

Targeting Taiwan:

Beijing's Playbook for Economic
and Cyber Warfare

By Craig Singleton,
RADM (Ret.) Mark Montgomery,
and Dr. Benjamin Jensen

With contributions from Elaine Dezenski,
Josh Birenbaum, and Annie Fixler

Research Memo | October 4, 2024



INTRODUCTION

“The complete reunification of the motherland must be fulfilled, and it will definitely be fulfilled,” declared Xi Jinping on the 110th anniversary of the Chinese Revolution of 1911, underscoring Taiwan’s reintegration into China as a core element of his vision for the “great rejuvenation of the Chinese nation.” For the Chinese Communist Party (CCP), using minimal military force and preserving Taiwan’s infrastructure and economy during reunification are paramount.

A cyber-enabled economic coercion campaign is the CCP’s most strategic and logical approach to realizing this long-term national priority.

The CCP’s strategy to win without fighting is not new. In writings by ancient strategists Sun Tzu and Kautilya, undermining enemy morale and cohesion plays a prominent role. But modern globalization has created more economic connections that China can exploit to achieve coercive aims. Technological innovation created even more digital connections, offering more possibilities for coercion, including through the targeting of critical infrastructure.

Yet the analysis in Washington shaping U.S. strategy toward China does not reflect this reality. There is a conceptual gap. A growing number of war games and tabletop exercises (TTXs) in Washington and Taipei study the “cross-strait invasion” scenario or the “joint blockade” scenario — what operational planners commonly refer to as the “most dangerous” scenarios. War by other means and subterfuge are afterthoughts to modeling naval campaigns and counting missiles.

To overcome this analytical gap, the Foundation for Defense of Democracies and the Taiwan Academy of Banking and Finance conducted a TTX on the “most likely” scenario: Sometime in the next decade, China will combine economic coercion, malicious cyber activity, and limited military moves short of kinetic attacks to break Taiwan’s societal and/or economic resilience and force a major adjustment in its policy toward unification. In this scenario, China learns from Russia’s mistakes and “wins” without a bloody war and widespread condemnation.

The TTX involved 20 players, the majority of whom were senior Taiwanese banking and finance experts, replicating senior policymakers in Taiwan, the United States, and China. The first scenario, “the Long Walk,” involved a protracted and graduated economic coercion campaign to target Taiwan’s resilience and cohesion. The second scenario, “the Ghost in the Machine,” involved cyber-enabled economic warfare over weeks and months (not years), placing pressure on players to identify more immediate options to increase resilience to avoid a major crisis in the future. In this scenario, the CCP simultaneously continued economic attacks on critical infrastructure, disrupted supply chains, reduced confidence in Taiwanese manufacturing, and unleashed cyberattacks and disinformation campaigns that undermined communications, energy, and banking systems. The TTX concluded with a series of crisis vignettes that forced players to re-evaluate their strategies to account for a gray zone campaign and a prolonged military exercise that isolated Taiwan for months.

China’s Siege Mentality

Across the TTX, China’s actions against Taiwan extended beyond the traditional concept of a blockade. Instead, China’s broader siege mentality aimed to gradually starve the island of resources and attack its critical infrastructure to drain its resilience. This strategy involved not just the restriction of goods and services but also sustained psychological and economic warfare to encircle and weaken Taiwan from within. The objective was not just containment but also the eventual capitulation of the besieged.



Dr. Benjamin Jensen introduces TTX scenario.

The insights from the TTX were stark. **An integrated cyber and financial/economic attack by the CCP against Taiwan is a significant risk.** The diplomatic and economic costs to the CCP are lower than expected, and the likelihood of success, barring significant actions by Taiwan, the United States, and other partners, is much higher than expected. The CCP's barrier to entry is lower than a blockade or cross-strait invasion. Beijing has the ability to back in or back out as needed; the "tools" or "weapons" are cheap and sometimes re-usable; and Beijing has plausible deniability for certain actions (especially in cyberspace). The risk thresholds for Taiwan — to both economic and societal resilience — are rapidly approached as the economic and psychological effects produce political pressure on Taipei to act in a manner that military threats short of war do not.

One alarming insight from the TTX was that many CCP actions did not "trip" any redlines in Washington or among allies that an invasion or blockade would. In other words, unless the United States develops, exercises, tests, and calibrates responses to economic and cyber campaigns, Washington's reactions will likely be too slow to meaningfully support Taiwan.

Resilience is key for Taiwan to prevent attacks, mitigate the impact of attacks, and hasten the response and recovery from attacks. In short, Taipei, together with Washington and regional allies, must strengthen Taiwan's economic, cyber, and societal resilience to extend its ability to withstand Chinese coercion from weeks to months or years. Building resilience is a process. It is deliberate and time-consuming and requires coordination across the public sector, private industry, and civil society.

But it can be done. Taiwan can reduce its exposure to Chinese financial influence while building redundancies in communications and energy infrastructure. Adopting lessons from U.S. efforts to improve public-private collaboration, Taiwan can advance its cyber resilience by improving threat sharing, prioritizing certain infrastructure assets — what Washington calls systemically important entities — and designating a civilian agency to coordinate critical infrastructure defenses. To improve societal resilience, Taiwan can continue investing in counter-disinformation efforts to combat efforts to degrade public trust.

The United States and its Asian allies, meanwhile, can strengthen Taiwan's integration into global markets and help Taiwan build more cyber-secure networks. And Washington and its partners can identify pre-agreed responses to CCP economic coercion, including multilateral economic retaliation against key sectors in mainland China.

With the CCP at its center, a network of dictators and despots is building a new authoritarian playbook. Democracies, in turn, need options for campaigning in the gray zone that balance escalation risks with ceding the initiative to despots. The report takes the first steps in providing a framework for thinking about how to defend democracies under siege around the world.

Why FDD and TABF Conducted This TTX

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based nonpartisan, nonprofit research institute focusing on national security and foreign policy. FDD studies the challenges of beleaguered democracies under threat from authoritarian adversaries. This includes Israel, Ukraine, and Taiwan. The Taiwan Academy of Banking and Finance (TABF) is a nonprofit organization advised by the Financial Supervisory Commission of Taiwan. It is the leading organization in Taiwan for research and training banking professionals and for supporting policy initiatives to strengthen Taiwan's financial sector. FDD and TABF share a common concern about the readiness of Taiwan and the United States to deal with a cyber-enabled economic coercion campaign. They conducted this TTX in Taipei in August 2024.

GAME DESIGN, CCP ACTIONS, AND U.S.-TAIWAN REACTIONS

The TTX forced the players, the majority of whom were senior Taiwanese banking and finance experts, to consider a protracted, graduated economic coercion campaign and a crisis defined by cyber-enabled economic warfare. Assuming the roles of senior policymakers in Taiwan, the United States, and China, the players assessed the most likely and dangerous actions the CCP could take short of war to isolate and coerce Taiwan. The TTX concluded by forcing players to re-evaluate their strategies in light of a gray zone campaign and a prolonged military exercise that isolated Taiwan for months.

In each scenario, the players assessed the most likely CCP economic and financial warfare tactics and evaluated a menu of coercive options. (See appendices for quantitative assessments.) For each of the coercive options, players assessed the severity of China's move based on whether the measure changes the decision-making calculus in Taiwan (overall coercion); how vulnerable Taiwan is to the measure today (current vulnerability); if Taiwan can withstand and/or rapidly recover (current resiliency); if it compels Taiwanese political officials to act in the short term (political pressure); and if the effect could cascade beyond Taiwan's borders (spillover risk). (See Data Analysis in the appendices for the scores.) The U.S. and Taiwan teams then developed consensus estimates and assessed the likely impact of the coercive campaign based on how long it would take to cause disruption and how the campaign would affect GDP, price inflation, stock markets, the value of the New Taiwan Dollar, lending, credit ratings, and insurance premiums.

CHINA'S STRATEGIC CALCULUS

In building the game, researchers focused intently on Beijing's strategic calculus. China's actions reveal a deliberate strategy to reshape the regional balance of power and incrementally weaken Taiwan's political, economic, and social fabric. Beijing seeks a long-term shift in the status quo, using a phased and adaptable campaign involving economic, cyber, and military coercion to advance reunification. The TTX reflected China's principal objective to

apply pressure from multiple angles, employing integrated operations designed to erode Taiwan's economic and political resilience, ultimately making Taiwan more susceptible to capitulation.

The China team assessed that China's strategic thinking will likely focus on the following:

- **Political Leverage:** Utilizing economic and cyber operations to destabilize Taiwan's political environment and erode public trust in the government.
- **Psychological Warfare:** Instilling fear and uncertainty in Taiwan's population and government to undermine public confidence in Taiwan's ability to defend itself, thereby making the island more vulnerable to Chinese reunification narratives.
- **Economic Disruption:** Targeting critical sectors and infrastructure to create immediate and significant disruptions, thus weakening Taiwan's ability to sustain prolonged resistance against Chinese pressures.
- **Covert and Overt Tactics:** Employing a mix of covert cyber operations and overt economic measures to maintain plausible deniability while complicating Taiwan's and the international community's ability to respond effectively.
- **Flexibility and Escalation Control:** Maintaining the ability to escalate or de-escalate operations and adjust tactics as necessary based on Taiwan's responses and the international community's reactions.
- **Demonstrating and Refining Capabilities:** Showcasing China's advanced cyber and economic warfare capabilities to deter external support for Taiwan, particularly from the United States, and to project power both regionally and globally.

THE LONG WALK

In the Long Walk scenario, players assessed how the CCP could use protracted, graduated, economic and financial coercion — a multi-year siege in the shadows — targeting Taiwan's resilience and cohesion.

The Taiwan team estimated that China would focus on capturing elites and shifting public opinion while expanding currency manipulation, waging lawfare targeting executives, and creating bureaucratic friction to reduce the ability of Taiwanese firms to move money out of the mainland and Hong Kong. This would have a significant impact on economic growth and market stability over months, resulting in increased inflation and a potential lending freeze. The U.S. team also estimated that China would expand its use of lawfare and bureaucratic measures to slow Taiwanese economic growth but assessed that China was more likely to focus on trade manipulation than currency manipulation.

The China team, however, exercised strategic patience. Beyond causing economic disruptions and widespread uncertainty, Beijing's war of attrition primarily sought political leverage over Taipei by allowing time for the economic and psychological effects to accumulate. China's approach provided flexibility to escalate or de-escalate coercive measures in response to international dynamics.

The China team relied heavily on targeted trade manipulation involving Taiwanese agricultural products, textiles, and chemicals. (See Table 1.) China also sought to manipulate market confidence by affecting investor sentiment and financial market stability, including through disinformation, which the China team assessed was unlikely to provoke a strong response from either Taipei or Washington. These disinformation campaigns sought to instigate bank runs, capital flight, and stock market instability.

Table 1: China's Actions During the Long Walk Scenario

Trade Manipulation

Agricultural Products: Ban imports of Taiwanese agricultural products like pineapples, mangoes, and tea.

Textiles: Impose high tariffs or outright bans on Taiwanese textiles and apparel, disrupting a significant export sector.

Tourism: Restrict or ban Chinese group tourism to Taiwan to exert economic pressure on Taiwan's tourism industry.

Chemicals: Ban imports of Taiwanese chemical products, including specialty chemicals to damage Taiwan's industrial sector.

Market Confidence Manipulation

Stock Market: Use state-owned enterprises and proxies to engage in coordinated short-selling of key Taiwanese stocks, creating panic and driving down market values.

Disinformation Campaign: Spread rumors and false information through state media and social media about financial instability or impending economic crises in Taiwan, targeting companies like TSMC (Taiwan Semiconductor Manufacturing Company).

Influencing Ratings: Using skewed or false data, attempt to influence international credit rating agencies to downgrade Taiwanese firms or the country's credit rating.

Financial System Fragmentation

Interbank Transfers: Limit or freeze interbank transfers between Taiwanese and Chinese banks, causing delays and disruptions in financial transactions.

International Payments: Restrict or block payments and remittances to and from Taiwan, creating chaos and impacting businesses reliant on cross-border transactions.

Financial Services: Impose sanctions or financial restrictions on key Taiwanese financial institutions, cutting them off from financial markets.

As the U.S. and Taiwan teams predicted, the China team targeted major Taiwanese businesses and banks by using expanded bureaucratic procedures and delays to slow the transfer of funds out of the mainland and Hong Kong, holding capital hostage and/or requiring that it be reinvested in projects favorable to the CCP. China also blocked payments and remittances to and from Taiwan and restricted the activities of key Taiwanese financial institutions.

To counter China's administrative measures, the U.S. team used existing bureaucratic tools, altering existing executive orders on forced labor to expand the range of inspections and reviews of goods exported from China. The U.S. team was also confident it could use diplomacy and law enforcement to counter CCP efforts to manipulate credit rating agencies, assessing that China's efforts could provide the U.S. government with a predicate to expand U.S. Trade Representative investigations. Finally, the U.S. team assessed that China's efforts to deny payment transfers from the mainland and Hong Kong would trigger Western firms to accelerate their exit from China. If anything, Washington could seize on this new risk environment to advocate for "ally-shoring," urging businesses to invest in democracies that respect free markets and the rule of law.

The Taiwan team took a more defensive approach. It sought a coordinated diplomatic effort to help Taiwanese firms move manufacturing to the United States or nearby countries like Mexico, noting that Taiwan does not have spare domestic capacity. The Taiwan team also discussed the need to expand ongoing efforts to counter Beijing's malign cyber-enabled influence operations lest the CCP use the information high ground to justify efforts to isolate Taiwan economically. Finally, the Taiwan team saw a need to develop loan vehicles and other financial instruments to support firms targeted by the CCP and help private sector firms accelerate their departure from the mainland.

The China team saw the U.S. moves as largely counterproductive, potentially unconstitutional in some cases, and almost certain to trigger industry blowback. This was particularly true regarding expanding the forced labor-related executive orders, which would potentially take months or years to enforce. The China team also assessed that these new bureaucratic burdens would fall largely on multinational firms, although the team acknowledged that these moves could exacerbate de-risking narratives and lead some multinationals to further reduce their Chinese supply chain dependencies.

Conversely, the China team assessed that, using other tools, Washington could have undermined China's attempts to isolate Taiwan. For example, while symbolic, sending a high-level diplomatic delegation to Taiwan along with a group of American CEOs would signal that the United States is serious about strengthening economic ties with Taiwan. Such a move could encourage other countries to do the same, thereby further undermining China's isolation campaign. The China team noted that expressing interest in fast-tracking a proposed U.S.-Taiwan free trade agreement would also accomplish this objective. Lastly, the China team was surprised at how reluctant Taiwan was to use its leverage with respect to semiconductor exports. Simply announcing plans to slow or halt the export of semiconductors and their components, coupled with backchannel messaging, could give China pause.

For the Taiwan team, the larger question was how to accelerate trade diversification away from China without overly compromising its business community. The team discussed the need to expand discussions about building industrial parks in Northern Luzon and/or Mexico and explore ways to use the tax code to incentivize firms to move money out of Hong Kong because this concentration of Taiwanese capital is at risk. The central challenge, however, is a lack of trust: the business community is weary of Taiwanese government policy even when it seeks to help them.

The Taiwan team also noted that most of their policy options required international coordination, making them difficult to implement. Diplomacy and economic statecraft would have to be coordinated through multiple channels to synchronize policy responses and build cohesion with the business community.

Finally, the team discussed mapping economic interdependencies and risks in support of Taiwanese business diversification efforts. International companies are eager to find alternatives to their existing business operations in China. The challenge is building sufficient trust and establishing a comprehensive assessment of the different economic, trade, and financial strategies required to support the diversification and de-risking process.

At the end of the scenario, collectively, the three teams discussed leading indicators that might reveal China's intent to launch a sustained coordinated economic warfare campaign against Taiwan. (See Table 2.)

Table 2: Indicators the CCP is About to Launch a Sustained Coordinated Economic Warfare Campaign Against Taiwan

Comprehensive Trade Restrictions: Broad and multi-faceted trade restrictions on a range of Taiwanese exports and imports.

Targeted Sanctions on Key Industries: Sanctions or economic measures targeting Taiwan's critical industries (e.g., semiconductors and electronics).

Escalation in Rhetoric: An increase in hostile and aggressive rhetoric from Chinese officials and state media, explicitly targeting Taiwan's economic stability.

Diplomatic Maneuvering: Efforts to isolate Taiwan diplomatically, such as lobbying other countries to sever economic ties with Taiwan or withdraw recognition of Taiwan.

Prolonged Military Presence: Sustained and heightened military presence in the Taiwan Strait or prolonged, large-scale military exercises.

Market Interference: Manipulating financial markets, such as large-scale short-selling of Taiwanese stocks or currency manipulation to destabilize the New Taiwan Dollar.

Financial Coercion: Pressure on multinational corporations to withdraw investments from Taiwan or cease operations, backed by threats of punitive measures in China.

THE GHOST IN THE MACHINE

Unlike the Long Walk, this scenario forced players to respond to a crisis over weeks and months as opposed to years. This placed more pressure on players to increase resilience to avoid a major crisis resulting from a future cyber-enabled economic warfare campaign.

The U.S. team estimated that China would target critical infrastructure, specifically energy, and banking and finance while seeking to disrupt supply chains and reduce confidence in Taiwanese manufacturing. The team saw the greatest danger from sustained attacks on energy infrastructure, including liquid natural gas (LNG) imports and storage, that could lead to rolling blackouts and energy rationing. This would undermine the tech sector and cause public panic. The U.S. team believed China would pair this campaign with cyberattacks to undermine confidence in banking and public exchanges, compounding public panic and reducing investor confidence.

The Taiwan team assessed that China would wage cyberattacks on energy and financial infrastructure. While the Taiwanese public has historically demonstrated it can survive weeks with little or no energy, modern energy consumption levels and manufacturing demands are much higher. The Taiwan team assessed that China would target the financial system — exchanges and easy pay systems — to undermine investor and public confidence.

The Taiwan team believed China would also impose a digital blockade by cutting fiber optic cables and hacking a major telecom company to isolate the island and create panic. China could also launch distributed denial-of-service attacks, overwhelming Taiwanese networks already stressed by reduced bandwidth. The Taiwan team believed that the extent of the financial fallout would depend on the length of the cyber campaign and the depth of short-term price fluctuations linked to hoarding.

These estimates largely paralleled the China team's approach. The China team assessed that Beijing would disrupt Taiwanese society while maintaining adaptability and enough ambiguity and deniability to limit a U.S. response.

This logic led to three targets: financial system cyberattacks, cutting submarine cables, and energy infrastructure attacks. (See Table 3.)

Table 3: China’s Actions During the Ghost in the Machine Scenario

<u>Financial System Cyberattacks</u> Malware Insertion: Deploy malware to disrupt banking networks, particularly targeting interbank transfer systems to cause delays and transaction errors. DDoS Attacks: Launch distributed denial of service attacks on online banking platforms, preventing customers from accessing accounts and conducting transactions. Data Breaches: Steal sensitive financial information and threaten its release. Ransomware: Use ransomware attacks to lock up critical financial data. <u>Severing Submarine Cables</u> Plausible Deniability: Use Chinese shipping and non-military vessels to cut cables, making the actions appear as accidents or isolated incidents. Underwater Drones: Deploy underwater drones to cut or damage submarine cables at strategic points but ensure the operations seem haphazard and uncoordinated. Coordination and Timing: Target cables at different times to maximize disruption and prolong recovery while maintaining the appearance of random incidents. Disinformation Campaign: Spread disinformation about the causes of the outages to create confusion, delay responses, and avoid direct attribution to China. Repair Prevention: Use diplomatic and covert means, like filing false maritime navigation warnings, or bureaucratic means to delay repairs, extending disruption. <u>Energy Infrastructure Attacks</u> Malware Infiltration: Use malware to disrupt the operations of power plants, targeting control systems to cause shutdowns and outages. Grid Attacks: Conduct cyberattacks on the power grid’s infrastructure, targeting substations and transformers to create widespread and prolonged outages. SCADA Systems: Target supervisory control and data acquisition (SCADA) systems that control energy infrastructure, causing operational failures and safety concerns. Physical Sabotage: Combine cyberattacks with physical sabotage, such as coordinated attacks on key transmission lines and substations, to maximize disruption and complicate recovery efforts.
--

The China team aimed to cause immediate and significant disruption to Taiwan’s critical infrastructure and economy by integrating economic pressure with cyber operations while also instilling fear and uncertainty in Taiwan’s population and private sector, undermining public confidence in the government.

The China team launched cyberattacks against Taiwan’s banking networks, particularly targeting online banking platforms and interbank transfer systems. The attacks caused delays, transaction errors, and financial turmoil, and

undermined public trust in the sector. Next, the team used non-military Chinese vessels to repeatedly cut Taiwanese undersea cables to paralyze internet and telecommunications services, creating chaos and communication breakdowns while maintaining plausible deniability. Finally, the China team launched cyberattacks on Taiwan's energy grid. Once again, the objective was disruption — power outages, industrial production stoppages, and interruptions to daily life. Targeting hard-to-replace transformers ensured longer power outages, while targeting industrial control systems caused operational failures and safety concerns.

Given this mix of cyber and physical sabotage, the U.S. team recommended steps to enhance Taiwanese resilience. First, Washington signaled a willingness to use diplomacy, economic sanctions, and even military action to counter cyber aggression. The goal was to complicate, if not deter, Chinese targeting of critical infrastructure. If the United States could engage other democracies to adopt a similar stance, it would bolster the deterrent signal.

Second, the U.S. team discussed supporting efforts to diversify Taiwan's energy market, including by using small modular reactors (SMRs). The Taiwanese team remained wary of pursuing nuclear energy, at least in the short term, because of domestic politics and concerns about the commercial viability of SMRs. The China team noted that the best way to build resilience in the short term was to stockpile backup equipment and expand LNG storage capacity.

Third, the U.S. team discussed creating a mirrored exchange for Taiwan to support the continuity of its economy. Washington might also create a mechanism or backstop through the Federal Reserve to allow dollar transactions or currency swaps to help stabilize the Taiwanese dollar.

Lastly, the U.S. team discussed working with Taiwan and key allies, like Japan, to store cables and invest in ships and crews to rapidly repair or lay new cable while also building capacity to share bandwidth in the event China severely degrades Taiwan's communications infrastructure. This multi-year effort would likely require broad international coordination to ensure sufficient downlink stations and on-demand satellite access across multiple networks.

The Taiwan team focused on how to absorb shocks in a manner that did not disrupt democracy or long-term economic prospects. The team discussed electric grid resiliency efforts, including using solar panels connected to large batteries, expanding geothermal production, creating local resilience hubs to store energy and even facilitate medical treatment during a crisis, and learning from Ukraine about rapid grid repair.

The team discussed creating a large-scale cloud backup of the economy, learning from Estonia's Data Embassy program and from Ukraine's efforts to move its data outside the country after Russia's full-scale invasion. The Taiwan team also noted that ongoing cyber workforce investments were key to increasing its resilience.

Finally, the Taiwan team discussed ideas to improve the resilience of undersea cables, as well as establishing connectivity between Japan, Taiwan, and the rest of Southeast Asia, thus making efforts to cut cables in Taiwan likely to affect states across the region. The team also discussed incentivizing Southeast Asian countries to store data in Taiwan, creating a data shield that would alter CCP cost-benefit calculation.

A fundamental cost differential hung over the discussion. For China, cyber is a cheap and easy tool of coercion, while Taiwan's efforts to build economic and cyber resilience and energy diversification would be very expensive, rely heavily on multilateral coordination, and take years to implement while not preventing cyber-enabled sabotage in the interim.

The discussions concluded with a conversation about the leading indicators that Beijing planned to use cyber operations as part of its economic coercion campaign. Building on the prior discussion, the teams focused on increased cyber reconnaissance, coordinated cyberattacks, and supply chain attacks as well as warnings and advisories from partner governments or private cybersecurity firms. (See Table 4.)



TTF participants from the Foundation for Defense of Democracies

Table 4: Indicators the CCP is About to Use Cyber Operations as Part of a Sustained, Coordinated Economic Warfare Campaign Against Taiwan

Increased Cyber Reconnaissance: Increased cyber reconnaissance of critical infrastructure, financial institutions, and government networks, including probing for vulnerabilities and mapping networks.

Coordinated Cyber Activity: Simultaneous or closely timed cyberattacks on multiple sectors, suggesting a well-planned and synchronized effort.

Advanced Persistent Threats (APTs): Deployment of APTs to maintain prolonged access to critical systems, preparing for long-term operations.

Data Exfiltration: Increased theft of sensitive economic and military data.

Public and Private Warnings: Official statements or advisories from cybersecurity firms and government agencies about increased threats from China-linked actors.

Supply Chain Attacks: Targeting software and hardware supply chains to insert malicious code or backdoors to prepare for broader attacks.

Diplomatic and Rhetorical Signals: Escalating rhetoric from Chinese officials and state media, coupled with diplomatic maneuvers that isolate Taiwan economically.

HEAVY HAND STRESS TEST

In an effort to stress-test the policy options from the first two scenarios and develop more recommendations, participants tackled two additional scenarios. These “heavy hand” scenarios outlined ways the CCP could complement long-term economic coercion, financial warfare, and cyber campaigns with gray zone activity and military pressure short of war.

The first scenario, Gray Dawn, portrayed an escalating series of gray zone incursions around Taiwanese territory, backed by law enforcement and coast guard activity. In the scenario, the CCP leaked reports of upcoming military exercises, threatened to occupy offshore islands, bribed media officials, and used influence operations to promote surrender and social unrest. Simultaneously, the CCP used contracts in futures markets to short Taiwanese stocks, creating selling pressure and inciting large-scale capital withdrawals. The resulting depreciation of the New Taiwan Dollar triggered a real estate sell-off. Collapsing property prices and insufficient collateral spurred bank runs. (See Table 5.) Multiple Taiwanese players saw this as China’s preferred coercive strategy.

Table 5: China's Actions During the Gray Dawn Scenario

Covert Cyber Operations

Energy Sector: Disrupt power plants and the electricity grid, causing rolling blackouts.

Financial Sector: Disrupt banking operations, causing transaction delays and instability.

Communications: Target telecommunications infrastructure, causing internet outages and communication breakdowns.

Supply Chains: Disrupt logistics and supply chain management systems to create delays and shortages in key goods.

Economic Quarantines

Strategic Goods: Blockade strategic goods such as oil, natural gas, and essential raw materials, creating shortages.

Ports and Shipping: Use naval and coast guard vessels to intercept and delay commercial shipping to and from Taiwan.

Export Restrictions: Impose export restrictions on high-tech goods and components crucial to Taiwan's manufacturing sector.

Diplomatic Pressure: Use diplomatic channels to discourage other countries from trading with Taiwan.

Information Warfare

Disinformation Campaigns: Spread false information about government corruption, economic instability, and public safety issues through social media and controlled media outlets.

Deepfake Technology: Use deepfake videos and audio to create convincing but false narratives about key political figures and events.

Influence Operations: Leverage social media influencers and paid trolls to amplify divisive issues and create social unrest.

Hack-and-Leak: Dox government and media agencies to undermine public confidence.

The U.S. team assessed that the CCP's overt actions made it easier for Washington to justify using conventional military activity to respond. Washington could conduct short notice/no notice strait transits and reposition carrier strike groups while increasing readiness and scheduling high-level visits to Taiwan. The U.S. team assessed that its prior responses to long-term economic coercion and financial warfare (Long Walk) and cyber campaigns (Ghost in the Machine) required this overt military pressure to establish clear red lines. The U.S. team also recommended announcing a willingness to escort commercial ships to Taiwan to preclude CCP escalation beyond gray zone activity. The team discussed expanding this to include coalition escorts of commercial traffic.

The U.S. team doubled down on using administrative measures and expanded inspection regimes. The U.S. team saw these measures as another direct warning to CCP leadership given the limited short-term options to bolster Taiwanese resilience. In short, the U.S. team saw its role as stopping the crisis from escalating while Taiwan invested in decreasing its vulnerability and increasing its resilience. Neither Taipei nor Washington could stop Beijing's coercion, but they could alter its expected benefits by signaling escalation risks and hastening Taiwan's

ability to absorb and adapt. As part of this effort, the U.S. team stressed the importance of Taiwan expanding public messaging to counter Beijing's malign cyber-enabled influence operations.

The U.S. team also discussed the need for more dynamic interagency playbooks for addressing complex crises short of war so that Washington can combine military and non-military actions — for example, synchronizing efforts to prevent bank runs and the collapse of financial markets with military signaling, defensive cyber operations, and revealing intelligence to expose Beijing. According to the U.S. team, the playbook itself should have tailorable, pre-planned coercive measures — similar to flexible deterrent options/flexible response options in military planning — that the president could approve during a crisis. The menu should focus on developing competitive strategy instruments that target key sectors in China. Building this menu, clearing options with legal and agency-level review, and rehearsing them in advance would be critical for Washington to support Taiwan in a timely manner during a crisis.

The Taiwan team focused on societal resilience. The team emphasized that the size of Taiwan's foreign reserves and the robust insurance industry's offshore holdings gave the country more flexibility than most realized. Expanding currency swap provisions and financial system stress tests and encouraging companies to leave China would make Taiwan even more resilient. Business officials from Taiwan noted that major firms have continuity plans and actively discuss with their boards the risks of CCP coercion. Requiring large firms to undergo continuity planning and risk management training at organizations like TABF could enhance these measures. Players noted, however, that the real challenge resided at the consumer level. Citizens would struggle if panic caused bank runs or cyberattacks disabled ATMs.

Time was a key variable. Most economic penalties take time to change adversary decision-making. One Taiwanese banker noted that by the time U.S. regulatory agencies like the Securities and Exchange Commission launched investigations into U.S.-listed Chinese firms, the crisis would likely be the new normal. Thus, Taiwan players concluded that even their most powerful partner — the United States — had a limited ability to counter political warfare and gray zone activity.

Outside of the economic sphere, the Taiwanese team discussed expanding cyber protection teams. While the country is producing technical talent sufficient to defend its networks, the question is how best to coordinate across the public and private sectors and with international actors, including Five Eyes countries and large multinational firms.

The group sought to explore more creative roles for the private sector to counter gray zone activity, including using “contractor owned, contractor-operated” models to, at a minimum, document Chinese coercion but possibly also to complicate the CCP's decision-making process. The U.S. and Taiwan teams were divided on how far Taiwan could take this before China used it as a pretext to respond.

Players also discuss how Washington could help connect Taiwan and other free nations. One Taiwan player suggested a defining speech by U.S. leaders outlining the importance of winning a new Cold War and linking European security concerns to the Asia-Pacific and Taiwan.

The teams discussed using civil society and international fora to discuss gray zone tactics by authoritarian states. Civil society can help coordinate non-governmental responses to gray zone activity, while working through the G7 or with Five Eyes countries would offer Taiwan a chance to engage diplomatically despite recognition challenges.

Finally, the Taiwan team discussed building and rehearsing Taiwan’s own interagency crisis playbook. The team noted that even the process of creating the playbook would likely have a positive signaling effect on Beijing.

The China team noted that Taiwanese financial resilience would complicate Chinese decision-making but that the U.S. use of conventional military forces would not. While overt Taiwanese military measures only burned readiness, gave the CCP a justification for more provocative behavior, and risked compounding public panic, the China team urged Taiwan to consider employing a mix of its own gray zone operations and covert action to complicate China’s objectives. In particular, the China team noted the benefits of leaking information to amplify uncertainty in Beijing, including information, real or imagined, about robust U.S. training and weapons assistance to Taiwanese forces.

The China team discussed how messaging by the Taiwanese government about resilience planning could actually complicate decision-making in Beijing. A CCP assessment that Taiwan could withstand coercion would spark internal debates about the efficacy of its own capabilities given the CCP’s desire to establish new baselines rather than seek a *fait accompli*. American, European, or other international infrastructure protection, cyber detection, and resilience support for Taiwan would compound these concerns. The China team believed Beijing would be concerned that Taiwan’s ability to not just outlast, but potentially thrive, in the face of Chinese gray zone coercion could strengthen Taiwanese confidence and demonstrate the limits of the CCP’s coercion.

In the second scenario, Joint Sword Shadow, the CCP combined cyber and economic coercion campaigns with an expanded, 90-day military exercise. Missile tests disrupted commercial traffic, and the exercise effectively blockaded major ports, limiting the flow of essential resources and reducing foreign trade. There were also reports that CCP hackers stole critical data and prepositioned malware in key institutions for future, coordinated disruptive cyberattacks. (See Table 6 for leading indicators the players discussed in this scenario.)

Table 6: Indicators the CCP is About to Launch a Large-Scale, Coordinated Economic Warfare Campaign in Conjunction With Military Exercises

Increased Military Activity: An uptick in large-scale military exercises near Taiwan, particularly those involving combined arms and joint operations. Cyber-Military Coordination: Simultaneous cyberattacks targeting critical infrastructure and financial systems coinciding with military maneuvers. Mobilization of Reserves: Mobilization of military reserves and state-owned enterprises for logistical support, indicating preparation for prolonged operations. Public Announcements: Announcements or state media reports highlighting the necessity of “defensive” economic measures and military readiness. Intensified Rhetoric: Hostile rhetoric from Chinese officials and state media, framing Taiwan as an economic and military threat. Economic Sanctions: Trade restrictions, tariffs, or embargoes targeting key Taiwanese industries as a precursor to broader actions.

In response to this scenario, players stressed the importance of diversifying Taiwan's energy sector. Without energy, the economy would grind to a halt, other critical infrastructure sectors would falter, and citizens would struggle with daily life. This led to a discussion about "quarantine proofing" Taiwan's reliance on LNG imports, including by negotiating new gas contracts with democratic states, purchasing more ships, and securing access to vessels unlikely to succumb to CCP pressure. One player pointed to the growing relationship between Qatar — a major LNG supplier to Taiwan — and the CCP.

Players noted that Taiwan needed to expand its storage capacity including by building floating LNG terminals for processing and storage. The United States and key allies like Japan could supplement this by creating intermediate staging and storage areas. Players also discussed rehearsing convoy escorts to sustain imports.

These measures would not only increase resilience but also signal resolve to the CCP. Through routine convoy operations exercises that build interoperability, Washington and Taipei could signal that the United States and its partners have the capacity to challenge a blockade. The larger the coalition escorting LNG (and other major resources) to Taiwan, the stronger the deterrent signal. One player noted that showing how the crisis affects shipping premiums and regional trade could help recruit states that do not recognize Taiwan. Framing the convoys as a humanitarian response would also amplify negative perceptions of the CCP. Players also discussed reminding China that its shipping insurance premiums were also going up.

The Taiwan team approached this crisis as an effort by Beijing to force serious political concessions from Taipei. The team reiterated the importance of accelerating its business community's departure from China through a mixture of tax policy, credits, and subsidies, possibly applying lessons from Japan's experience. In 2005, the Japanese government proposed the China Plus One strategy, which encouraged firms to hedge by investing in another state when making investments in China. Over the next 20 years, the government incentivized decoupling and promoted alternative supply chains. Starting in 2020, these measures included manufacturing subsidies totaling over \$3 billion in the first round alone. Parallel to industrial subsidies, the Ministry of Economy, Trade and Industry set up reshoring programs, while the External Trade Organization designed programs to reorient other supply chains to ASEAN nations, India, and Bangladesh. Between 2020 and 2022, this effort resulted in 439 subsidized onshoring and 104 nearshoring projects.

For the U.S. team, China's use of conventional military assets counterintuitively made it easier to respond and legitimized the use of more aggressive instruments to support U.S. companies seeking to leave China. The U.S. team stressed the need for a plan for rapid decoupling, using administrative procedures to deny key resources (like silver powder) to China, and revoking China's most favored nation status. Both the U.S. and Taiwan teams assessed that the more the measures hit Beijing's economic prospects, the more likely Xi would be to avoid a direct confrontation.

The Taiwan team warned that deploying forces to signal resolve would burn readiness, while prematurely mobilizing reservists could trigger widespread panic and play into China's larger plan to use fear and uncertainty to erode societal cohesion. The discussion thus turned to indirect methods for confronting China including contracting intelligence, surveillance, and reconnaissance capabilities and using small drones to monitor and frustrate CCP activity. Some players also recommended using decoys and limited electronic warfare to disrupt CCP operations.

Players debated whether cyberspace offered Taiwan a way to match Beijing's escalation without triggering a larger conflict. Applying lessons from other democracies under siege, including Ukraine and Israel, players discussed defensive, and even offensive, cyber operations. While less discussed, the players noted that the United States and Europe could increase Taiwan's cyber capacity through cross-sector, cross-national exercises and improved information sharing.

While military means dominated the conversation, the Taiwan team also reaffirmed the idea of local community resilient hubs. One participant outlined an idea of converting underground parking facilities into local centers for power storage (i.e., large battery) and civil defense, including medical triage and assembling.

Teams discussed complementing these hubs with digital forms of resilience. Israel has a robust notification system to warn citizens of incoming rockets and missile attacks. The Ukrainian system that provides updates on missile warnings also helps the government coordinate emergency response and reconstruction and provides a frictionless system for identity cards and business permits. Citizens are now even using it to report Russian troop movements.

Taiwan has the resources to create a digital identity system backed up with a secure, cloud architecture. Ukraine's experience shepherding its critical data to cloud platforms hosted outside the country may prove illustrative. Digital apps could also help identify manipulation and cyber events, expanding Taiwan's existing counter-influence operations capabilities. The more Taipei links these digital efforts with robust investments in civil defense, the more effective the signaling will be.

The China team noted that both the U.S. and Taiwan teams had difficulties differentiating between the Gray Dawn and Joint Sword scenarios. In a real-world setting, Beijing could capitalize on this uncertainty to dial up or down its planned moves. The China team believed Beijing would seek to heavily influence, if not outright control, the information environment and questioned whether Taiwan had the means or political will to counter this objective.

The China team noted time was both its enemy and its friend. Taiwan would remain extremely vulnerable during the long time it would take for Washington and Taipei to operationalize many of the proposed countermeasures. Yet the longer Taiwan held out, the more likely that the United States and like-minded partners could raise the diplomatic stakes and pressure China into a face-saving off-ramp.

TOP RECOMMENDATIONS

During the TTX, within weeks of escalating CCP pressure, Taiwan faced significant societal issues, stemming in part from energy and communications insecurity. China's win-without-fighting strategy is predicated on these societal issues forcing Taipei to capitulate. By improving Taiwan's resilience — and the resilience of all democracies — to withstand authoritarian aggression, the United States and its partners can undermine China's ability to launch coercive campaigns in the first place.

1 - STEPS TAIWAN CAN TAKE TO IMPROVE ITS RESILIENCE

Taiwan faces a formidable challenge. Beijing's strategy is multifaceted, encompassing not only economic pressure but also targeted cyberattacks, disruptions to critical infrastructure, and efforts to diplomatically isolate Taiwan. The solutions are complex, often costly, and logistically challenging. Implementing them will demand significant regulatory adjustments, political will, robust public-private partnerships, and international support.

Taiwan's strategy must be comprehensive. The economic components should focus on three core objectives: reducing exposure to Chinese financial influence; bolstering external linkages with global markets; and proactively communicating the strength and security of Taiwan's banking sector to bolster confidence and preparedness before a crisis. Taipei must also improve cyber resilience — particularly its critical infrastructure and communications networks — and societal resilience.

Capital and Financial Resilience

Beijing seeks to undermine Taiwan's economic sovereignty by threatening capital held in Hong Kong and the mainland and targeting the financial mechanisms that link Taiwan to these regions. China also aims to exploit domestic vulnerabilities within Taiwan, incite societal panic, erode investor confidence, and destabilize markets. To counter these threats, Taiwan must secure capital repatriation, protect its financial infrastructure, and strengthen global market connections.

- *Secure Capital Repatriation and Financial Mechanisms:* Taiwan must reduce its exposure to Chinese influence by ensuring the safe repatriation of Taiwanese capital from Hong Kong and the mainland. Stress-testing financial institutions against sudden Chinese restrictions is essential. Taiwan should implement regulatory reforms, including tax incentives, to streamline capital transfers and safeguard assets. Given China's control over cross-strait financial channels, Taiwan should explore rerouting capital through third countries.
- *Establish a U.S.-Based Mirror Stock Exchange:* Creating a mirror stock exchange in the United States would protect Taiwanese companies and markets from Chinese cyberattacks or disruptions. Cloud-based hosting could minimize the stock market's downtime, thereby protecting investor confidence.
- *Explore Establishing a Currency Swap Mechanism:* Establishing a currency swap agreement with the United States could help stabilize the New Taiwan Dollar in the face of sell-offs during a crisis, protect it from market volatility driven by Chinese actions, ensure liquidity, and reinforce investor confidence. An agreement would also have a trickle-down effect, providing banks with dollars to promote stability.
- *Enhance Public-Private Financial Partnerships:* By involving financial institutions in stress testing and crisis response planning, Taiwan can leverage private expertise and resources to strengthen its financial defenses. These partnerships help align public and private efforts to safeguard the economy. Proactive communication between the government and the public also helps maintain confidence in Taiwan's banking sector.

Energy Resilience

Energy resilience is essential for maintaining Taiwan's stability across all sectors, from industrial production to financial infrastructure. By strengthening and diversifying its energy infrastructure, Taiwan can better withstand and quickly recover from disruptions.

- *Promote Citizen-Level Energy Resilience:* Taiwan should implement a mix of taxes and grants to encourage the widespread adoption of solar panels, home battery systems, and geothermal energy solutions at the household level. This can not only reduce the burden on the grid and create a more distributed, robust network but also foster citizen-level resilience, ensuring that Taiwan can better endure potential disruptions.
- *Diversify LNG Storage and Supply Chains:* Expanding Taiwan's LNG storage capacity, including floating storage, and its shipping fleet is critical. Taiwan should deepen its energy partnerships, particularly with Australia, to diversify LNG imports and reduce reliance on pro-China countries like Qatar. Japan and the Philippines can also build LNG storage in their countries while the United States and other partners improve terminals, ports, and storage facilities on Taiwan's east coast. Additionally, Taiwan should explore strategies to reflag LNG vessels during hostilities to deter China from targeting these vessels.
- *Reignite Nuclear Power for Resilience:* Taiwan should build electric grid resilience by expanding stockpiles of spare parts and diversifying generation sources. In addition to expanding wind and geothermal production, Taiwan should reconsider its nuclear power policy. Small modular reactors (SMRs), including ship-based SMRs,

may be a low-cost option. China is less likely to launch cyberattacks on SMRs for fear of cascading effects. Additionally, Taiwan should consider restarting its decommissioned nuclear reactors, which could provide an immediate and stable source of energy. These options, however, may be politically fraught given that the government just completed denuclearization efforts.

Industrial and Market Diversification

Taiwan's reliance on China as a primary trading partner and manufacturing base exposes it to significant risks. Taiwan must diversify its industrial base and expand into new markets. By strategically relocating industries, developing new market opportunities, and fostering international partnerships, Taiwan can build a more robust economy that is less vulnerable.

- *Incentivize Industry Relocation from China:* Taiwan should offer incentives, such as tax breaks, low-interest loans, and subsidies, to encourage Taiwanese businesses to relocate from China to other countries. Southeast Asia, Japan, or Northern Mexico can serve as alternative manufacturing hubs, reducing dependency on China. Taiwan can also draw lessons from Japan's successful efforts to diversify production locations.
- *Develop a Mechanism for Evaluating New Market Opportunities:* Taiwan should establish a mechanism for evaluating and prioritizing new market opportunities based on economic growth, political stability, trade barriers, and the intensity of China's influence over the host government.
- *Foster International Partnerships to Counter Isolation:* Taiwan should deepen economic and trade partnerships, even if these engagements fall short of formal diplomatic recognition. By pursuing technological collaborations, strategic trade alliances, and participation in multilateral economic forums, Taiwan can strengthen its global presence, reinforce its role as a valuable and reliable partner, and counter China's efforts to isolate it.

Infrastructure and Communications Resilience

Taiwan's infrastructure and communication systems are vulnerable to cyberattacks and physical sabotage. China's strategy likely includes exploiting these vulnerabilities to isolate Taiwan, disrupt its economy, and erode public confidence. By investing in redundant systems, enhancing cybersecurity, and improving physical security, Taiwan can mitigate disruptions and maintain continuity of operations across key sectors.

- *Explore and Develop Redundant Communication Systems:* Taiwan should explore investing in satellite-based data systems and securing additional satellite communications capacity. Taiwan should also explore on-call cable-laying ships and creating a regional network of redundant communication cables. Collaboration with the United States and other partners can bolster these efforts.
- *Explore Data Storage Off-Island:* Learning from Estonia's Data Embassy program and Ukraine's efforts to move critical data out of the country at the start of Russia's full-scale invasion, Taiwan should consider a comprehensive, national cloud-based data back-up system to ensure continuity of government, communications, and the economy. Cloud-based backup systems off-island would also provide financial institutions with greater operational resilience.
- *Enhance Cybersecurity for Critical Infrastructure:* Taiwan must prioritize cybersecurity for financial institutions, energy, transportation, and communication networks. Developing a skilled cyber workforce will bolster defenses and support economic growth. Implementing advanced threat detection and stress testing will help protect against potential cyberattacks.

- *Secure and Modernize Physical Infrastructure:* Taiwan should modernize its physical infrastructure, including power grids, water systems, and transportation networks, to withstand cyber and physical attacks. Backup power and alternative supply routes will help ensure continued operation during crises.

Cyber Resilience

Cyberattacks allow the CCP to maximize impact while simultaneously maintaining plausible deniability and limiting international backlash. By exploiting vulnerabilities in Taiwan's critical infrastructure, China will attempt to instill fear and undermine confidence in the government. Taiwan faces cyber challenges to its critical infrastructure similar to those in the United States, and so it should be no surprise that many of the recommendations for Taiwan's cyber resilience mirror those being pursued in the United States.

- *Prioritize What Matters:* Taiwan should analyze and determine which critical infrastructure assets are most important and ensure that these entities receive improved access to threat information and network defense support. These benefits should also come with requirements to invest in cybersecurity, participate in continuity exercises, and maintain well-constructed recovery plans.
- *Build a Better Public-Private Collaboration:* Taiwan's government and private sector need a shared understanding of the threat. Taiwan should develop the capability to rapidly distribute threat information and advisories. Taipei should also develop sector-specific incident response and recovery plans and comprehensive training and exercise programs to improve mitigation and recovery capabilities.
- *Designate a Civilian Agency to Coordinate Critical Infrastructure Defenses:* Improving public-private collaboration requires a whole-of-government effort but also requires a single agency to own the mission. Taiwan should create a new (or task an existing) civilian agency to expand public-private partnerships and work with local governments.
- *Expand Defensive Cyber Capacity and Consider Building Offensive Capabilities:* Ukraine provides lessons for Taiwan on the importance of robust cyber defense. Taipei should create a more effective cyber workforce and establish partnerships with international technology and cybersecurity firms to protect the integrity of government and private sector networks. At the same time, Taiwan should consider developing an offensive cyber operations capability — something Ukraine did not have in February 2022 — to impose costs on China in cyberspace.

Societal Resilience

Taiwan's societal resilience is the center of gravity of the CCP's cyber-enabled economic coercion campaign. All the recommendations above are critical to societal resilience, but there are society-specific recommendations that Taiwan should consider as well.

- *Conduct a Resilience Assessment.* The Taiwanese government is reportedly establishing an economic and societal resilience task force to assess Taiwan's vulnerabilities and develop a comprehensive plan to address these gaps. This effort should include the private sector, which owns and operates some of the most important infrastructure under CCP assault.
- *Invest in Efforts to Counter CCP Malign Influence Operations:* Few countries are as experienced as Taiwan in dealing with persistent foreign cyber-enabled influence campaigns. Taiwan must maintain and expand these efforts.

- *Inform the Public About Resilience Efforts:* Societal resilience against economic pressure is a deterrent against CCP coercion. Taiwan needs robust public messaging about its ongoing resilience activities — including continuity planning by firms and government efforts — that reassures the public about the government’s efforts without triggering widespread panic.
- *Expand Reserve Capability and Capacity:* Taiwan’s military reserves can play a critical role in a military coercion or cyber-enabled economic coercion campaign. The reserves can help control infrastructure systems that have lost aspects of their automation, restore order, and support utilities. However, this will require a reorganization of the reserves.
- *Use Global Civil Society Groups to Complicate China’s Efforts:* Taiwan can leverage multilateral and global civil society organizations to complicate China’s cyber-enabled coercion and financial warfare. Proceedings can help draw attention to Chinese siege tactics and help drive consensus responses to gray zone activity.

2 - STEPS AMERICA AND ITS PARTNERS CAN TAKE TO IMPROVE TAIWAN’S RESILIENCE

The United States and key allies must help Taiwan improve its economic resilience, deter further CCP provocation, and respond to gray zone attacks. Many of the recommendations above require close collaboration with Washington and other partners. In addition, the United States should act unilaterally and take bilateral steps with Taiwan, and with a wide range of democratic allies and partners, to impose economic costs on China, improve Taiwan’s economic resilience, and strengthen Taiwan’s cyber capacity. Enhancing Taiwan’s resilience not only does not strain U.S. financial capabilities but actually makes it less likely Washington will need to deploy assets to help Taiwan overcome CCP coercion.

Economic Pressure on China

- *Develop Joint Escalation Playbooks to Counter CCP Coercion:* The United States should develop a playbook to check Chinese economic coercion and financial warfare. The United States should also encourage allied adoption of economic provisions that push back against the CCP’s non-market practices. The playbook should include options to punish China’s regulatory arbitrage; impose joint or complementary sanctions on state-owned entities that support or facilitate military actions against Taiwan; sanction civilian ships involved in maritime militia efforts; and engage with Japan and the Philippines on measures to secure trade lanes. This joint escalation playbook should impose significant costs up front lest China adapt to gradually increasing sanctions as Russia has done.
- *Combat Unfair Trade Practices:* Washington should operationalize tools to combat intellectual property theft and unfair trade practices, combining the Special 301 report (published annually by the U.S. trade representative) of countries engaging in intellectual property rights violations with sanctions mandated by the Protecting American Intellectual Property Act of 2022 on entities and individuals stealing trade secrets.
- *Expand Pro-Transparency and Human Rights Economic Initiatives:* Washington should consider increasing the scope and enforcement of the Uyghur Force Labor Prevention Act, particularly in response to an escalation of Chinese gray zone tactics or economic coercion. Washington should consider other financial and economic tools to promote transparency initiatives that counter China’s human rights violations, forced labor, environmental degradation, surveillance of dissidents, and anti-competitive practices.
- *Signal Capital Flight Risk:* The United States should signal to China the risk of private foreign capital exiting Hong Kong and the mainland in larger amounts if China escalates its economic coercion and financial warfare

campaign against Taiwan. U.S. policymakers may also want to signal to the markets that divestment would be prudent if China engages in more aggressive economic coercion.

- *Impose Export Restrictions on China:* Washington should be prepared to sever key U.S. exports to China. Washington should work with allies to analyze key intermediary components and materials that China needs and identify how to cut off supplies. Washington and its allies should expand restrictions on key precursors China needs for its Made in China 2025 initiative, like the silver powder required for solar panels.

Taiwan's Economic Resilience

- *A Bilateral Free Trade Agreement:* Washington should consider a bilateral free trade agreement between the United States and Taiwan and encourage other countries to do the same. Commerce is a critical substitute for traditional diplomacy given Taiwan's central role in the global economy.
- *Expand Co-Production and Ally-Shoring:* Through ally-shoring, the United States should expand co-production opportunities for Taiwanese industries, focusing on critical supplies that Taiwan currently sources from factories on the island or in mainland China. Taiwan should examine what industrial capacities it can offshore to more protected or resilient countries. Taiwan could also use the ally-shoring of critical emerging technologies as an inducement for greater economic ties with partner countries.
- *Support Taiwan's Inclusion in Multilateral Economic Fora:* The United States should include Taiwan in efforts to make all democratic economies more resilient against authoritarian influence. The United States should work with G7 finance ministers to build greater joint resilience against autocratic market manipulation and forge a plan to counter China's gray zone provocations. Washington should also promote Taiwan's inclusion in the International Monetary Fund, which would provide Taiwan access to the rainy-day fund should Beijing's actions cause a balance of payments problem.
- *Include Taiwanese Private Capital in Democracy-Led Development Initiatives:* To counter China's Belt and Road Initiative, democratic countries should unleash the power of private capital to support infrastructure and development in emerging markets. The United States should bring Taiwanese private capital into an allied consortium of private players, creating a pipeline of democracy-led projects that improves relations between Taiwan and potential partners in emerging markets.

Cyber Resilience

The United States has a robust cyber partner capacity-building program. It can provide cybersecurity support and guidance across a number of federal agencies.

- *Military Security Cooperation.* The fiscal year 2024 National Defense Authorization Act tasked the Pentagon with "cooperating on defensive military cybersecurity activities with the military forces of Taiwan." Specifically, Washington should work with Taiwan to: defend Taiwanese military networks, infrastructure, and systems; counter malicious cyber activity that has compromised these networks; leverage U.S. commercial and military cybersecurity technology and services to harden Taiwan's military and systems; and conduct cybersecurity training with Taiwan. Existing Defense Department efforts are still nascent but must be accelerated.
- *Provide Advice on Private-Public Collaboration:* The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has worked on several cyber resilience efforts that Taiwan is beginning to tackle. While CISA has not "solved" these problems in the United States, the agency's experiences are relevant to Taiwanese counterparts.

3 - STEPS THE UNITED STATES CAN TAKE TO IMPROVE RESPONSE TIMES OF DEMOCRACIES TO AUTHORITARIAN GRAY ZONE COERCION

Taiwan is not alone in its struggle against authoritarian coercion. Increasingly, dictators and despots are using the ambiguity of the gray zone, coercion short of war, and cyber operations to pressure free nations. This puts a premium on developing new tools to counter the authoritarian playbook. Democracies need options to balance escalation risks without ceding the initiative to despots. This requires a holistic approach, new ways of shortening the time for interagency processes to align with national security bureaucracies across multiple countries, and a recognition that the new Cold War will be won through societal resilience.

- *Develop an Interagency Playbook of Options to Counter China:* The U.S. government should develop a new interagency playbook with options for countering China in a crisis short of war. This playbook should cut across traditionally stove-piped authorities and develop responses that combine cyber, economic, military, legal, and diplomatic levers. Rather than being subject to the crisis of the moment, the playbook should have options that are pre-vetted and reviewed by agency counsels. Periodic crisis planning exercises should vet and refine playbook options. This pre-planning and rehearsing will reduce the time to respond to a crisis while also allowing a framework for long-term planning. This approach would ensure that senior U.S. officials have options they can execute rapidly if China attempts to change the status quo.
- *Increase Interoperability with Key Partners:* Alliances are a key U.S. asset. Washington should work to align its interagency playbook with expected allied and partner responses. The United States should exercise the playbook options with key partners and expand other exercises to increase interoperability. For example, Washington should engage in extensive cyber-crisis response planning with Japan and Taiwan, to include testing the ability to defend against a large-scale cyberattack. Exercises should also increase the ability of states to work together in high-pressure situations that emerge from gray zone competition. For example, the United States could conduct convoy exercises with Japan, Taiwan, and others to demonstrate and expand the ability to escort commercial shipping during a crisis.
- *Explore Novel, Indirect Ways to Support Partners Under Siege:* The United States should explore novel, indirect ways of supporting a partner under siege. This includes working with partners to develop mechanisms to utilize private sector capabilities. This can help Taiwan avoid a readiness trap where it responds to every hostile act in the gray zone. For decades, commercially owned, commercially operated contract vehicles have supported intelligence collection and logistics, offering risk- and cost-reducing ways of countering gray zone activity. For Taiwan, increasing maritime and cyber domain awareness helps reduce the CCP's coercive potential. The better the intelligence, the more calibrated Taiwan, the United States, and partner nations can be. The United States should work with Taiwan and other key partners to explore a common vehicle to fund counter-gray zone activity, including surveillance, cyber defense, and even air-to-air refueling and logistics. This vehicle would make defense dollars go further and bring in private sector innovation.

CONCLUSION

The tabletop exercise confirmed that an integrated cyber and economic warfare campaign is a significant risk for Taiwan. The limited diplomatic, economic, and military cost to the CCP — especially compared to the blockade or cross-strait invasion scenarios — means that China can turn up and down the pressure at will. Most concerning, the compounding financial and psychological effects impose escalating political pressure on Taipei without crossing any U.S. redlines.

The answer for Taiwan is to increase economic and societal resilience. Extending the island's ability to withstand CCP coercion from days and weeks to months and years not only provides time for America to impose countermeasures and corral reluctant democratic allies but also decreases the likelihood of CCP aggression in the first place. Building this resilience itself takes time and coordination across central and local governments, the private sector, and civil society. Identifying and mitigating complex interdependencies in critical infrastructures and deploying novel technologies to enhance digital resilience must happen before, not during, a crisis.

Taiwan is not alone in its struggle to combat authoritarian coercion. Democracies around the world are under siege by an increasingly aggressive and coordinated axis of authoritarian states. The United States and its allies need pre-planned, dynamic, coordinated, and rehearsed playbooks with creative options for countering China in the Indo-Pacific, Russia in Eastern Europe, Iran in the Middle East, and their fellow travelers around the world.

APPENDICES

MENU OF CCP ECONOMIC COERCION AND FINANCIAL WARFARE OPTIONS

The tables below provide an overview of the options players used to make their assessments about possible CCP activity.

The Long Walk

A. Lawfare Comes to the Firm. The CCP charges the top 10 Taiwanese banks in China with tax evasion and violations of other major laws, suspending their operations and freezing their assets. Simultaneously, false claims spread on social media that these banks were causing financial difficulties for parent companies. Stocks plummet.
B. Lawfare Targeting Executives. The CCP charges more than 10 major Taiwanese companies with tax evasion and/or environmental pollution. China uses the charges as a pretext to restrict the personal freedom of the CEOs and to freeze their assets, leading to a wave of bad debts for banks. Negative comments about Taiwan from influencers and business leaders surge. Stock prices plummet, and capital exits Taiwan en masse, resulting in a sharp depreciation of the New Taiwan Dollar.
C. Market Confidence Manipulation. China bribes international investors and/or credit rating agencies to release news about the financial difficulties of Taiwanese insurance companies, leading investors to sell off stocks and customers to cancel policies, resulting in liquidity problems for insurance companies.
D. Trade Manipulation. China requires Taiwanese goods imported into China to be labeled as “China Taiwan” or face bans. Simultaneously, the CCP bans exports of Chinese goods to Taiwan, causing shortages. The Taiwanese government faces calls from business groups and others to acquiesce.
E. Resource Restrictions. China bans rare earth materials exports to Taiwan while demanding Japanese companies cease exporting semiconductor chemical materials to Taiwan or face procurement stoppages. The CCP also halts water supplies to Kinmen during its dry season.
F. Market Pressure. China demands foreign investors withdraw from Taiwanese stocks or face restrictions on their operations, causing selling pressure and loss of investor confidence.
G. Enhanced Bureaucracy. China requires Taiwanese businesses remitting funds back to Taiwan to obtain various approvals, complicating the process of ending and liquidating their operations in China.
H. Financial System Fragmentation I. China restricts Taiwanese banks from using China’s transfer systems, preventing these banks from providing financial services to Taiwanese businesses.
I. Financial System Fragmentation II. China limits remittances between Taiwan and China. Profits earned by Taiwanese businesses in China cannot be transferred back to Taiwan, and businesses in China cannot access financial support from Taiwan.
J. Credits and Liquidity Manipulation. China instigates public distrust to cause bank runs and insurance policy cancellations, creating liquidity crises for Taiwanese banks and insurance companies.
K. Currency Manipulation. China uses domestic and international leverage to attack Taiwan’s foreign exchange market, causing the devaluation of the New Taiwan Dollar and capital outflows.
L. Strategic Divestment. China threatens and entices foreign companies with critical technologies in semiconductors, chemical materials, rare earths, and electric vehicle batteries to withdraw investments from Taiwan and cease providing related patents to Taiwanese industries.
M. Enhanced Sanctions II. China imposes sanctions on Taiwanese industries, forcing partners to stop supplying key technologies, raw materials, or products and to impose high tariffs on imports from Taiwan.
N. Elite Capture. China buys off Taiwanese elites, including business leaders, celebrities, and public officials, to influence public opinion in favor of China or to promote policies that weaken Taiwan and benefit China.

The Ghost in the Machine

A. Energy Infrastructure. The CCP launches cyberattacks on Taiwan's power distribution system, causing outages in science/industrial parks and interruptions in traffic signal systems. The attack escalates into an electricity crisis. The CCP uses deepfakes to fabricate a video of Morris Chang criticizing the government to further catalyze public dissatisfaction and panic.
B. Banking System. The CCP launches cyberattacks that paralyze the Taiwan central bank's real-time gross settlement system, causing interruptions in inter-company fund transfers and chaos in stock market settlements. The CCP uses deepfakes to fabricate videos of financial experts exaggerating the severity and claiming that people's savings are gone, prompting social unrest.
C. Financial Sector. The CCP hacks the Taiwan Stock Exchange, Futures Exchange, or Taiwan Depository & Clearing Corporation systems, causing account discrepancies or preventing normal trading and disrupting the capital market order. The CCP compounds the cyberattack by using social media bots to spread rumors that personal transaction data has been destroyed with no recoverable backups.
D. SWIFT. The CCP uses cyber intrusions to compromise major Taiwanese banks' SWIFT systems. The attacks result in stolen money. Simultaneously, the CCP infiltrates media outlets and publishes fake news exaggerating the severity, creating panic, a stock market crash, and a bank run.
E. ATMs. The CCP hacks major Taiwanese bank ATMs to dispense money automatically, using social media to spread rumors that bank data has been destroyed, with no recoverable backups. The attacks create widespread panic, triggering a stock market crash and a bank run.
F. Depositor Deception. The CCP hacks major Taiwanese banks' systems to alter customer deposit data and exploits the manipulation using videos on social media to cause public panic and a bank run.
G. Customer Leaks. CCP-affiliated APTs steal customer financial customer data and personal information from Chunghwa Telecom's Internet Data Center and release the information online, causing a widespread breakdown in trust.
H. Manufacturing and Services. CCP cyberattacks disrupt major Taiwanese firms, impacting their ability to operate and pay employees, suppliers, and taxes in a timely manner.
I. Ransomware. Chinese hackers escalate ransomware attacks targeting Taiwanese citizens to trigger financial disruption and a loss of confidence in the government.
J. Data and Communication. China destroys data in Taiwan's data centers, such as those of Chunghwa Telecom and Far EasTone, undermining public confidence in the financial system and government.
K. Digital Subversion. China uses online tools for public opinion attacks, including fake social media accounts, to undermine Taiwan's government, financial markets, and society, eroding public confidence in Taiwan's financial market while creating an impression of dependency on China.
L. Deep Fakes. China conducts deepfake attacks, fabricating false statements by government officials, social opinion leaders, or business leaders about Taiwan's financial market, damaging trust in the financial market.
M. Sophisticated Social Engineering. China conducts social engineering attacks on Taiwan's financial personnel, infiltrating financial institutions to disrupt internal operations or steal important data.
N. Supply Chain Disruption. China uses cyber means to alter product specification information between supply chain partners, causing downstream companies to use incorrect materials or components, resulting in product quality issues.

DATA ANALYSIS

This section analyzes how individual players rated 14 CCP coercive measures included in the following appendix. Players assessed the severity of China's move — from 1 to 10 — based on whether the measure changes the decision-making calculus in Taiwan (overall coercion); how vulnerable Taiwan is to the measure today (current vulnerability); if Taiwan can withstand and/or rapidly recover (current resiliency); if it compels Taiwanese political officials to act in the short term (political pressure); and if the effect could cascade beyond Taiwan's borders (spillover risk). This system allows a more granular analysis of how players assessed economic coercion and financial warfare. The findings are consistent with the general observations outlined in the main body of this report. The tables below are the average scores.

The Long Walk

	COERCION	VULNERABILITY	RESILIENCE	POLITICAL PRESSURE	SPILLOVER RISK	VUL-RES (VR)#
<i>*Lawfare Firm</i>	5.6	5.4	5.3	6.6	4.75	0.1
<i>+Lawfare Executives</i>	5.9	6.6	5.8	6.9	4.5	0.9
<i>^Market Confidence Manipulation</i>	4.4	4.1	6.6	5.3	3.875	-2.5
<i>^Trade Manipulation</i>	6.6	6.3	4.8	7.4	5.625	1.5
<i>Resource Restrictions</i>	6.0	6.3	4.9	6.9	5.5	1.4
<i>Market Pressure</i>	5.3	5.4	5.3	5.5	4.875	0.1
<i>*Enhanced Bureaucracy</i>	4.6	6.4	4.4	6.1	4.125	2.0
<i>Financial Fragment I</i>	5.0	5.6	5.4	5.6	4.125	0.3
<i>^Financial Fragment II</i>	6.1	7.0	4.1	6.8	4.875	2.9
<i>Credits and Liquidity Manipulation</i>	5.1	5.0	5.9	5.8	4.75	-0.9
<i>+Currency Manipulation</i>	4.8	4.9	5.6	5.6	4.125	-0.8
<i>Strategic Divestment</i>	6.4	5.6	5.8	6.6	5.875	-0.1
<i>Enhanced Sanctions II</i>	5.6	5.9	4.8	5.3	4.875	1.1
<i>+*Elite Capture</i>	5.0	4.6	5.5	5.3	2.875	-0.9
<i>MEAN</i>	5.5	5.6	5.3	6.1	4.625	
+ = U.S. team preference * = Taiwan team preference ^ = China team preference # This score compares the assessed vulnerability of Taiwan to the coercive measure to the degree to which society can absorb the blow and rapidly reconstitute. A higher score implies Taiwan would struggle to stop the attack and recover, creating a new coercive baseline.						

In the Long Walk, individuals rated the most coercive options as trade manipulation (6.6) given the potential to disrupt complex supply chains, followed by strategic divestment (6.4) and measures the PRC could take to fragment the financial system through limiting the free flow of funds from China to Taiwan (6.1). Players were least concerned about market manipulation (4.4), owing to the strength of Taiwan's banking and finance sector.

Players assessed that Taiwan was most vulnerable to administrative measures (7.0) limiting financial flows from China to Taiwan (financial fragmentation II), followed by lawfare targeting executives (6.6) and enhanced bureaucracy targeting remittances (6.4). Players also assessed Taiwan to be least resilient when confronted with enhanced bureaucracy (4.4) and financial fragmentation II (4.1). The U.S. and Taiwan teams' preferences during the scenarios for using administrative and bureaucratic measures over trade manipulation indicate players' focus on vulnerability and resilience rather than coercive leverage.

Players assessed that Taiwan would experience the most political pressure from trade manipulation (7.4), followed by lawfare measures targeting executives (6.9) and resource restrictions (6.9). Forms of lawfare were prominent in both the U.S. and China team recommendations and reflected how China could adopt low-cost coercive measures.

Finally, players assessed that strategic divestment (5.9) and trade manipulation (5.6) were the most likely to affect the regional, if not global, economy. China could prompt foreign firms to withdraw investments from Taiwan, threatening or enticing those with critical technologies in semiconductors, chemical materials, rare earths, and electric vehicle batteries. This pressure could extend to intellectual property, with China also demanding that companies cease providing related patents to Taiwanese industries. When combined with efforts to change the flow of imports and exports, these coercive measures would have an impact on global supply chains.

The Ghost in the Machine

	COERCION	VULNERABILITY	RESILIENCE	POLITICAL PRESSURE	SPILLOVER RISK	VUL-RES (VR)
+*^Energy Infrastructure	7.4	7.0	4.1	7.4	4.9	2.9
+*^Banking System	7.1	5.5	5.9	6.8	5.5	-0.4
*^Financial Sector	7.5	6.5	6.1	7.5	6.1	0.4
SWIFT	7.5	6.1	5.8	7.5	5.8	0.3
ATM	7.0	5.1	6.4	7.4	5.0	-1.3
Depositor Deception	6.9	5.6	5.5	7.4	5.0	0.1
Customer Leaks	5.6	6.0	6.0	5.4	3.5	0
Manufacturing and Services	6.8	6.0	5.4	6.9	5.1	0.6
Ransomware	6.4	5.9	4.6	6.8	4.3	1.3
Data and Communication	6.6	6.6	5.0	7.4	5.4	1.6
Digital Subversion	6.0	6.3	6.0	5.6	3.8	0.3
Deep Fakes	5.5	6.0	5.6	5.9	3.9	0.4
Sophisticated Social Engineering	5.0	6.0	5.4	6.0	3.6	0.6
+Supply Chain Disruption	6.0	5.8	5.5	6.0	5.4	0.3
MEAN	6.5	6.0	5.5	6.7	4.8	2.9
+ = U.S. team preference * = Taiwan team preference ^ = China team preference						

In Ghost in the Machine, individuals rated the most coercive options as measures targeting payment systems (SWIFT [7.5] and Financial Sector [7.5]), followed by energy infrastructure (7.4). These individual estimates matched the group consensus. Players assessed that cyber-enabled economic and financial warfare was most coercive when it turned off the lights and affected the ability of citizens and businesses to access digital payment systems. The combination had the potential, outlined in group discussions, to produce panic buying, leading to price inflation and fear that China could exploit.

During discussions, the Taiwan team was confident that the country was fielding a cyber workforce capable of defending its banking and financial services. They were not as confident about the energy sector. The convergence of group and individual estimates suggests a need to explore cross-sector stress testing and cyber exercises.

This pattern extended to assessments of vulnerability. Players assessed that energy infrastructure was the most vulnerable (7.0), followed by digital and communication (6.6) and the financial sector (6.5).

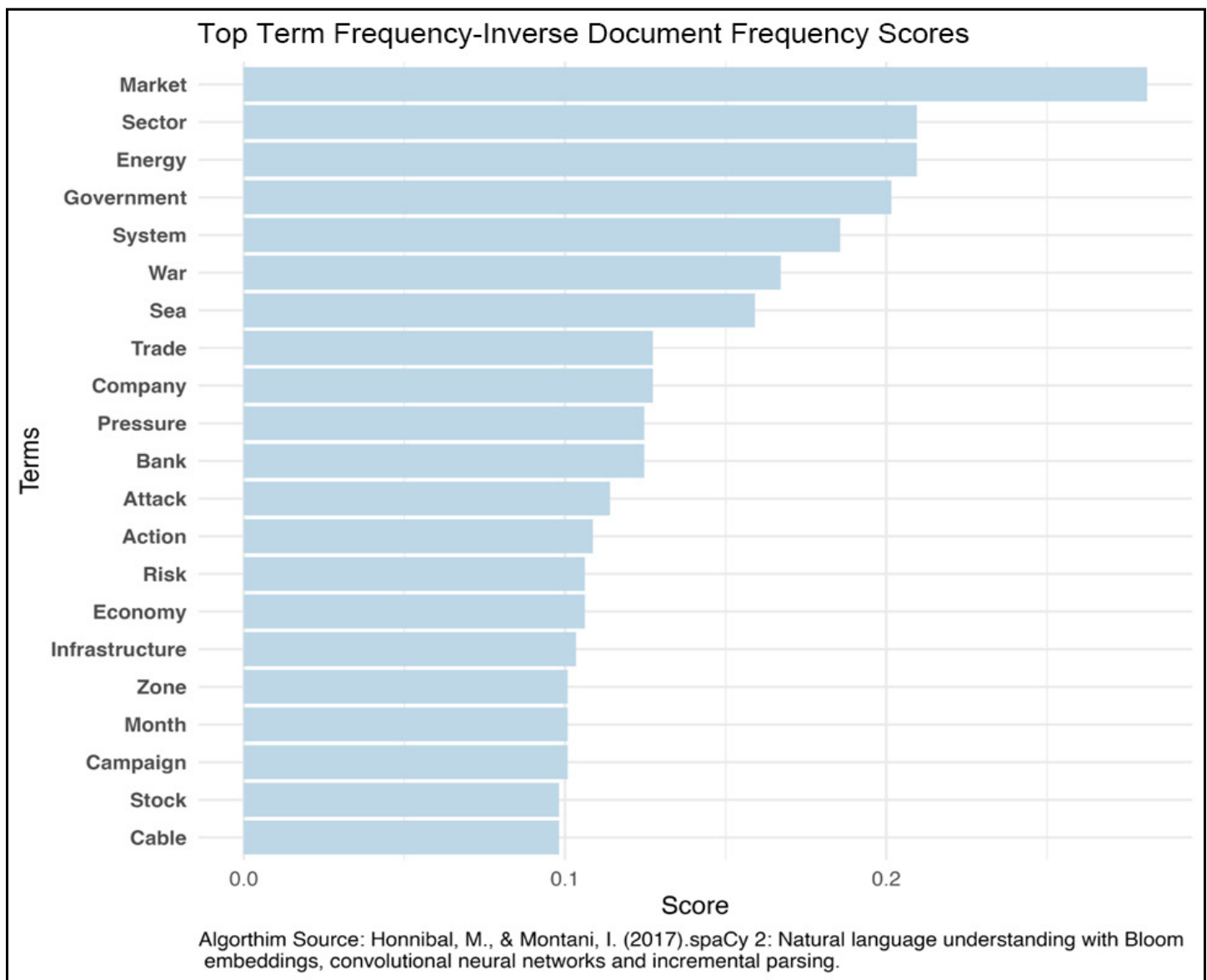
There were also key interdependencies that emerged during group discussions. Risks to energy infrastructure and the ease with which Beijing could conduct a digital blockade compound concerns about the vulnerability of the financial system. Both the Taiwan team and the China team discussed a mix of cutting undersea cables alongside cyberattacks designed to overload transformers and take major telecom providers offline.

Concerns over cyberattacks on payment systems and the energy sector carried into individual player assessments of political pressure. Players rated cyberattacks against financial services and payment systems (7.5) and energy infrastructure (7.4) the highest. Players also saw this as extending to complex attacks designed to take major indexes — from stock to foreign exchange — offline while spreading propaganda to further undermine investor confidence.

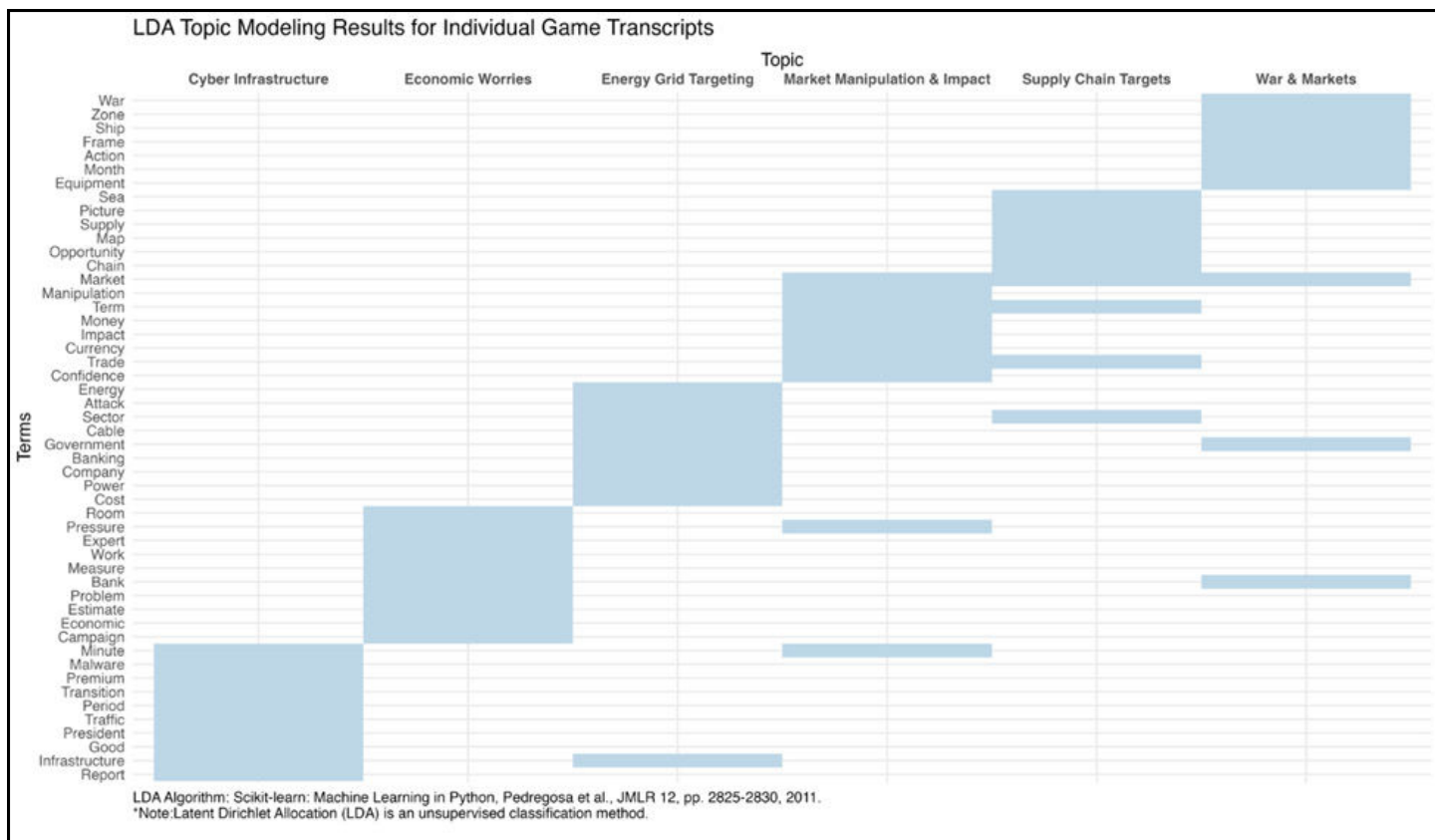
Lastly, players assessed that complex cyberattacks against the financial system (6.1) were most likely to cause spillover effects. Players were generally concerned with how a major attack could not only undermine confidence in Taiwan but also spread through the region. Multiple participants referenced historical precedents for the interconnectedness of markets in the Asia-Pacific.

NATURAL LANGUAGE PROCESSING

The research team used translated text from audio recordings to analyze the collective dialogue across the TTX. The team used spaCy as a core natural language processing (NLP) library and cleaned transcripts using Custom Regex Filtering to ensure the analysis focused on the most relevant content. The team then conducted Term Frequency-Inverse Document Frequency (TF-IDF) Analysis and Latent Dirichlet Allocation (LDA) Analysis. TF-IDF scores nouns to identify the most common topics, using the scikit-learn library, a common NLP resource. LDA is a form of topic modeling designed to uncover underlying themes within transcript texts. The graphs below illustrate the results and discuss the findings.



The most frequent nouns reflect the focus on economic coercion and financial warfare. The frequency of the term “market” reflects both discussions about negative market impacts as well as discussions about how China could manipulate markets. The frequency of the terms “sector,” “trade,” “company,” “pressure,” “bank,” and “stock” reflects an extension of concepts about economic coercion and aligns closely to the China team’s objective of targeting critical sectors and infrastructure to create immediate and significant disruptions and then using economic instability and public discontent to force political changes and concessions. Finally, the frequency of the words “energy,” “infrastructure,” and “cable” reflects a recurrent theme about the vulnerability of Taiwan’s critical infrastructure. The distribution of language across individual players thus matched the sentiments observed by the TTX facilitators.



Topic modeling confirmed the observations based on analyzing noun frequency. The discussions focused on economic worries and market manipulation along with infrastructure vulnerabilities related to cyberattacks, energy grids, and supply chains.

LOGIC TEST

The TTX used a series of escalating scenarios. To test whether or not coercive pressure increased across scenarios, the researchers performed a logic test, analyzing paired sample mean T-Tests (one-tailed) to compare the average coercive pressure scores by player across treatments. The results below compare 1) Long Walk and Sword Shadow; 2) Long Walk and Ghost in the Machine; and 3) Gray Dawn and Sword Shadow. The desired player response framework (i.e., experiencing escalation as they develop their policy options) is logical and consistent if the following conditions are met at a $P < .05$ level. Sword Shadow — the most escalatory scenario — had a higher average coercion score than Long Walk (the lowest) and Gray Dawn. Ghost in the Machine had a higher average coercion score than Long Walk. As seen in the tables below these conditions were met. The logic test confirmed the TTX players were indeed reacting to increased pressure across the treatments, allowing the research team to study economic coercion and financial warfare under different conditions.

t-Test: Paired Two Sample for Means (Coercion)

	<i>Long Walk</i>	<i>Sword Shadow</i>
Mean	5.455357	8.9375
Variance	0.463861	0.4625
Observations	16	16
Pearson Correlation	-0.22232	
Hypothesized Mean Difference	0	
Df	15	
t Stat	-13.0895	
P(T<=t) one-tail	6.53E-10	
t Critical one-tail	1.75305	

	<i>Long Walk</i>	<i>Ghost in the Machine</i>
Mean	5.455357	6.517857
Variance	0.463861	0.541156
Observations	16	16
Pearson Correlation	0.574678	
Hypothesized Mean Difference	0	
Df	15	
t Stat	-6.48748	
P(T<=t) one-tail	5.13E-06	
t Critical one-tail	1.75305	

	<i>Gray Dawn</i>	<i>Sword Shadow</i>
Mean	8.375	8.9375
Variance	1.05	0.4625
Observations	16	16
Pearson Correlation	0.035875	
Hypothesized Mean Difference	0	
Df	15	
t Stat	-1.86052	
P(T<=t) one-tail	0.041265	
t Critical one-tail	1.75305	

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

FDD's Center on Economics and Financial Power

FDD's Center on Economic and Financial Power (CEFP) studies national economic security, with a focus on how the United States can leverage its economic and financial power to achieve its national security objectives. CEFP promotes greater understanding of how the U.S. government can best employ its economic and financial authorities to counter its adversaries.

FDD's China Program

Leveraging the full scope of economic, financial, military, political, cyber, and technology tools, FDD's China Program exposes and challenges the wide-ranging threats posed by the Chinese Communist Party. FDD's China team includes experts with Chinese-language skills, data-driven mining capabilities to examine Chinese language sources, and experience in government, intelligence, the military, and the technology sector.

Craig Singleton is a senior fellow at FDD, where he also serves as senior director of FDD's China program. He previously spent more than a decade as a senior U.S. diplomat, completing multiple overseas assignments in the Middle East, Latin America, and East Asia. While stationed in Washington, DC, Craig focused on developing policies aimed at confronting China's malign influence activities and North Korea's nuclear weapons program.

RADM (Ret.) Mark Montgomery serves as senior director of FDD's Center on Cyber and Technology Innovation and directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Previously, he served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Montgomery served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

Benjamin Jensen is a senior fellow for Futures Lab in the International Security Program at the Center for Strategic and International Studies (CSIS). He is also a professor of strategic studies at the Marine Corps University School of Advanced Warfighting. Dr. Jensen has spent the last decade researching the changing character of political violence, technology, and strategy. He has worked with the Defense Advanced Research Projects Agency (DARPA), Marine Corps Warfighting Lab, NATO, the U.S. Army, and a range of government agencies and foundations to develop wargames and scenario-driven exercises exploring strategy, defense analysis, crisis response, military planning, and complex emergencies.

With contributions from Elaine Dezenski, Josh Birenbaum, and Annie Fixler.

The authors and contributors would like to thank TABF CEO **Dr. Hank Huang** for his leadership on this event.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.