

TESTIMONY OF MICHAEL W. STUDEMAN
REAR ADMIRAL (RADM), U.S. NAVY RETIRED
FOR THE CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

July 23, 2025

“Stand with Taiwan: Countering the PRC’s Political Warfare and Transnational Aggression”

Good morning Chairman Sullivan, Cochairman Smith, and distinguished members of this Commission. I am Mike Studeman, a retired two-star admiral with 35 years of service as an intelligence officer. Thank you for the opportunity to appear before you to discuss PRC political warfare against Taiwan, how Taiwan is dealing with it, and what more to do about it.

The views expressed in my testimony are my own and do not represent any organization I am currently or previously affiliated with as a retired officer or as a formerly active duty member of the military.

In terms of my background, my last four assignments before I retired in 2023 were Commander of the Office of Naval Intelligence, Director of Intelligence (J2) for the Indo-Pacific Command, Director of Intelligence (J2) for the Southern Command, and Commander of the Joint Intelligence Operations Center at U.S. Cyber Command. I have a Master’s in Asian Affairs from the Naval Postgraduate School in Monterey California and studied Mandarin Chinese at the Defense Language Institute. I served in a variety of intelligence posts around the world and at sea dealing with a range of global geopolitical issues, but also developed substantial experience in China matters across many jobs over decades going back to the late 1990s. I’m currently a MITRE National Security Fellow and advisory board member of the National Bureau of Asian Research.

Strategic Perspective

I’d first offer that political warfare has deep roots in Chinese history, culture, and mindsets. Political warfare is about expanding one’s political power at the expense of an opponent’s. In 1948, George Kennan defined political warfare as the “employment of all means at a nation’s command, short of war, to achieve its national objectives.” Given the efficacy of political warfare over millennia in China, Beijing will never desist from using this expression of power to achieve its ambitions. Many nations engage in mild forms of political warfare all the time, but authoritarian states dominated by a history of communist and Marxist-Leninist ideologies have taken political warfare to their Machiavellian extremes, supercharging their states to perfect

the dark arts of manipulation and subversion. By subversion, I mean the DoD definition of “actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority.” During the Cold War, America dealt with Soviet political warfare that took the form of “active measures,” so this type of shadow fighting short of war is not new to the U.S. A central question is how we can learn from our 20th century experiences to guide our individual and collective responses to the 21st century manifestations of tyranny that are now resurging at scale and scope.

A key macro-strategic point to make from the outset is that CCP political warfare is not just happening over there in Taiwan, but globally, including over here in America. China treats every day as a Super Bowl event as they attempt to win influence across the far reaches of the planet. Unfortunately, the American public continues to suffer from chronic inattention blindness of CCP efforts both outside and inside our lifelines, largely due to the cooption of the U.S. entertainment industry by the CCP and the reticence of multiple administrations in the White House to adequately describe the full extent of Chinese malign action in our homeland and beyond. Even while we might assist partners in pushing back against Chinese influence, we will need to address the reality that CCP’s political warfare activities have already gone a long way to psychologically anesthetize the American public, hush business leaders, intimidate scholars and academia, and create an environment of self-censorship on a wide range of clear and present China dangers.

Overarchingly, we would be well-served to view political warfare as an infinite game and wicked problem with no permanent winners or losers, no agreed-upon rules, a fluctuating set of players (many unknown), and no finish line. Political warfare does not eschew targeted violence, and agent provocateurs often look like ordinary, unassuming people who live seemingly innocuous lives amongst us. Infinite games are struggles for advantage that place a premium on flexibility and resilience by an expansive set of players at all levels who must all become adept at dealing with constant fluctuations, ambiguity, and dynamic contestation across multiple domains of influence. To gain the upper hand against adversarial “red” players, “blue” players of all stripes must acknowledge the brutal facts of their existence (understand the nature of the fight we are in, which is Cold War-like) and be reminded that our most evergreen advantages will stem from projecting a better, long-range vision for the future than China, developing trust-centered partnerships, and committing to just causes that inspire others to voluntarily work together to advance the higher purposes of freedom, dignity, truth, peace, equality, justice, and self-determination.

PRC Political Warfare on Taiwan

The CCP seeks to degrade the political order in Taiwan, sow divisions, undermine its democratic institutions, strengthen CCP sympathizers and pro-unification proxies, increase Taiwan’s dependence on the PRC, accentuate historical and cultural ties to bind Taiwanese to the mainland, and ultimately weaken the will and desire of the Taiwan people to forestall any political takeover by Beijing. Taiwan continues to bear the brunt of Beijing’s political warfare efforts, which are relentless, pervasive, and all-encompassing.

The CCP has been engaged in a steady and robust campaign over decades to disintegrate resistance to unification using a combination of carrots and sticks, though its efforts in recent years have dramatically expanded as it attempts to arrest what Beijing sees as alarming strategic trends regarding its core sovereignty issue. Those include Taiwan's growing sense of self-identity (not Chinese), strengthening relations with the U.S., and the third straight win for the Democratic Progressive Party, now represented by a vocal advocate for de jure independence, President Lai Ching-te.

As with many other decisions, Xi Jinping has shown he is the chief engineer of his own crises. Beijing refuses to see that its prolific rhetoric about "reunifying" Taiwan, including Xi's statements about not leaving the Taiwan problem for future generations and directing the PLA to be ready to take Taiwan by 2027, combined with its actions to rapidly modernize its military and conduct Taiwan invasion exercises and blockade rehearsals, created the catalyzing events that fundamentally changed the status quo over Taiwan. CCP choices drove Taipei to self-strengthen and seek outside help to ward off CCP-initiated threats. Regardless, Beijing is now using even sharper power pressure tactics that continue to increase in frequency, diversity, complexity, and intensity, exacting significant (punitive) costs on Taiwan and destabilizing the Western Pacific.

China's political stratagems and cognitive warfare against Taiwan, including the use of the Three Warfares (public opinion, media, and legal warfare), are well covered in a variety of scholarly works. I defer to John Dotson's written testimony submission for this session to better understand specific methods and tactics the CCP employs. I commend his authorship of the Global Taiwan Institute report titled "The Chinese Communist Party's Political Warfare Directed Against Taiwan: Overview and Analysis" from May 2024. Jukka Aukia also published a detailed report relevant to this commission from the Hybrid CoE titled "China's Hybrid Influence in Taiwan: Non-State Actors and Policy Responses" from April 2023. A January 2021 CSIS report called "Protecting Democracy in an Age of Disinformation: Lessons from Taiwan" is also relevant and useful.

To summarize, the CCP's political warfare efforts are a highly orchestrated, interconnected, and multi-tiered set of activities that include so-called white, gray, and black elements: White, or overt means, involve CCP diplomatic and economic actions, official statements and state-controlled media propaganda, military operations, and trade relations that are used as levers of influence.

Gray, or semi-overt means, involve law enforcement and militia encroachments in the maritime space, the use of foreign media and advanced information technology tools including algorithms and bots to propagate and reinforce disinformation, funding and manipulation of political parties and front groups, discounted junkets for politicians, academics, journalists, and students to visit China (who are then subjected to influence by CCP United Front representatives), temple donations and cultural exchanges, and co-option of social media influencers and entertainment celebrities, to name a few.

Black, or covert means, involve agents emplaced for the purposes of espionage, influence, and/or sabotage, recruitment of former security force personnel, use of ghost fleet vessels to damage Taiwan infrastructure, establishment of sleeper cells and weapons caches, offensive cyber operations, computer network exploitation, and activation of criminal groups such as the Triads in Taiwan for various purposes ranging from harassment to potential assassinations. For Taiwan, there is no ability to distinguish between benign and malign Chinese actions. CCP infiltrations and co-option are legion. Every connection, relationship, arrangement, communication, and interaction has proven to serve as a possible threat vector for CCP influence and interference.

Taiwan's Measures to Protect Itself Against Political Warfare

Taiwan has proven remarkably resilient in the face of the CCP's incessant political warfare onslaught; however, in the face of rampant CCP actions to disrupt, corrupt, and usurp power on Taiwan, Taipei's leaders knew they needed to strengthen its overall defense and security posture and raise the costs of doing business for those complicit in subversive activities. In March 2025, President Lai announced 17 strategies to address five major threats posed by China: threats to Taiwan's sovereignty, military infiltration, obscuring national identity, societal infiltration through cross-strait exchanges, and economic coercion. The president defined his multi-faceted strategy as follows:

1. Responding to Threats to National Sovereignty

1. Promote the *Four Pillars of Peace* action plan to demonstrate Taiwan's resolve against annexation by China.
2. Collaborate with allies to convey Taiwan's opposition to China's efforts to erase its sovereignty internationally.

2. Responding to Military Infiltration and Espionage

1. Restore the military trial system to handle cases involving active-duty personnel suspected of treason or espionage.
2. Establish personnel management acts for military judges and separate organization acts for military courts and prosecutors.
3. Revise regulations for retirement benefits and penalties for expressions of loyalty to China by military personnel.

3. Responding to Threats Against National Identity

1. Enhance scrutiny of Taiwanese citizens applying for identification documents in China, especially military personnel, civil servants, and educators.
2. Implement stricter requirements for Chinese nationals applying for permanent residency in Taiwan, prohibiting dual identity status.
3. Adjust residency systems for individuals from Hong Kong or Macau with additional provisions for long-term residency.

4. Responding to United Front Infiltration Through Cross-Strait Exchanges

1. Raise public awareness about risks associated with travel to China and implement registration systems.
2. Establish a disclosure system for exchanges with China involving public officials and welfare organizations.
3. Restrict approval for Chinese individuals coming to Taiwan based on their united front history and cross-strait conditions.
4. Depoliticize cultural, academic, and educational exchanges while promoting healthy cross-strait interactions.
5. Enhance support for Taiwan's cultural industries to strengthen democratic cultural creation and competitiveness.
6. Provide entertainers with guidelines on conduct in China and address actions that endanger Taiwan's dignity.

5. Responding to Economic Coercion

1. Strengthen measures against cognitive warfare and cybersecurity threats via AI, internet applications, and other tools.
2. Conduct a comprehensive review of administrative ordinances related to national security enforcement.
3. Implement legal frameworks to address gaps in regulations ensuring effective enforcement of national security measures.

Other notable Taiwan measures to protect itself include the updating of Taiwan's National Security Law in 2022, which included more severe penalties for colluding with adversaries and tighter scrutiny on individuals and organizations with ties to China. Criminal penalties have been imposed for economic espionage and trade secret misappropriation in various crucial technology areas.

Political actors and parties are prohibited from receiving mainland funding and dual nationals who have the right to live and work in the PRC have been banned from running for office. Political parties are now required to issue annual financial statement meeting official standards. A regulatory framework has also been created to oversee private foundations that receive money.

Taiwan is increasingly investigating and prosecuting more espionage-related cases (64 in 2024, up from 16 in 2021) with perpetrators, including retired and active-duty officers, receiving multi-year prison sentences. In 2022 and 2023, Taiwan authorities reportedly broke up 11 spy rings. In a breathtaking case, Taiwan arrested a former three-star Army general for planning to create a "Fifth Column" sabotage unit designed to assist the PLA in militarily seizing Taiwan. In another example, four soldiers who worked in the Presidential palace and paid to collect intelligence were also caught and arrested.

Beyond jail time and fines, the 2002 National Security Law amendments added loss of pension penalties to military personnel, civil servants, teachers, and employees of state-owned

institutions for illegal activities aimed at assisting the PRC. Amendments to Taiwan's Criminal Code of the Armed Forces are being considered regarding penalties for expressing loyalty to the enemy or involvement in pro-China united front work. Military courts with prosecutors are being revived. The time after leaving the government has also been lengthened before public officials can visit the mainland. Taiwan is stiffening accountability and sending a message about the price of working or profiting as a CCP shill.

To address the growing threat of cyberattacks and infiltration, Taiwan plans to establish a National Cyber Security Command as early as next month (August 2025), which will add an operational arm to map Taiwan cyber vulnerabilities, identify threats, coordinate across government and private industry, and build resilience in Taiwan's critical infrastructure and key industries. The new command will work in tandem with the National Institute of Cybersecurity, which was established in 2023 to advance domestic digital resilience. These two organizations look to the Administration for Cyber Security under the Ministry of Digital Affairs (MODA) for Taiwan's national cybersecurity strategy, regulatory framework, and resource allocation. Taiwan is also implementing zero trust architectures and examining AI safety and quantum technologies, as well as other techniques, to help deal with current and future intellectual property theft, ransomware, deep fakes, and automated cyber assaults. Taiwan is one of the most cyber-afflicted places on earth with tens of millions of attacks per month originating from PRC state-based and patriotic hackers.

Notably, Taiwan has made significant strides in devising a strategy to counter the worst of the CCP's disinformation efforts. Taiwan has a small number of non-governmental fact-checking organizations that help invalidate fake news, expose forged documents, and discredit the firehose of falsehoods from mainland China. Regulations were established in 2018 and 2019 to punish those disseminating disinformation that is proven malicious, false, and harmful, although attribution in those cases remains difficult. The Ministry of Digital Affairs has helped institute government procedures and software to identify any trending disinformation in social media circles and nip it in the bud by performing instantaneous corrections. Government agencies created Civic Integrity Teams that are authorized to provide rapid, brief clarifications to debunk any social media distortions related to their mission. In general, Taiwan is on higher alert for any PRC attempts to create "infodemics" that could generate "affective polarization," fabrications curated to evoke emotional responses and drive wedges between Taiwan citizens, especially around election periods. Fortunately, Taiwan government credibility was burnished during the COVID years as they consistently provided prompt, reliable, and life-saving guidance to the public.

The Ministry of Justice Investigations Bureau has also established a nascent Cognitive Warfare Research Center designed to unveil and prosecute CCP collaborators, "useful idiots," and those in Taiwan who might cause public panic, maliciously stir up discontent with the government on controversial issues, manipulate the social atmosphere through content farms, defame government officials through deep fake videos, or mislead voters with fabricated political commentary. The burden of proof and supporting evidence has proven such a high threshold that few prosecutions have carried through on these issues to date.

On the economic side, although still a vulnerability that the CCP frequently exploits (for example, by calibrating bans on Taiwan agriculture, fruit, and petrochemical products), Taiwan has also been diversifying its supply chains and markets away from China to reduce Beijing's leverage. In 2010, 84% of Taiwan's outbound foreign direct investment went to China. In 2024, only 8% of Taiwan's FDI went to China. Taiwan's New Southbound Policy, which was initiated in 2016, continues to redirect business into Southeast Asia, South Asia, and the Pacific Islands. Taiwanese businessmen have also reduced their presence in mainland China; less than half reside there compared to 15 years ago (~175,000 remain).

In addition, Taiwan has instituted export control measures to restrict trade with certain approved countries and listed entities, especially related to advanced chips and China. The Foreign Trade Act forms the legal basis for managing the trade of Strategic High-Tech Commodities (SHTC). Exports of SHTCs require special permission. Violations of export controls can lead to criminal or administrative penalties, depending on the destination and severity. Taiwan has also adopted a control measure to strengthen checks on end-uses and end-users of such commodities. Taiwan effectively has a system for two-way screening for both inward and outward investments.

Chinese information and communications technology from the likes of Huawei, Alibaba, and Lenovo have been banned. Penalties for falsifying country-of-origin labels to hide Chinese imports have also become more severe.

Other efforts designed to address PRC malign influence include the February 2025 decision by the Taiwan Ministry of Education to bar two PRC schools affiliated with the United Front Work Department from conducting exchanges in Taiwan. The Ministry also barred any exchanges with the "Seven Sons of National Defense," PRC universities that traditionally funnel technology and graduates to the PLA. On top of this, the Ministry of Education supports media literacy training for Taiwan youth to help them become more discerning consumers of information.

Common sense yet long overdue decisions have also been made. In 2024, the Taiwan Mainland Affairs Council banned Taiwan citizens from working at the All-China Federation of Taiwan Compatriots (ACFTC), which had been composed mainly of Taiwan residents of the PRC whose official aim is Chinese unification.

Perhaps the most significant political effort underway to stop the PRC from using KMT proxies in the Legislative Yuan from undermining the DPP government and the executive branch (for example, withholding funding for defense for months) is an election recall for a number of members of parliament. Recall results will come in two waves over the next two months. The recall process is complicated in Taiwan, but if the DPP can take back six seats in the legislative body, they will regain the majority and thwart persistent KMT spoiler actions designed to weaken the presidency and many of Lai's policies and spending priorities related to national security. The pro-unification wing of the KMT stands to be exposed, shamed, and penalized for

its deep connections with the CCP if many of Lai's new accountability measures are successfully implemented, which explains some internal political resistance to some of his ideas.

In the summer of 2024, President Lai also established a Whole of Society Defense Resilience Committee chaired by the President. The committee involves representatives from government agencies, industry and civil society groups, along with leading experts across multiple sectors to help strengthen resilience under any conditions--peacetime, crisis, or war--in Taiwan. Six major thrusts include: (1) civilian force training and utilization, (2) strategic material preparation and critical supply distribution, (3) energy and critical infrastructure operations and maintenance, (4) social welfare, medical care, and evacuation facility readiness, (5) information, transportation, and financial network protection, and (6) continuity of leadership and ensuring the ability of leaders to strategically communicate in a crisis.

Taiwan is also building up defense capabilities that range from expanding manufacturing for unmanned systems, extending reservist training time, conducting more realistic exercises such as the currently underway Han Kuang 41 annual exercises, evaluating stockpiling options, and strengthening civil defense cooperation in a variety of areas. Taiwan is also evaluating or implementing new concepts related to littoral warfare, integration of unmanned and manned systems to create a more hybrid force, and defense in depth to include deep operations, urban warfare, and whole of society defense. The Minister of National Defense's strategic priorities include improving asymmetric capabilities, operational resilience, reserve forces, and counter gray zone activities. President Lai has also committed to spending more than 3% of Taiwan's GDP on defense, up from ~2.5%.

Recommendations on How the U.S. Can Help Taiwan

I would first point out that while the U.S. should consider expanding ways that it supports Taiwan, many of Taiwan's resiliency efforts that are already in place or in motion contain lessons for the U.S. and other allies and partners in how to confront endemic CCP political warfare and influence activities on their own soil.

An executive list of those areas where further advancements and cooperation might strengthen Taiwan:

- **Strategically, help reduce Taiwan's international isolation, including by using U.S. influence to encourage Taiwan admission to international bodies, programs, and projects that do not require statehood status.**
- **Further encourage Taiwan to spend more of its GDP on defense.**
- **Build in more opportunities for Taiwan to expand its Global Cooperation and Training Framework, which was established in 2015 to foster international partnerships on public health, law enforcement, cybersecurity, humanitarian assistance/disaster relief, and media literacy. Consider adding Taiwan training for the international**

community on China's political warfare doctrine, tools, practices, and lessons in how to counter them.

- Support deeper Taiwan and the U.S. cooperation on cyber defense, cybersecurity operator training, development of hunt teams, incident response lessons on foreign adversary tactics, and sharing of emerging malware/zero-day vulnerabilities and advanced persistent threat techniques. Regularize Taiwan Ministry of Digital Affairs, U.S. Cyber Command, and Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) coordination to increase resilience of Taiwan's critical infrastructure.
- Help Taiwan upgrade its classified clearance system, including reviewing classification categories, special access program procedures, sponsorship, background investigative vetting, adjudication procedures, continuous evaluation standards, and an associated law enforcement regime strict enough to enhance transparency and accountability for protecting sensitive information and dealing with unauthorized disclosures or other breaches of trust.
- Encourage Taiwan to adopt more stringent insider threat technologies across all sectors of society (but especially in government/security organizations and defense industries) using a number of world-class vendors that provide advanced user behavior analytics, user activity monitoring, and data loss prevention software, which can protect privacy while rapidly identifying concerning actions that deserve timely remediation and action.
- Cooperate with Taiwan on ways to improve procedures for selective disclosures of sensitive or classified cases of CCP political warfare activities to further expose PRC malign action and heighten global awareness of the threat.
- Help Taiwan develop a stricter, but fair-minded regulatory and liability framework over media outlets that act as mouthpieces for CCP propaganda and disinformation.
- Ensure that evolving Ukrainian lessons learned from the fight against Russian aggression in Europe promptly flow to Taiwan, facilitated as required by the best partner nations with insights and access to those lessons.
- Continue to help Taiwan develop and mature its Defense Innovation Office and related defense acquisition processes to help them streamline fielding of new defensive capabilities. Share process, authority, funding, and organizational lessons from the U.S. Defense Innovation Unit and other DoD Rapid Capabilities Offices in order to help Taiwan more rapidly adopt, experiment, and field a family of diverse systems needed on the battlefield soonest.

- **Restore funding and organizational support for American public diplomacy and strategic messaging efforts in the Department of State and across the government to enable the U.S. information instrument to highlight Chinese and Russian ambitions, strategies, tactics, and actions designed to undermine key pillars of U.S. and Western strength. Reverse cuts and firings to critical organizations like the Agency for Global Media, which must address these issues through essential programs such as the Voice of America and Radio Free Asia and Europe. Reverse reductions in the U.S. Foreign Service that threaten to cede more diplomatic and information space to American adversaries to grow their influence at our expense.**
- **Issue a congressional mandate to the U.S. Intelligence Community to produce an annual threat assessment on Chinese and Russian political warfare similar to the annual DIA China Military Power report. Such a report should increase societal awareness of extant and developing political warfare stratagems and tactics, and compile best practices to address them, drawing from lessons learned from our European and Indo-Pacific allies, Latin American friends, and other partners such as India and Taiwan.**