note Taking Guide are available upon request

Solutions Spreadsheet

Solutions Spreadsheet.pdf