

Trilemma of Cyberattacks, Cybercrimes and Cognitive Warfare: Institutionalizing Digital Forensics and Its Architecture for Philippine Implementation

By: Teodoro Lloydon C. Bautista, DPA

Background

The Philippines is at the crossroad of its journey as a nation-state. Having gained independence from the United States in 1945, the country is still a cornerstone in the US-led defense and security apparatus in the Far East as part of the First Island Chain Strategy. This US decades-old strategy was to contain Communist China far-off the Pacific Ocean through forward operating bases in a string of islands encircling her - Japan, South Korea, Taiwan, Philippines and Malaysia. The Philippines is caught in a rivalry of great powers between the USA and China, causing regional instability and dragging the country to potential nuclear warfare. China's 10 Dash Line destabilized the region when it claimed the entire South China Sea, where several countries, such as Vietnam, Indonesia, Malaysia, Brunei, and the Philippines, are likewise asserting their own maritime claims. Despite the 2016 Permanent Court of Arbitration's ruling by The Hague in favor of the Philippines, China chose to ignore the international court's decision and invoke her territorial claims over the entire South China Sea.

Meanwhile, advances in the Internet and digital technologies brought down walls that once prevented China from permeating her influence across East Asia and Southeast Asia. Her Belt-and-Road-Initiative made headways across the Indo-Pacific, spreading investments in aerial and sea ports, railways and critical infrastructure to signal the rise of China as the region's hegemon. The US military-industrial complex seeks to block China's rise while raking in huge revenues from selling missiles and arsenals. Thus, a new arms race erupted in the region, not only on the kinetic front but on the cyber domain as well. Sophisticated, state-of-the-art digital technologies are being deployed against countries through cyberespionage, political disinformation and online financial fraud. China is determined to shift the battle with the US in the virtual world, where asymmetrical powers can be taken advantage of and the national will can be undermined.

The Philippines is struggling to fend-off Chinese-sponsored cyberwarfare that repeatedly forayed into its government, private industry, academia and civil society. Slonopas (2024) referred to cyber warfare as the strategic deployment of cyber attacks by a nation-state or international organization to target another country's national security, civil infrastructure, or civic infrastructure. These attacks are directed to undermine crucial systems, spread disinformation, and destabilize economies. Hacking, malware, and Distributed Denial of Service (DDoS) are all examples of cyber warfare attacks. Cyber

attackers commonly target various essential infrastructures, including fuel companies, utility companies, financial institutions, and governments.

Cyber warfare scenarios include hacking virtual networks to gain unauthorized access and obtain data or plant viruses. Viruses may damage, destroy, or seize control of computer systems, jeopardizing government, private, and public infrastructure. These cyberattacks soon intensified because of the country's intransigent position against Chinese illegal and unlawful incursions into the West Philippines Sea. The Chinese naval militia has harassed and water-cannoned Philippine Coast Guard vessels patrolling its sovereign waters and supplying its marine forces in the BRP Sierra Madre, grounded in Second Thomas Shoal (Ayungin Shoal), roughly 194 kilometers from the Province of Palawan. In the cyber domain, China-backed hackers, such as the Advanced Persistent Attack 41 (APT41), breached the websites of several Philippine databases and stole sensitive data related to the West Philippine dispute.

The use of disinformation and propaganda to sway public opinion in favor of China has swarmed traditional and social media in the Philippines amid its stance and close collaboration with the US allies. A Chinese political disinformation campaign has ramped up, sowing political division between the camps of former President Rodrigo Roa Duterte and incumbent President Ferdinand Marcos, Jr. – two dominant political forces in the Philippines today. AI-generated content used in digital smear campaigns have increased in social media platforms, sending highly partisan messages to provoke anger on both camps. It soon conflated with the multi-billion pesos corruption anomalies in the Department of Public Works and Highways (DPWH), that aroused outrage among Gen Z and Millennial population. Currently, protestors are demanding accountability and ouster of President Ferdinand Marcos, Jr, a throwback from recent youth unrest in Indonesia, Nepal and Madagascar.

Together with major data breaches and disinformation, the Philippines is encountering increasing cybercrimes, like online fraud and online sexual exploitation. There are a host of factors that exacerbate this, like abject poverty, unemployment, and human trafficking. These social and economic problems have intersected and resulted in the high volume of cybercrimes. Top reported crimes included online selling scams, digital frauds, and online child pornography. In 2024, a study reported that Filipinos lost an estimated US\$8.1 billion in the past 12 months due to text messaging scams. Since the banning of Philippine Offshore Gaming Operators (POGOs), their former employees of the Philippines have set-up their own guerrilla fronts to continue their own online scamming activities undetected. Access and affordability of the Internet connectivity among the poor have spurred a virtual cottage industry of sex trafficking, peddling sexually explicit videos and digital photos of innocent children by their parents and relatives. The Philippine National Police (PNP) and law enforcement agencies are struggling to respond and combat these 21st-century digital crimes.

The trilemma of cyberattacks, cybercrimes and cognitive warfare are testing the capabilities of Philippine defense and public safety systems. The intersection of these cyber threats – the trilemma - is a recurring challenge to the country's peace, rule of law, political stability, and national sovereignty. Several pieces of legislation had been passed to respond to the trilemma. One landmark law is the Cybercrime Prevention Act of 2012 (Republic Act No. 10175), which defines and penalizes various offenses through computer systems like hacking, illegal access, identity theft, online libel, child pornography, and cybersex. Another is the Data Privacy Act (Republic Act No. 10173), which protects personal data and information in both government and private sectors. However, the reality persists that these laws were difficult to enforce amid problems of interagency coordination, bureaucratic red tape, inadequate funding, poor training, and absence of shared databases. Such a situation often happens in many cross-cutting societal problems in the Philippines. The uniqueness of the trilemma, however, lies on its technological scale, volume, velocity, anonymity and impact of its negative externality across time and beyond boundaries.

Several agencies were tasked to solve the trilemma, but to no avail. The Department of Justice (DOJ) has organized the Office of Cybercrime, which principally investigates, files and prosecutes criminal actions against violations of cyber laws. The National Bureau of Investigation (NBI) has the Cybercrime Division, which handles the investigation and conducts searches and seizures of cybercrimes. The Philippine National Police (PNP) established its own Anti-Cybercrime Group (ACG), which enforces cybercrime laws and leads the investigation and apprehension of offenders. The Department of Information and Communications (DICT) plays the overall coordinator among different agencies in policies and plans on cybersecurity as well as education and awareness. The Cybercrime Investigation and Coordination Center (CICC) is an interagency body that crafted and formulated the national cybersecurity plan. The country's Armed Forces also created its own AFP Cyber Command, which focused on defending against cyber-attacks, gathering intelligence and information, and even undertaking cyber warfare against foreign adversaries.

Notwithstanding the laws, agencies and their mandates, the Philippines remained vulnerable to the burdens of the trilemma. Threats to the country due to cyber attacks, cybercrimes and cognitive warfare continue to intensify and overwhelm security forces due to the country's technological handicaps. While the threats evolved and dangerously morphed in deadlier forms, Philippine government agencies are finding their footing to effectively deploy resources and strategies to protect and defend the country's cyberspace.

This study now comes to fore in how to truly 'operationalize' the strategic approaches to combat and defeat the trilemma. And the Republic of China (Taiwan) is a practical benchmark for the Philippines in devising concrete measures, such as digital forensics, to solve the trilemma. At the moment, the Philippines has formulated laws and strategies to respond to the trilemma, but are struggling to implement them on the ground, to convert

them into doable and responsive anti-cybersecurity measures, and to scale them up toward cyber resilience.

Like the Philippines, Taiwan is relentlessly facing a huge volume of cyberattacks. In one article, senior Taiwanese officials revealed that the country receives more than 5 million cyberattacks per day. Frontinet, a US-based cybersecurity firm, reported that Taiwan is a hotspot for malicious actors, with roughly 55 percent of billions of malware attacks in the Asia Pacific Region (Yao-Chung Chang, 2024). Similar to the Philippines, cyberattacks, cybercrimes and disinformation campaigns are becoming the dominant 'gray zone' tactics by the Chinese Communist Party-People's Liberation Army (CPP-PLA) - a similar strategy they employed against Taiwan. Cyberattacks can be in the form of Distributed Denial of Services (DDOS) and Advanced Persistent Threats (APT) to weaken Taiwan's critical infrastructures, such as banking, energy, telecommunications and water supply. Cybercrimes can take the form of digital frauds or hacking that damage the economies through state-sponsored organized crime activities. The line between cyberwarfare and cybercrime can be blurred especially if cybercrime is a launching pad for a cyberattack. Taiwan is working towards cyber resilience amid Chinese aggression, short of actual wartime attack.

Significant online disinformation was a playbook used by Chinese 'hacktivists' to sow confusion among Taiwan citizens. The most glaring was the release of a 300-page e-book called "The Secret History of Tsai Ing-wen" to discredit Taiwan's former president by claiming her mother was a prostitute and that she falsified her PhD academic records. This was denied by her alma mater, the London School of Economics and Political Science (LSE), and confirmed her degree. Using software developed by ByteDance Ltd, a Chinese firm known as Duoyin, pro-Beijing trolls released short videos on YouTube, X and Tiktok with fake news anchors and AI-generated voice-overs. This was the handiwork of Chinese operatives to destroy Taiwan's Democratic Progressive Party (DPP), which opposed China's attempt to retake the island.

The use of AI is one the greatest threats in the country's political stability, with deepfake technology used to impersonate public figures and distort reality. Cyberattacks against government websites and databases have continued despite firewalls and encryption systems installed by authorities. Meanwhile, China has heavily employed cognitive warfare to weaken the public support towards the Marcos administration, instigating political polarization to veer public opinion away from the South China Sea dispute. The trilemma cannot entirely be overcome through Philippines' cyber defense policies and reliance on external technologies.

Thus, this study is crucial to Philippine authorities not only to reclaim lost battleground in the cyber domain but to explore the steps taken by Taiwan in dealing with cyberattack, cybercrimes and cognitive warfare. Its goal is to inform Philippine policy makers on the 'how' to overcome the burdens of this trilemma, that is now the scourge of the country's sustainable peace, economic development and overall security.

Issues

To sum up, the Philippines and Taiwan share a common battle in confronting a rising hegemon whose military operations escalated from cyber espionage, political disinformation to actual cyberattacks, short of outright war. Cyberwarfare is a preliminary option for China, short of kinetic warfare, by launching attacks against both countries' defense systems and critical infrastructures – prelude to striking first to prevent enemy retaliation. Chinese-sponsored cybercrimes, such as hacking and digital frauds, posed to undermine both countries' financial and monetary systems. Finally, the widespread dissemination of fake news and political disinformation controlled by China to both countries has an adverse impact on their economies, their people's social cohesion and their governments' abilities to protect and safeguard their peoples.

Thus, this study shall answer the following issues:

1. What are Taiwan's current strategies and approaches to combat cyberattacks, cybercrimes and cognitive warfare that the Philippines can take a page from to overcome this trilemma with actual operators on the ground?
2. What would be the risks and challenges for both the Philippines and Taiwan if China's cyberwarfare is left unchecked and dominates both countries?
3. How can the Philippines integrate Taiwan's best practices through legislations, programs and processes as well as trigger a cohesive security arrangement between the two countries?
4. How do we institutionalize digital forensics in the Philippine public safety and defense system to counter cyberattacks and cybercrimes?

Research Design

This study shall use a descriptive-qualitative approach, adopting the Case Study Method on Taiwan's cybersecurity policies, plans and programs. It shall conduct extensive literature review and onsite visits to Taiwan for actual direct observation. This research was conducted during a five-month period of fellowship, two months in the Philippines and the three remaining months in Taiwan.

The major datasets shall be derived from key informants with the Taiwan ministries, specifically in the following: (1) Ministry of Digital Affairs, (2) Ministry of Defense, (3) Ministry of Foreign Affairs, and (4) Institute of National Defense and Security.

The data collection and interpretation employed content analysis, through person-to-person interviews and structured questionnaires.



Literature Review

Taiwanese strategies to combat Chinese cyber warfare

Taiwan stands out as the clearest example of a contested state, with China's continued assertion of unquestionable right to reclaim Taiwan as part of the mainland. Although Taiwan has limited diplomatic recognition due to the One China Policy, Taiwan's pivotal role in US First Island Chain Strategy, like the Philippines, its global semiconductors and advanced microchips industry, and robust democracy has thrown the country into the crosshairs of US-China Great Powers rivalry (Wu, 2025).

With China's expanding economy and vibrant export industries, the new hegemon has allocated substantial resources towards strengthening its Information and Communication Technology (ICT) toward a higher grand strategy. China's 100th year anniversary of the PLA founding forebodes Taiwan's unification to the mainland by diplomacy, either by diplomacy, coercion or even war. US security analysts appeared more fixated in 2027 as the deadline set by Chinese leader Xi Jinping to retake Taiwan with military force (Culver, 2025). This overarching national goal has intensified China's use of ICT and other cutting-edge technologies to subvert Taiwan's independence through cyberattacks, cybercrimes and cognitive warfare – the trilemma.

Cyber-attack is the process of attempting to steal data or gaining unauthorized access to computers and networks before the data breach. Ultimately, the goal is to either disable the victim's computer network or gain access to the data and infiltrate connected networks (Fortinet, 2025). Some examples are malware, phishing, ransomware, denial of services, and man-in-the middle, among others. In the case of China, the country has deployed cyberwarfare as an offense-dominant strategy, offering inexpensive, anonymous and automated means of attacking high-value targets, such as critical infrastructures. More importantly, they weaken the enemies' will and determination, by sowing chaos and confusion to their people and government.

Cybercrime refers to criminal offenses committed using the computer, the Internet or another computer network as a component of the crime. This may include data thefts, cyberstalking, cyber harassment, fraud, or unlawful access to electronic communications. Others like doxing, which is posting personal details of a victim online for harassment or swatting, which is reporting a false report to direct the police to respond to a location, seldom happens in the Philippines (Cobb, 2024). The goal is to illegally obtain funds by targeting computing devices and conducting malicious activities that compromise the network integrity and availability.

Cognitive warfare uses technology as a weapon to alter the person's cognitive and thought processes as well as the brain and nervous system that underpins its functions. It takes advantage of digital technologies to influence and disrupt the person's cognitive

functions, such as memory, attention, communications and even emotion. For example, troll armies sending photos of dead children to the public due to military operations. Through a period of time, cognitive warfare uses cognitive biases to modify the thinking and habits of victims, causing irreversible effects on their cognitive personality (Claverie, 2025).

According to Pryor (2018), Taiwan faced 20 to 40 million cyber-attacks per month. Cyber-attacks are directed at Taiwan's critical infrastructure (i.e., distributed denial-of-service) or trade secrets through hacking (Robinson et al. 2015). Some of these attacks can actually be in the form of physical sabotage, such as cutting-off submarine cables on which Taiwan's broadband connectivity primarily relies. According to TeleGeography, Taiwan has 14 submarine international cables, with the 15th (Apricot) to be completed in 2026. Nine of Taiwan's cables can be summarily disconnected by China without warning. The US government rejected Google and Facebook's overtures to connect a new cable between the US mainland and Hong Kong. This forced these companies to connect the US, Taiwan and the Philippines instead. Today, Taiwan is building her own domestic satellite communications to preserve government networks in the advent of a Chinese attack. There can also either be a point-to-point microwave network or a local municipal mesh network on hidden rooftops.

Like most nations around the globe, Taiwan is fighting cybercrimes, like Internet child pornography, infringements on intellectual property rights, and theft of industrial secrets of their microchip technology. Online fraud and ransomware have generated heavy losses in many firms as well as eroded public confidence in the financial and monetary systems. Meanwhile, cryptocurrency is employed by crime syndicates for money laundering and hidden transactions. Considering the wide availability of Internet-enabled digital devices, anyone with IT skills can exploit the anonymity and velocity of this technology to commit illegal activities and conceal their identities from detection (Huang, 2020). Chinese-backed crime groups are having a field day attacking Taiwan and the Philippines via online digital fraud.

The Chinese People's Liberation Army (PLA) has also employed criminal gangs as proxies to steal or hack electronic data, compromising Taiwan's financial systems. These Chinese-sponsored crime groups, mostly hackers, will infect systems of private owners by detecting a flaw and planting malware. At an appropriate time, the group shall cripple the system and extract a King's ransom from the victims. A subcomponent of these cybercrimes encompassed digital fraud, data phishing, and deep fakes to embezzle huge sums of money using chicanery and deceit.

Taiwan is swamped by political disinformation from China, that sow discord among its populace. Libicki (1995) enumerated seven components of information warfare (command-and-control, intelligence-based, electronic, psychological, hacker, economic, information, and cyberwar), on which cognitive warfare fell under the category of psychological warfare. Taiwan's Ministry of Digital Affairs (MODA) refused heavy-handed

censorship, which is a hapless reaction to removing malicious content akin to a game of whack-a-mole.

But China chose censorship by strictly controlling the Internet and suppressing free speech, transparency and democratic participation. She bans the most popular application-level services or replaces them with local varieties since they originated from Western adversaries. China's ambition to influence people's minds is beyond Westerners' comprehension. Subverting democratic institutions and eroding the trust of both Taiwan and Philippine governments is the greatest threat to China's cyberwarfare.

Singh (2024) defined 'cognitive warfare' as tactics designed to influence people's mindsets and actions at a wider reach and scale. Unlike 'information warfare' that manages the flow of information, Hung & Hung (2020) defined 'cognitive warfare' as the ability to influence and control the mental state and behaviors of others to respond and act based on the information. The concept has much to do with neuroscience, which focuses on the brain's cognitive processes. In fact, the authors said that cognitive warfare seeks to manipulate and affect the minds of targeted individuals, who are profiled as vulnerable to such messaging.

Meanwhile, here are some measures Taiwan used to combat cyberattacks:

- Improve transparency by revealing Chinese influence on Taiwan's media, academia, companies and temples
- Update laws on fair competition by preventing Google and FB from diminishing local news and journalism
- Institute laws to prevent China's attack on dissidents through proxy agents
- Breach's China's Great Firewall
- Work with democratic forces in and outside China to circumvent censorship.
- Offer training for critical thinking and media literacy

The risks and challenges for both the Philippines and Taiwan if China's cyberwarfare continue unchecked

There is a deep, troubling reality that China is winning the cyberwar against her prospective enemies, particularly the United States of America (USA). With the power of the Internet and advanced digital technologies, China seemed to dominate the digital battle space.

Nueberger (2025) disclosed that Chinese sponsored hackers, dubbed "Salt Typhoon," gained access to major US telecommunication networks with the ability to track down conversations of US intelligence officers and law enforcement agents across the US mainland. The author likewise raised alarms that Chinese cyber-operations had been prepositioned in US critical infrastructures, like water, power grids, and other systems,

gaining the capacity to hold implants on these structures through time, remain dormant and unseen, and be activated on command to attack the US with a malicious code (Neuberger, 2025). As of now, China can launch cyber-attacks against US critical infrastructures, disrupting oil and gas pipelines, water supply and even rail systems. This is China's preemptive strategy in case of an outbreak of conflict with the US.

Over the past two decades, Taiwan has been the world's hub for semiconductors and advanced microchips. The country has struggled in confronting cyberattacks from various states like People's Republic of China, North Korea and Russia. In response to these threats, Taiwan formulated its National Cybersecurity Strategy - a crucial document delineating the overarching vision, guiding principles, threat assessment, and strategic thrusts in the cyberdomains. The cyberattacks on Taiwan's microchip industry can adversely affect 60% of the world's supply of microchips in vehicles, robots, digital computing, smart phones, and even manufacturing.

With the intensifying US-China rivalry, Beijing has deployed an array of gray-zone¹ operations, such as cyberattack, cybercrime or cognitive warfare. In the 2018 "Kansai Airport Incident," Chinese sponsored trolls spread fake news of the inefficiencies of Taiwan officials compared to competent Chinese 'wolf-warrior' bureaucrats, resulting to the suicide of an embarrassed Taiwanese diplomat and unravelling a political crisis. There was no truth in the social media news. While cognitive warfare has been unraveled in many nations, it is still difficult to suppress in both the Philippines and Taiwan since adversaries take advantage of the democratic spaces and freedom of expression.

During the 2020 COVID-19 pandemic, the so-called "Vaccine Chaos" had fingerprints of Chinese sponsored troll farms, discrediting the ruling Democratic Progressive Party (DPP) for the vaccine shortage. The same tactic was employed in the "Egg Shortage Crisis" during the 2023 election year, which caused votes against the DPP candidates. Overall, China's cognitive warfare is to weaken the DPP's legitimacy before the eyes of the Taiwanese population. During the 2024 national elections (presidential and legislative seats), China interfered by instigating tax investigation and land use questions on Foxconn (a principal supplier of Apple products in China), derailing its founder, Terry Gou, from running for office. This strategy also extended in China's promotion of the "Doubt America Theory," which primarily led to a mistrust of America's strategic intention to defend Taiwan. This skepticism grew with the US military's pull-out after decades of occupying Afghanistan and almost abandonment of Ukraine during the height of Russian invasion.

The Chinese People's Liberation Army has undertaken information manipulation across Taiwan traditional and social media platforms. This was designed to undermine

¹ The term "gray/grey zone" refers to a situation in which the state activities are not clear whether they are legal or illegal, acceptable or unacceptable, in a conflict that falls below the threshold of a direct armed confrontation. China uses "salami-slicing" approach, whereby they achieve incremental gains, like artificial island build-up, without provoking other claimant countries towards armed retaliation.

social cohesion, erode public trust in government's efficacy, and soften people's resistance to China's forced unification agenda. Not only that, it also promoted doubts about America's commitment to assist Taiwan in the outbreak of war across the straits (Kramer, Yu, Webster, & Sizeland, 2024).

Another risk is Taiwan's critical infrastructure that is crucial to her economy and societal functioning. These include energy, banking and finance, hospitals, communications, transportation, and water. Each is pivotal to running a society and each is mutually reinforcing through digital technology deployed in their operation. It is reported that Taiwan absorbs roughly 5 million cyberattacks per day against government websites, with 15,000 per second. Most of these attacks ostensibly targeted government offices, police departments, finance institutions, and banking systems. Worse, some cyber attackers used a range of techniques from command-and-control to "living-off-the-land," which allowed them to conceal their intrusions over time while engaging in guerilla type of cyberattacks.

Ultimately, the risks and challenges, if the trilemma remained unchecked, are the creeping invasion operations of China in both countries. The cyberwarfare are gray zone tactics to reinforce the overall strategy to retake Taiwan by 2049, while subverting the Philippine claim in the South China Sea. These incidents, short of war, aimed to establish a beachhead and swarm both countries with small fires as diversion, while China gradually built-up its military and consolidated its position in the region. As time passes by, China can kinetically subvert, politically occupy and diplomatically leverage both countries to counterbalance the US presence in the Indo-Pacific region.

Integration of Taiwan's best practices through legislations, programs and processes

Taiwan created a cybersecurity strategy in phases to confront the cyber trilemmas originating from China – its main aggressor. As Taiwan announced its independence from China, these cyber trilemmas alarmingly intensified, affecting the fabric of its peace and stability.

The DPP government first organized the National Information and Communication Strategy Taskforce (NICST) in 2001, an interagency body formed to promote information and communication security. In the following year, it created the National Center for Cyber Security Technology (NCCST), which had the capacity to offer technical services, such as pre-incident protection, during-incident response, and post-incident forensics and recovery to all ministries.

During Phase I (2001 to 2004), the underlying goal was to ensure a secure communication and information environment in the wake of intensifying Chinese cyberattacks. The build-up of the technical staff's competencies in the NCCST was important to support key government ministries in public services, designating standards and protocols in cyber security incident reporting, and monitoring and auditing mechanisms. Education and training on cyber security was intensified, including public

awareness of these cyber trilemmas. Laws and regulations were amended to be responsive to the cyber security threats as well as technical standards, audit and inspections. One of its achievements was qualifying and installing the Information Security Management System (ISMS) for critical infrastructures.

During Phase II (2005 to 2008), the major milestone was the institutionalization of the National Security Operation Center (N-SOC), with a 24/7 cyber security defense. This included the national early warning, alert and monitoring system, with the expansion of cyber security operations across ministries and other societal members.

During Phase III (2009 to 2012), the cybersecurity strategy was officially mainstreamed into Taiwan's population, encouraging all institutions – businesses, academia, and civil society – to conduct cyber security inspections and evaluation of cyber threats for data users and customers. The promotion of cybersecurity awareness spread across businesses, schools, non-government organizations, and ordinary households, and became integrated in Taiwanese' way of life.

During Phase IV (2013 to 2016), the National Strategy for Cyber Security Development Program (2013 to 2016) was approved, which primarily promoted talent cultivation and international exchanges to invite more qualified people and create competency certifications. Among other remarkable initiatives were cybersecurity defense and intelligence sharing, building governance structures, evaluating maturity levels of ministries, creating the Institute of Watch Internet Network (iWIN) as oversight to Internet content, conduct of cyber security offense and defense drills, and even planning scenarios and simulation, among others.

During Phase V (2017 to 2020), it dedicated into the launching Taiwan's cybersecurity defense through four strategic priorities: (1) enhancing the base environment for cyber security, (2) creating a national cyber security joint defense system, (3) increasing the autonomy of cyber security industry, and (4) cultivating high-quality cyber security talent.

These phases gradually strengthened Taiwan's capabilities to mitigate cyber security threats and improve resilience in confronting the cyber trilemmas. Taiwan's cyber security was directed toward how Taiwan installed defensive measures to detect and prevent intrusions into its cyber domain, such as communication lines, networks, routers, critical infrastructures, or even people's minds and interactions.

The Cybersecurity Management Act is the primary law governing cybersecurity in Taiwan. It applies to government agencies, specific non-government agencies in-charge with critical infrastructures, state-owned business, and other government-sponsored foundations. It imposes cybersecurity protection measures on specific industries like banking, finance and telecommunication sector. Under the law, any cybersecurity incidents must report one hour of discovery and response measures must be completed

within 36 to 72 hours. Those covered organizations must comply with the cybersecurity requirement under ISO/IEC 27001.

Currently, Taiwan has explored the use of cloud-based technologies to establish a duplicative set of cyber-enabled governmental functions outside the country. These data farms can store and protect Taiwan's data abroad and ensure the continuity of vital services. Cloud providers, like Amazon Web Services, are enthusiastic to support Taiwan's cloud-based strategy. The adoption of private-sector cybersecurity providers is also a game changer for Taiwan. The US is facilitating Taiwan's initiatives to procure private-sector defensive cyber operations. With its reserve force, Taiwan is also organizing the surge capability of cyber security experts, who will support and defend the country against Chinese cyber-attacks. Finally, the Taiwan Space Agency has launched a dedicated Low Earth Orbit (LEO) satellite communication to avoid dependence on undersea internet cables, which could be severed by Chinese war ships and vessels.

Institutionalize digital forensics in the Philippine public safety and defense system to counter cyberattacks and cybercrimes

As far as cyberattacks and cybercrimes are concerned, the Taiwanese government established the Ministry of Digital Affairs (MODA) in 2022. It issued cyber security policies and guidelines to oversee the implementation of cybersecurity responses against attacks. The Administration for Cybersecurity (ACS) is tasked to implement and manage the strategy. Under the MODA, the National Institute of Cyber Security (NICS) was organized to produce R&D, focus on talent cultivation, and provide technical services for national cyber defense. This reinforced the use and application of digital forensics, which is the cornerstone of Taiwan's strategy in ensuring an effective and resilient cyber defense against the increasing volume of cyber-attacks.

The MODA actively integrates digital forensic into its national cybersecurity strategy. Digital forensics can identify and track down cyber-attack origins, choose the appropriate incident response, and gather evidence of state-sponsored cyber warfare. There are available digital scanners and cyber-attack analysis tools to understand the scale and scope of the data breach. Tools can trace entry points and attack vectors deployed by hackers, and suggest immediate response.

Digital forensic investigators can capture data on evolving cyber-attacks, such as the use of IoT botnets for DDOS attack or theft of trade secrets in Taiwan's microchip industry. The intelligence is shared across ministries, systems operators, and foreign partners to strengthen early warning systems and join cyber defense operations.

Taiwan police force has a special unit for investigating technology crimes. In addition, the Ministry of Justice Investigation Bureau (MJIB) created in 2006 the Cyber Forensics Laboratory, qualifying for accreditation with ISO/IEC 17025 (Huang, 2020). In 2008, a malware variant known as TAID00R was used to launch cyberattacks against Taiwanese

government agencies and businesses. These come from borders beyond Taiwan, roughly between 20 to 40 million incidences.

Taiwan has improved its digital forensic capabilities to track sources of these criminal activities and malware used. In July 2016, a hacking syndicate was able to illegally withdraw NT\$83.27 million from the First Commercial Bank ATMs. Within a week, Taiwan police recovered NT\$77.48 million fund and arrested three of the members of the crime group. What is important in the solution and prosecution of the case was the cooperation with international law enforcement agencies. Taiwan's Criminal Investigation Bureau (CIB) worked with the European Union Agency for Law Enforcement Cooperation (Europol) to exchange intelligence and evidence, specifically data from the suspects' mobile phones. This resulted in the arrest of the mastermind in the criminal hacking syndicate, known as Dennys.

Taiwan has carried out immense support to digital forensic analysis across ministries. There are cyber defense technologies, like the AI-assisted threat identification platforms – the Ransom Hunter - and even drills and simulation exercises to boost preparation across critical infrastructures. Foremost, the Ministry of National Defense also created its own Military Cyber Security Commands, which protects the country against cyber warfare and collaborates with the academia and private sector experts.

Findings, Discussion and Analysis

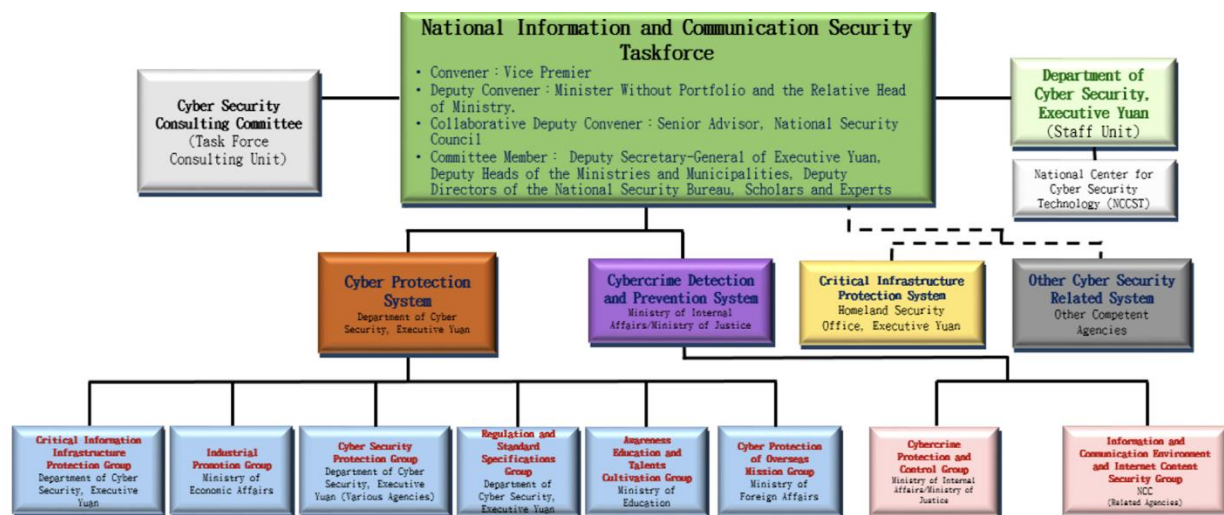
1. Taiwanese strategies and approaches to combat Chinese cyberattacks, cybercrimes and cognitive warfare

Taiwan has systematically built up its cyber defenses, knowing fully well the capabilities of China to launch outright cyberattacks on her systems. Jieh-min (2025) claims that Taiwan is a 'sovereign-contested' state whose independence continues to be challenged by China (or People's Republic of China) and whose de jure status is rejected by Western powers, such as the USA, due to the One China Policy. To understand Taiwan's strategies and approaches to fend-off China's assertions to unify Taiwan into the mainland, it is crucial to note the concept of a 'contested state' – one with de facto autonomy, independent economy and even foreign policy, such as the issuance of passports to other countries (Wu, 2025).

For decades, such a status quo has been a modus vivendi to avoid outright war and ensure stability across the Taiwan Strait. However, this faces the threat of China's rising power, growing assertiveness to claim Taiwan, and intensifying rivalry with the USA. These challenges are escalated by Beijing's mounting military threats, economic coercion, cyber-attacks and cognitive warfare.

Taiwan is well-aware that cyberattacks, cybercrimes and cognitive warfare intertwined to amplify Beijing's political narratives and strategic agendas across multiple

domains. The trilemma assists the Chinese Communist Party's ultimate goal of Taiwan's reunification into the mainland. It mutually reinforces China's grey zone tactics, foreign information manipulation and interference, and cognitive warfare (Lee, 2024). Hence, Taiwan established the NICST in January 2001 to oversee the national cybersecurity policy and other initiatives. With the shifting strategy to prioritize cybersecurity as a national security issue, the Executive Yuan (Cabinet) created a special unit dedicated to cybersecurity affairs in August 2016, the Department of Cyber Security, replacing the original task force – the Cyber Security Office. As the technical staff unit of NICST, the Department was tasked to promulgate guidelines, policies and plans. Below is the organizational structure of NICST.



Meanwhile, the National Center for Cyber Security Technology (NCCST) was organized in March 2002 to act as the think tanks and staff unit of the NICST, supporting the cyber security protection mechanism, before-and-after incident response, and post-incident recovery and forensics. Through its technical services, it helps government agencies and core industries in boosting their cyber security protection capabilities and information sharing to mitigate cyber threats and attacks.

2. Risks and challenges for both the Philippines and Taiwan if China's cyberwarfare is left unchecked and dominate both countries.

The advent of the Internet and proliferation of ICT has not only improved people's lives but tremendously advanced warfare across unstable regions. Despite the manifold benefits of ICT, it precipitated a host of risks and challenges as well. Both Taiwan and the Philippines face the proliferation of cybersecurity threats, such as data breaches, hacking, and cyber-attacks on critical infrastructures. Taiwan endured an average of 2.16 million cyberattacks per day in 2024, a 60 percent rise from 1.33 million in 2023, mostly targeting government websites and services originating from mainland China (Temple-Raston, 2025). The Philippines, on one hand,

There is a strong correlation between China's cyber aggression or "gray-zone" tactics with Taiwan's political assertions for independence and autonomy. When former Taiwan President Lee Teng-hui asserted her country's separate identity and status from China in July 1999, it was a sharp departure from the One China Policy, that incensed China to launch cyber-attacks against Taiwanese government websites – defacing them and uploading China's red flag. These cyber-attacks steadily increased in volume and velocity. Taiwanese officials detected roughly 10,000 suspicious social media accounts, with many in Facebook, which disseminate disinformation and fake news (Lee Y. , 2025).

Some cyberattacks were aimed at stealing sensitive intelligence, patents, trade and industrial secrets. A case in point was the Chinese-sponsored Salt Typhoon, which was a complex, sophisticated operation against a country's critical infrastructures. Ultimately, the greatest weakness of the Philippines is Chinese hackers' ability to exploit the flaws in Philippines' infrastructures, such as firewalls, or used stolen passwords by state sponsored hackers. Once inside, these hackers put malware and hijacked the system to secure control. The attackers subsequently used computers, servers, routers and other devices to compromise Philippine networks and conduct surveillance operations.

Beijing has increasingly employed hybrid warfare strategy and grey zone tactics, intertwined with malign influence and legal strategies. A case in point was the "Kinmen incident" on February 14, 2024, near Taiwan's controlled islands. A Chinese fishing boat wandered into Taiwan's territorial waters and was subsequently pursued by its coast guards. The boat capsized, killing two of the people on board. China took advantage of the incident by portraying Taiwan as mistreating Chinese fishermen and deployed its coast guards near the Kinmen islands.

During the heightened tensions, the Taiwan Affairs Office (TAO) of the People's Republic of China State Council framed the incident as Taiwan's fault while asserting that the innocent Chinese fishermen were murdered, amplifying the narrative across multiple platforms, such as state media, key opinion leaders, online troll armies. These pro-China messaging were found in China Central Television (CCTV), Yuyuan Tiantian, Weibo, WeChat, and Today Strait. Chinese trolls, such as Diba, disseminated the narrative in global platforms like Facebook and Instagram (Placeholder2) (Lee, 2024). After negotiations, the Taiwan government returned the fishermen's bodies and paid for repatriations. However, this only galvanized further incursions of China Coast Guard (CCG) in the Kinmen waters.

Cyber warfare likewise aims to subvert Taiwan's democratic institutions through fake news, political disinformation, and fomenting distrust into the government. Disrupting government operation and delivery of public services through DDOS operations is one way of undermining public trust in the government. China has escalated her cyber warfare campaign against Taiwan. The campaign is relentless and technically sophisticated. It is built on the backbone of state-sponsored espionage, psychological operations, breach of critical infrastructures, and political disinformation. It reinforced Beijing's strategy to

destabilize Taiwan, with military operations short of actual armed confrontation. Many Chinese-backed hackers are not only conducting intelligence-gathering operations but implant malware on critical infrastructures that can be activated in the event of an outbreak of military operations.

3. Integration of Taiwan's best practices through legislations, programs and processes towards cohesive security arrangement between the two countries.

In the wake of China's escalating cyberattacks in Taiwan, emphasis was directed toward cyber defense by capitalizing the investment in resources and strengthening cybersecurity management. In Taiwan, the cybersecurity market grew to an annual rate of 14 percent per annum since 2011, increasing from USD \$700 million to USD \$1.44 billion in 2017. Following Chinese relentless attacks on Taiwanese websites and critical infrastructures in 1999, the National Information and Communication Taskforce (NICST) was created under the Executive Yuan (Cabinet) to combat cyber-attacks in January 2001.

As mentioned earlier, the NICST carried out successive phases of strategic milestones, each spanning four years – from 2001 to 2004, 2004 to 2008, and so on. The aim is to lay out the groundwork and fortify the defense of Taiwan's critical infrastructure. During these phases, the NICST evaluated the type and intensity of cybersecurity threats against each ministry. From 2009 to 2012 and 2013 and 2016, the early gains were extended to foster collaboration with the private sector, heightened public awareness, and ensured regulatory compliance of local businesses. Taiwan's ultimate goal is to defend against cyber-attacks aimed at disrupting its command-and-control, logistic supply, and even essential public services at the outset of conflict.

Education institutions were encouraged to embark on initiatives to cultivate cybersecurity literacy through curricula, coursework and specialized programs. In the next phases, the focus was refining government policies and regulation, together with supporting the cybersecurity industry and nurturing talent acquisitions. In the fifth phase (2017 to 2020), which coincided with the term of President Tsai Ing-wen, the strategic directive was to explicitly link cybersecurity and national security. Within the national security framework, cybersecurity initiatives were intensified by the Tsai Administration to address the cybersecurity attacks. These included the following:

- Create cybersecurity-mandated agencies, like the National Information and Communication Security Office (NICSO) under the National Security Council (NSC), the Department of Cyber Security within the Executive Yuan, and the Information, Communication, and Electronic Force Command under the Ministry of National Defense

- New legislations were passed, such as the 2018 Information and Communication Management Act and amendment in the National Security Act in June 2019.
- In 2021, the government launched its Cybersecurity is National Security 2.0 Strategy, which underpins the protection of critical infrastructure and other core industries.
- Established the Ministry of Digital Affairs (MODA) in 2022, which is tasked to promote digital policy innovation and reforms across the cyberdomains, such telecommunications, information, cybersecurity, and internet governance.

To integrate a comprehensive approach on all these initiatives, the MODA established a think-tank, the National Institute of Cyber Security (NICS), tasked with conducting research, providing policy recommendations and offering technical services during cybersecurity threats to public and private sectors. President Tsai personally recognized the role of NICS, further amplifying the centrality of cybersecurity as a national security interest.

Taiwan's cybersecurity strategy ensures the wide involvement of academia, industry and civil society. It encouraged fact-checking organizations, such as the Taiwan FactCheck Center and Cofacts, to combat fake news and disinformation, while digital literacy are promoted to combat cognitive warfare. The role of the private sector is crucial, with firms like Meta and Line to flag and correct false content posted in real time. Rather than censorship, Taiwan leans on openness, transparency, and citizen participation to assist in fighting cognitive warfare.

Compared to past administrations, the Tsai government embraced a heightened determination to attain cybersecurity autonomy and resilience, while transcending beyond defensive measures but into actual offensive capabilities. This changed Taiwan's cybersecurity landscape, with reliance on offensive operations against adversaries. In the wake of the complexity and myriad cyberattacks against Taiwan, the new administration saw the need to establish the Information Communication Electronic Force (ICEF), as the unit overseeing Taiwan's offensive operations. Currently, Taiwan works closely with US allies in intelligence sharing and joint military preparations.

4. Institutionalize digital forensics in the Philippine public safety and defense system to counter cyberattacks and cybercrimes

With the explosive growth of the Internet in the 1990s, China imposed draconian measures to censor free online speech and block websites favorable to the West. But aside from screening subversive speech, China was able to effectively deploy technologies to identify malicious code before it attacks critical infrastructures, enabling Beijing to defend against cyberattacks. Unlike the Philippines, our water treatment plants, power grids, and telecommunications are vulnerable to cyberattacks. There are also laws that

prohibit Philippine intelligence agencies from monitoring private actors from cyber threats, without their express consent.

Compared to Taiwan, the assessment of the country's cybersecurity program revealed some deficits and vulnerabilities during the sixth phase (2021 to 2024). The domestic cybersecurity industry was relatively small and diminutive in scale, incapable of generating competitive value. Thus, it was critical to institute measures that shall fortify Taiwan's cybersecurity and resilience. Such a posture was supported by the new president, Lai Ching-te, who continued Tsai administration's belief that cybersecurity as a cornerstone of national security policy.

To advance Taiwan's cybersecurity capabilities across all domains, the Lai administration prioritized the collaboration with international stakeholders such as Western allies. Taiwan has partnered with the United States in a joint cyber-war exercise entitled "The Cyber Offensive and Defensive Exercises (CODE)" held in 2019. Other efforts included the Talent Circulation Alliance (TCS), in conjunction with the American Institute of Taiwan, that helped in talent exchange and acquisition. In 2020, a cybersecurity forum was organized to share insights and exchanges in strategies, together with the private sector. The Lai administration has incentivized public-private partnership to expand the cybersecurity industry and cultivate more innovations. The government has also implemented various programs geared toward educating citizens about cybersecurity threats. The initiatives were demonstrated in national cybersecurity awareness campaigns that revealed sources of cyber threats, disseminated best practices for securing digital devices and personal information, and provided guidance in detecting and reporting suspicious online activities. The Ministry of Education has spearheaded in offering cybersecurity education in accessible websites and other education materials.

Today, Taiwan is using Artificial Intelligence to discover patterns and similarities in cyberattacks. Hong-wei Jyan, Director General of Department of Cybersecurity, explained:

"We cannot analyze more than 10 million cyberattacks per month. AI identifies the patterns and similar characteristics. We have also turned to Blockchain in criminal investigations to secure digital evidence," (Ming, 2022).

In addition, the passage of Taiwan's Cyber Security Management Act now mandated all firms to define in detail their cybersecurity defense and to install an incident response and recovery plan. The Department of Cyber Security conducts regular audits to ensure that they are complying with the law.

Taiwan's cyber defense is increasingly aggressive and more institutionalized due to the scale and extent of cyber-attacks. Lai's administration has redefined cybersecurity as an essential survival of the state. In April 2025, the government issued the National Cybersecurity Strategy, which provided a more proactive approach, zero-trust

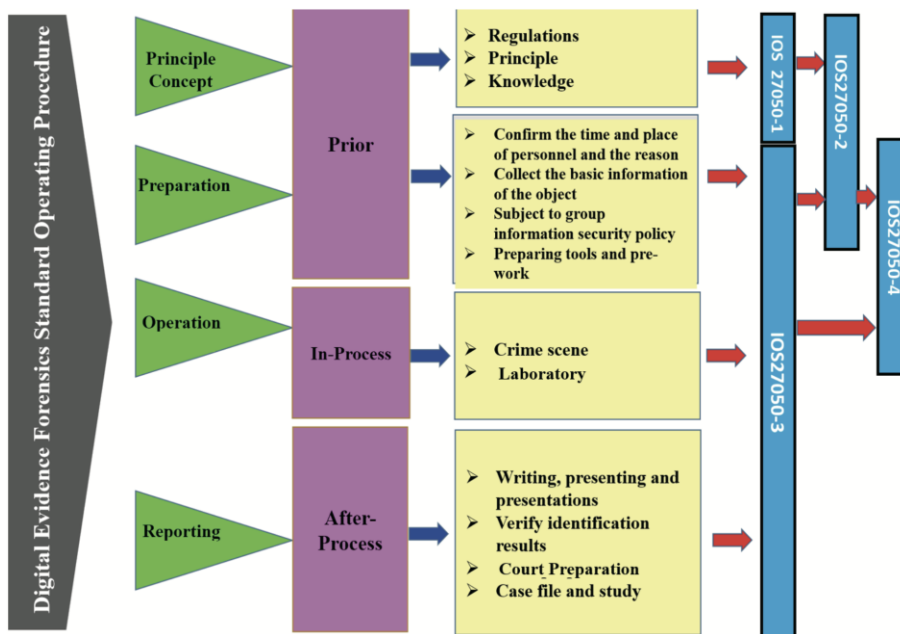
architecture, and quantum-resilient encryption, including the creation of the Joint National Cybersecurity Center.

In Taiwan, most organizations - private and public - adopted the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, which is a global standard guiding on electronic discovery. It established the process of identifying, collecting, preserving and producing electronically stored information for legal and investigative pursuits.² In the Philippines, there is a growing need for digital forensics carried out to computer systems, mobile devices, storage media, electronic files, and packets over the network, among others. Digital forensics is defined as investigating digital evidence using scientific verification and restoring the original appearance of the incident via retrieval, analysis and recovery for court proceedings (Chao-meng & I-Long, 2024). In the wake of such trilemma, the purpose of digital forensic is to find valid, admissible, and reliable evidence to prove cybercrimes and play a decisive role in related legal cases.

Meanwhile, the Digital Evidence Forensics Standard Operating Procedure (DEFSOP) is integrated into the ISO/IEC. A case in point was a cybercrime from September 2021 to March 2022 in Taoyun, Taichung in Taiwan. Through fake software, URLs and APPs were sent to different recipients using fake investment platforms, called “MCK” and “AXA Trading.” Fake information included stock prices, foreign exchange rates, and virtual current, causing US\$ 3.1 million to be siphoned from victims.

The DEFSOP has three focal areas - prior process, in-process, and after-process. Each area is subsumed under four stages - principle concept, preparation, operation and reporting. Figure 1 below provides an illustration:

² The goal of ISO/IEC 27050 is to assist organizations in conducting e-discovery in a legally defensible, efficient and secure manner. The processes reduced the risks to improper data handling, improved readiness for litigation and investigations, and aligned with broader information security purposes.



In the Philippine landscape, this Diagram gives us insight on how to institutionalize digital forensics across security agencies. In the prior-process, it covers the principles and preparation. The prior-process refers to the planning of cyber investigation related to the collection and safeguard of data to ensure its integrity and non-tampering. The in-process is the actual operation, involving five activities. These are (1) collecting and backing up digital evidence;; (2) identification and recording, (3) preservation, collection and backup, (4) search and seizure, and (5) packaging and transportation. And the after-process is when the report is made and presented as evidence before appearing in court.

Conclusion and Recommendations

In light of the foregoing discussions, this study concludes that Taiwan's cyber resilience was attributed to strong and responsive laws and governance structures, leadership support and adequate funding, private sector driven innovation, and societal involvement in cybersecurity preparedness and response. No stone was left unturned when Taiwan's Cabinet (Executive Yuan) prioritized cyber defense against China's existential threats to the island's national security.

Chinese disinformation campaigns, economic coercion and unlawful territorial incursions had intensified as Taiwan or the Philippines asserted their sovereignty. Cyberattacks can undermine the security of the entire island, causing leadership disarray, decline in social cohesion, energy shortages, and utter defeat of Taiwan military before the US 7th Fleet arrives to support the battle. As a national security approach, Taiwan believed in the principle of comprehensive security patterned after the Finnish model, one on which all vital functions of society are safeguarded jointly by government authorities, businesses, civic organizations and citizens. Thus, the national resilience was reinforced by the 2022

All-out Defense Mobilization Agency, a comprehensive management of planning for mobilization, administration, service, civil defense and building reserve capacity.

In this light, there are four classifications of strategic priorities that the Philippines can take a page from to shore up its own Cybersecurity Defense and Offense:

1. To finally operationalize the “Cybersecurity Strategic Plan” in the ground by engaging the private sector and academic institutions, together with the following activities:
 - a. Conduct industry-wide risk assessment and gap prioritization to build situational awareness
 - b. Organize the private sector in provision of resources and intelligence to combat Chinese cyberattacks
 - c. Develop key expertise in government agencies through secondment of experts from the private sector
 - d. Access and share data and intelligence across government agencies-oriented to national security and public safety
 - e. Designate a Cybersecurity Czar with competence and security of tenure
 2. To protect vulnerable critical infrastructures in the country, by:
 - a. Reviewing and amending existing laws and franchises dispensed to System Operators.
 - b. Tap other indigenous sources of electricity.
 - c. Explore alternative to undersea cables through low-earth orbit (LEO) communication satellites
 - d. Install off-island, cloud-based capabilities for data and information in the government and critical private sector.
 - e. Carryout the Self-Reliant Defense Industry Program through strong public-private partnership with key allies
 - f. Incorporate training of reserves and personnel on cybersecurity protection.
 3. To enhance cybersecurity through US support and talent acquisition
 - a. Acquire US talents to beef-up cybersecurity ecosystem
 - b. Ensure a surge in cybersecurity experts from education institution
 - c. Engage with the US Cyber Command and Taiwan’s to establish strong cyber defense
- D. Sustain cybersecurity defense through offense:
1. Conduct tabletop and simulation exercises on cyberattacks and other crisis scenarios

2. Field low-cost, proven-effective technologies, such as unmanned surface vessels, UAV, and naval mines
3. Develop offense capabilities against cyber-attacks.
4. Continue investment in defense spending to at least 1.5% to 2.0% of the GDP
5. Train local cybersecurity experts, not only on defense but offense against external cyberattacks
6. Integrate the role and participation of all sectors in Philippine society, especially academia and local government units

In Taiwan's case, the whole-of-society is essential to expand its resilience against China's growing militaristic aggression. It is a team effort, requiring the involvement of all sectors in society. But it asserts that only the central government can act as team captain, setting up the standards and expectations, narrowing down the priorities, allocating resources, and communicating and coordinating the nation's strategies. Only leaders in the national level can make all the move parts work together and fend off threats to national security.

References

- Abram, Tom (2025). *Taiwan's National Security Council: A discreet architect of the island's foreign and national security policy*. FRS.
- Chao-meng, L. & I-Long, L. (2024). Digital Forensics According to International Organization for Standardization/International Organization for Standardization 27050 and Digital Evidence Forensics Standard Operating Procedure: Use of Sensor Technology. *Sensors and Materials*, 36(6), 2315 - 2324
- Der-Tsai, Lee (2019). *Taiwan national cybersecurity strategy report*. "Cybersecurity is national security." National Security Council.
- Huang, M.-c. (2020, November 20). Taiwan is crucial to the global fight against cybercrime. Retrieved from [www.roc-taiwan.org](https://www.roc-taiwan.org/uploads/sites/157/2020/11/Taiwan-is-crucial-to-the-global-fight-against-cybercrime.pdf): <https://www.roc-taiwan.org/uploads/sites/157/2020/11/Taiwan-is-crucial-to-the-global-fight-against-cybercrime.pdf>
- Hung, T.-C., & Hung, T.-W. (2020). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies*, 7(4), 1-18.
- Kramer, F., Yu, P., Webster, J., & Sizeland, E. (2024). Toward resilience: An action plan for Taiwan in the face of PRC aggression. Atlantic Council: Scowcroft Center for Strategy and Security.
- Lee, S.-F. (2024, March 20). Decoding Beijing's Gray Zone Tactics: China Coast Guard Activities and the Redefinition of Conflict in the Taiwan Strait. *Global Taiwan*, 9(6), 6-6.

- Lin, Leo S.F. & Nomikos, John. (2018) Cybercrime in East and Southeast Asia: The case of Taiwan. A.J. Masys & L.S.F. Lin (Eds). *Asia Pacific Security Challenges* (pp. 65-84). Springer International.
- Lin, Ying-Yu. (2024) *China's cognitive warfare against Taiwan and Taiwan's countermeasures*. Taiwan Strategist No. 20
- Ming-Shih, Shen. (2024) *The development of Taiwan's asymmetric combat capabilities: A case study of the IDS and Military Interactions Between the US and Taiwan*. Taiwan Strategist No. 20
- Ming, E. L. (202, December 03). How Taiwan shores up its cyber defenses with AI and blockchain. Retrieved from govinsider.asia: <https://govinsider.asia/intl-en/article/how-taiwan-shores-up-its-cyber-defences-with-ai-and-blockchain-cybersecurity-hong-wei-jyan>
- Nd. (--). A study in Taiwan's Cybersecurity Management Act: Focus on critical infrastructure protection
- Neuberger, A. (2025, September/October). China is Winning the Cyberwar: America needs a new strategy of deterrence. Foreign Affairs.
- Slonopas, A. (2024, April 16). What Is Cyber Warfare? Various Strategies for Preventing It. American Public University. Retrieved November 17, 2025, from <https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare/>
- US Cybersecurity and Infrastructure Security Agency (CISA). (2022). Critical Infrastructure Sectors. Retrieved from <https://www.cisa.gov/topics/critical-infrastructuresecurity-and-resilience/critical-infrastructure-sectors>.
- Wu, J.-m. (2025). Great power competition in contested states: The case of Taiwan. *Asian Perspectives*, 49, 75-103.
- Yao-Chung Chang, L. (2024, February 5). Melbourne Asia Review. Retrieved from melbourneasiareview.edu.au: <https://melbourneasiareview.edu.au/taiwan-a-battlefield-for-cyberwar-and-disinformation/>

References