Cybersecurity as part of defense and security policy in Taiwan

Cybersecurity as part of defense and security policy in Taiwan

Dariia Tyshchenko

Taiwan faces growing cybersecurity threats, particularly from China, that challenge its security and democratic institutions. Taiwan has responded by investing in cyber infrastructure, expanding legal protections, and fostering public–private collaboration. It also has positioned itself as a regional leader in digital governance. However, vulnerabilities remain, including disinformation campaigns and undersea cable risks. This article examines Taiwan's current cybersecurity framework and proposes policy recommendations to strengthen coordination, protect critical infrastructure, and promote long-term resilience.

Introduction

Cybersecurity in Taiwan is not simply a technical issue but a cornerstone of its defense strategy amid escalating geopolitical threats. Taiwan is one of the global leaders in digital transformation, which uses technology to improve governance and public service delivery. However, the island faces constant pressure from mainland China, with 2.4 million cyberattacks daily in 2024, twice the amount compared to 2023 (Secretariat, National Security Bureau, Republic of China [Taiwan], 2025). The goals of the attacks vary from acquiring sensitive information for negotiations to obtaining Taiwan's tech industry trade secrets. Taiwan has also become a testing ground for cyber weapons that could later target other nations. In response, Taiwan has developed a strategy that combines active citizenship and digital democracy to counter cyber threats while differentiating itself from the mainland's authoritarian digital controls.

Taiwan is an essential player in global technology supply chains. Taiwan Semiconductor Manufacturing Company Limited alone produced ~90% of global logic chips in 2019 (Chiang, 2023). Taiwan's combining technical competencies with the advanced chip manufacturing industry makes it a key actor and a prime target in global cyberspace. Since its hardware sector is already globally dominant, Taiwan has increasingly invested in software development. The cybersecurity sector expanded 11.9% from 2020 to 2021, exceeding the worldwide average, with projected revenue of US$0.8B for 2024 (International Trade Administration, 2024). Taiwan's government also acknowledged the significance of cybersecurity. Former President Tsai Ing-Wen adopted the slogan "Cybersecurity is national security," which marked a transition from treating cyber threats as isolated technical issues to integrating them into a coordinated defense and security strategy (Office of the President, 2023).

The internet penetration rate in Taiwan, reported by the Taiwan Network Information Center, is 84.3%. Therefore, cyberattacks could immediately disrupt daily life for most citizens. Taiwan's rapid transition toward digital governance has revealed both opportunities and vulnerabilities. The National Health Insurance system, through its integrated digital network, enabled the government to track COVID-19 patients who had had contact with Diamond Princess cruise ship passengers. By linking National Health Insurance health records with customs' 14-day travel histories, authorities could identify contract points and quarantine at-risk individuals (Yen, 2020). Similarly, the health record database helped Taiwan establish a face mask rationing program during the global mask shortages. The civic technology community member Howard Wu created the Mask Map application, which utilized geolocation to show users which stores had masks in stock (Shibuya et al., 2022). While the virus containment strategy proved successful, it prompted concerns about privacy protection and system security. Centralizing personal health information and identity records created significant vulnerabilities to data breaches and unauthorized system access.

Digital governance in Taiwan does more than improve administrative efficiency; it also reinforces democratic values. The web platform vTaiwan exemplifies this dual function as a tool for public policy consultations where civil society members engage with industry professionals in public discussion. People can submit suggestions through polls, in-person meetings, and hackathons (Hsiao et al., 2018). The civic tech organization g0v also hosts Join, a petition website where proposals that gather over 5000 signa-

tures require a government response. The platforms successfully contributed to more than 20 digital policies, although critics question their effectiveness in creating substantive reforms (Ho, 2022).

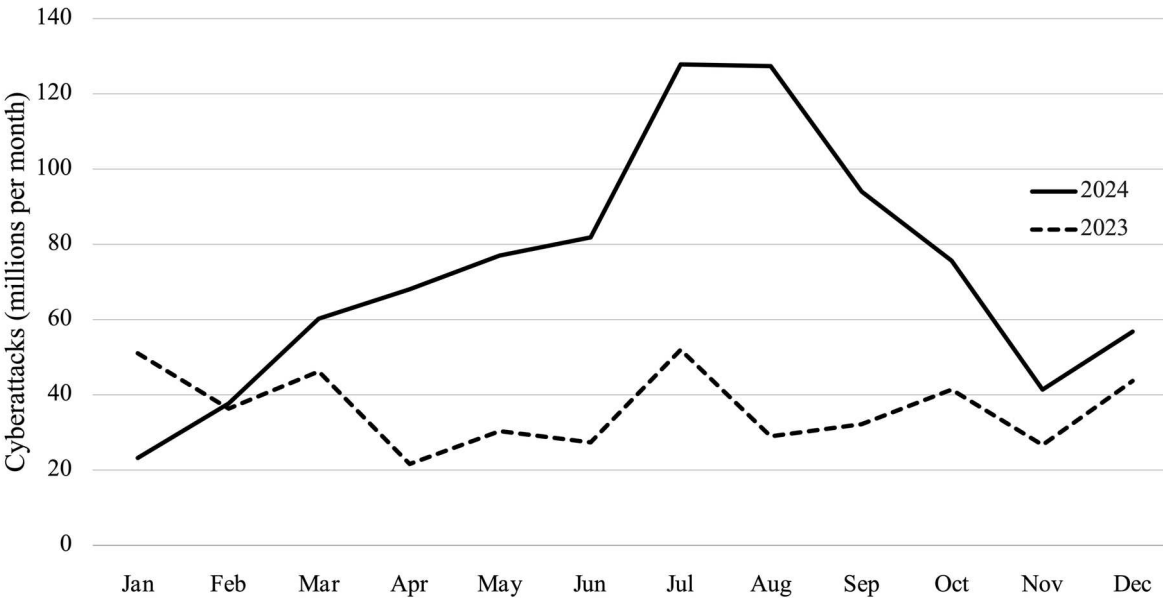
The dedication to democratic digital transformation led to the establishment of the Ministry of Digital Affairs (MODA) in August 2022. Unlike similar agencies in other countries focusing only on technological advancement, MODA must balance innovation with defending against some of the world's most sophisticated state-sponsored cyberattacks. The ministry currently leads the National Cybersecurity Strategy, working with the National Institute of Cyber Security to deploy AI-driven threat detection systems across critical infrastructure. The ministry applies big data analytics, artificial intelligence, and blockchain technology to defend against constant attacks (Ministry of Digital Affairs, 2025).

This article argues that Taiwan's integration of civic tech, democratic participation, and advanced cybersecurity infrastructure represents a distinctive model of digital resilience that not only defends against authoritarian cyber threats but also strengthens democratic governance itself. The comprehensive approach—from technical defenses to citizen engagement—leverages Taiwan's participatory values as a strategic advantage in cybersecurity.

Current cybersecurity threats

Russia's invasion of Ukraine prompted the international community to boost cybersecurity investments. Similarly, increasing geopolitical tensions led Taiwan to increase its cyber defense spending. The Presidential Office allocated NT$38.97 million for cybersecurity in 2020, representing an increase of more than 50% (Chun-hui & Hetherington, 2020). By early 2023, cyberattacks had increased 80% compared to previous years. Attackers launched 15,000 attempts per second, which made up 55% of all documented incidents within the Indo-Pacific region. As Figure 1 shows, 2024 saw yet more aggressive attacks, especially from China. The National Security Bureau registered 2.4 million cyberattacks on government networks.

Figure 1
Chinese cyberattacks on Taiwan in 2023 and 2024



Source: Secretariat, National Security Bureau, Republic of China (Taiwan), 2025.

Political events trigger higher frequencies of cyberattacks. The MODA recorded increased phishing emails and malicious links attempting to extract private information during the January 2024 elections period (Lorci, 2024). Because the elections use paper ballots, direct digital interference is impossible. However, the attackers targeted government facilities, law enforcement organizations, and financial institutions. Taiwanese government websites experienced distributed denial-of-service attacks exceeding normal traffic by 23 times when US House Speaker Nancy Pelosi visited in August 2022 (Chang, 2024).

Cyberattacks from China now target multiple essential sectors: government agencies, critical in-

frastructure, defense supply chains, and high-tech industries. Attackers exploit security weaknesses in the communication networks that civil servants depend on. Information service providers in Taiwan face an enormous surge in attacks, primarily targeting entities that handle official documents, cryptographic tools, and scheduling systems. Critical infrastructure systems encounter increasingly frequent breaches, especially targeting port and highway networks. Brute-force and ransomware attacks have been documented against academic institutions and research centers. China exploits Internet of Things device vulnerabilities to construct extensive botnets, which develop worldwide covert attack networks. The international group APT41 conducts espionage activities targeting high-tech companies for intellectual property theft. The group identifies and takes advantage of conventional software bugs that affect digital vendors' products, primarily Cisco, which specializes in networking infrastructure, and Citrix, known for its remote access and virtualization solutions (Secretariat…, 2025).

The linked network structure of Taiwan's critical infrastructure makes it susceptible to complex cyberattacks. Essential services that could be disrupted include energy, water supply, and telecommunications (Jing, 2021). Furthermore, Taiwan's governance structure faces severe risks from insider attacks, including deliberate and accidental breaches. Workers with access to private data can cause security breaches through accidental exposure or premeditated attacks.

Cyber-physical threats

The Taiwanese government faces an increasingly difficult challenge protecting its infrastructure from hybrid warfare, which blends conventional physical attacks with cyber operations. Taiwan's digital infrastructure faces significant risks due to its exposed undersea cables. Ninety-nine percent of Taiwan's digital communication flows through fiber-optic cables, with global network connectivity maintained through 14 international submarine cables and 10 domestic offshore cables (TeleGeography, 2025).

Recent events have underscored the risks that these cables face. In early 2025, the Chinese-controlled Tanzania-flagged vessel *Xing Shun 39* intentionally cut subsea cables near Taiwan's northeastern coast, disrupting external communications (Chinese Vessel Cut Subsea Cable…, 2025). The Togo-flagged *Hong Tai 58* vessel, crewed by Chinese sailors, severed Taiwan's subsea cable connecting Taiwan to Penghu (Lee, 2025). Subsea cables linking Taiwan to the Matsu Islands were cut 12 times in 2023 (Chiang, 2025). The repeated and coordinated nature of these incidents implies that Taiwan's digital infrastructure is under intentional attack. While China denies involvement, the pattern aligns with Beijing's dual-use strategy of employing civilian infrastructure—including shipping vessels and cable-laying companies—for geopolitical objectives. The US government halted the Pacific Light Cable Network project because of security concerns regarding Chinese-backed subsea cable infrastructure (United States Department of Justice, 2020).

Taiwan has established programs to diversify communication networks and decrease dependence on submarine cables. The government announced a plan to invest NT$40B in developing its low-orbit communication satellite system. The Taiwan Space Agency aims to deploy its first low Earth orbit communications satellite in late 2025, with a second following in 2026 (Po-hsuan, 2023). However, the Taiwanese space initiative has encountered obstacles due to delayed progress and insufficient resources. Meanwhile, the Taiwanese government is developing an alternative defense strategy to combat cyber-physical threats. The Submarine Cable Automatic Warning System now monitors international subsea cables, automatically triggering a warning when vessels approach. The Coast Guard Administration has pledged to enhance port inspections of foreign ships submitting deceptive entry information (Chiang, 2025).

Disinformation and the role of the civic tech community

Taiwan faces major misinformation and disinformation problems on social media platforms, such as Facebook, Line, and X (formerly Twitter). False information about politics, technological developments, and health issues erodes institutional trust and deepens political divisions. Political disinformation campaigns targeting Taiwan's elections serve Chinese objectives to damage Taiwan's democratic system (Wang, 2020). The primary purpose of traditional cybersecurity involves safeguarding systems and data, yet disinformation attacks exploit human social vulnerabilities—with destructive consequences. During the 2024 presidential election in Taiwan, Chinese-origin distributed denial-of-service attacks coincided with extensive disinformation campaigns to discredit President-elect Lai Ching-te and challenge electoral legitimacy (An, 2024).

A misinformation attack during Typhoon Jebi in 2018 against Su Chii-cherng, Taiwan's delegate to Osaka, contributed to his suicide. False reports claimed Taiwanese passengers at Kansai International Airport had to declare Chinese nationality to receive

evacuation assistance. While all passengers at the airport actually received transportation from the Japanese government regardless of nationality, these false reports spread through mainstream media. Fake posts emerged from Beijing-based IP addresses while local influencers opposing Su also participated in the campaign (Kao, 2021). While pressure from his superiors caused Su to take his own life, disinformation escalated the crisis.

Taiwan's political environment faces widespread influence from partisan misinformation. The Kuomintang received the "pro-Beijing" label after the party used manipulated images from Han Kuo-yu's presidential campaign showing supporters waving Chinese flags. During Tsai Ing-wen's presidency, fake reports spread about her 50-year cultural artifact loan to Japan and questioning her academic background (Bauer & Wilson, 2022). The narratives demonstrate how domestic actors exploit political disputes to form alliances with foreign actors.

China represents the primary source of disinformation that targets Taiwan. Chinese-origin disinformation cases increased 60% in 2024, to 2.16 million from 1.33 million in 2023. Facebook remains the leading information platform, but TikTok, Douyin, PTT, Dcard, and X are gaining popularity among younger users. AI-generated content, deepfakes, and fake accounts that use stolen media identities or hijacked credentials are at the core of these disinformation operations. Facebook identified over 28,000 fake accounts during 2024, with more than 21,000 originating on its platform (Secretariat…, 2025).

The operations executed by China have evolved to become more complex and diverse. Researchers have identified bot networks using synchronized timing, identical hashtags, and cross-platform URL-sharing mechanisms to steer trending topics toward misleading narratives like "Tsai Ing-wen surrender" and "Taiwan is China's Taiwan" (Jacobs et al., 2023). The bots leverage local controversies and divisive topics to manufacture fake grassroots support, a technique known as astroturfing. Disinformation and cyberattacks are recognized as integrated components of cognitive warfare rather than stand-alone threats. China exploits the brain's predictive systems through repeated fear-based content and deceptive information to break down mental defenses and alter political perceptions (Hung & Hung, 2022). The strategy ensures social and psychological effects endure even after successful defenses against cyberattacks, weakening democratic trust and intensifying social divides.

Taiwan has developed a robust civic tech ecosystem to address the spread of disinformation. Counter-disinformation initiatives center on groups, such as g0v, CoFacts, and Taiwan FactCheck Center. CoFacts operates within Line, Taiwan's leading messaging service, and has processed over 87,000 false information reports through human verification and machine learning methods (Rights CoLab, 2023). The Taiwan FactCheck Center conducts public workshops to teach citizens to detect deepfakes and false narratives, focusing especially on AI-generated misinformation about elections and vaccine safety (Hung, 2024).

Furthermore, the Ministry of Education published the *Digital Era Media Literacy Education White Paper*, a comprehensive policy agenda for incorporating information literacy into the official curriculum (Hung, 2024). The framework promotes critical thinking through five key components: access, analysis, creation, reflection, and action. The goal is to teach students to identify fake information and develop responsible content creation skills. This fits into a broader strategy: Taiwan's citizen-centric defense system model where all citizens are well-informed and serve as integral elements.

This resilient ecosystem emerges from the combined work of civic tech groups, ministries, industry, and educational institutions. Taiwan's experience demonstrates that disinformation transcends technology because it creates psychological and sociopolitical threats. Given regional information warfare and geopolitical tensions, Taiwan's investments in civic tech and digital citizenship are as vital as its traditional defense spending.

Domestic cybersecurity infrastructure and legal frameworks

Legal and institutional frameworks developed for digital transformation in Taiwan have elevated the island's cybersecurity resilience. The main initiative, the National Cyber Security Program (NCSP), launched by the Executive Yuan in 2017, built a systematic framework to unify Taiwan's previously fragmented cybersecurity programs and address increasingly complex cyber threats (Jakubczak & Yau, 2021).

The initial stage of the NCSP introduced a unified cybersecurity management structure by establishing the Department of Cybersecurity (DCS), real-time monitoring capabilities, and a comprehensive framework that established standards for securing critical infrastructure within the financial, energy, and health care sectors. The high number of daily cyberattacks on Taiwanese government websites during 2021 demonstrated the need for these reforms (Jakubczak & Yau, 2021).

The Taiwanese government has deployed security information and event management systems across

public sector networks to decrease security breach response times. The systems use threat data correlation to detect incidents instantly while providing real-time response capabilities. Taiwan continues to develop its cybersecurity infrastructure by adding artificial intelligence and big data analytics to boost predictive and automated capabilities (Albahri et al., 2024). AI defenses are essential considering that Taiwan's government systems face 20–40 million attacks monthly, mostly from China (Huang, 2020).

The NCSP maintains workforce development as its fundamental objective. In 2017, the DCS set a goal to reach 1224 civil servants who would be dedicated to cybersecurity, yet Taiwan had only 672 (Jing, 2019). The government addressed these workforce deficiencies by starting five cybersecurity master's programs and providing 400 hours of Ministry of Economic Affairs–funded training. The NCSP established a formal objective to increase the cybersecurity workforce by 25% by 2025 (Jakubczak & Yau, 2021).

The Cybersecurity Management Act of 2018 provided critical legal reinforcement for cybersecurity efforts. The Act compels government agencies and critical infrastructure managers to adopt standardized security controls, file yearly cybersecurity management reports, and undergo periodic evaluation (Garcia-Millan, 2019; Wang, 2024). Entities classified as Level C or above—a designation reflecting their cybersecurity responsibility based on service importance and risk level—must conduct regular penetration testing. The Act applies to financial institutions, energy facilities, water systems, telecommunications networks, and health-care organizations (Garcia-Millan, 2019). The legislation reflects industry-wide efforts to improve cybersecurity against supply chain weaknesses and AI-based threats.

Taiwan is developing advanced encryption capabilities as part of its cybersecurity approach, working to establish cryptographic methods that are secure against attacks by quantum computers and end-to-end encryption across 5G networks, which will defend against current and future quantum and AI-powered attacks (Albahri et al., 2024; Yau, 2019). These investments matter because of Taiwan's history of foreign attacks against its telecom infrastructure.

International cybersecurity collaboration

Taiwan's diverse international cooperation approach strengthens cybersecurity through technological exchanges while conveying strategic political messages. The One China policy prevents Taiwan from joining formal international cybersecurity forums, including the UN Group of Governmental Experts and the Budapest Convention, but Taiwan maintains extensive international collaborations. The US and several Indo-Pacific and European partners have significantly enhanced bilateral and multilateral cooperation with Taiwan in recent years because of Taiwan's geopolitical importance in digital security.

A major breakthrough in Taiwan–US relations occurred when both signed the 2019 Cybersecurity Cooperation Agreement, establishing mechanisms for information sharing and joint cyber threat evaluations and defense exercises (Huang, 2020; Yau, 2019). During 2019, Taiwan and the US conducted their most advanced operational collaboration, the joint Cyber Offensive and Defensive Exercise through the American Institute in Taiwan (Huang, 2020). The exercises simulate cyberattacks to assess defensive capabilities, exchange best practices, and improve operational compatibility. The Global Cooperation and Training Framework, launched by Taiwan, the US, and Japan, now includes Australia and the Netherlands, enabling Taiwan to organize workshops on cybersecurity governance, cyber hygiene, and election protection (Jing, 2019).

Through its participation in the Automated Indicator Sharing program, Taiwan joined forces with the US Department of Homeland Security to promote real-time cyber threat indicator sharing between governments and private sector partners. Major national computer emergency response teams (CERTs), including US-CERT, CERT-EU, JPCERT, and Trend Micro, signed memoranda of understanding with Taiwan to enable broader information-sharing networks (Jing, 2019).

The Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (TELWG) serves as a platform for Taiwan to participate in multilateral dialog while contributing to Asia-Pacific regional cybersecurity resilience and norm-setting efforts through its indirect influence. For example, Taiwan hosted the forty-first TELWG meeting in 2010, where delegates exchanged best practices on information and communications technology connectivity, cybersecurity frameworks, and capacity building. In addition, Taiwan's New Southbound Policy—launched in 2016 to deepen regional cooperation with 18 partner countries in Southeast Asia, South Asia, and Australasia—has incorporated digital and cybersecurity initiatives as part of its broader strategy to promote sustainable development, technological exchange, and good governance. As part of this effort, Taiwan shares expertise in critical infrastructure

protection and smart city governance with countries like Indonesia, Vietnam, and the Philippines to help bolster their digital resilience.

Recommendations

Implementing multiple regulatory reforms would strengthen Taiwan's cybersecurity infrastructure. Cyber threats evolve dynamically, so regulatory frameworks demand periodic updates to stay responsive. One such avenue is the Sustainable Development Best Practice Principles, a set of voluntary guidelines issued by the Taiwan Stock Exchange and Taipei Exchange. These principles encourage publicly listed companies—especially in the technology sector—to enhance corporate governance and risk management practices, including those related to information security and data protection. The Personal Data Protection Act must be expanded to protect users better from data misuse as data breach incidents grow more sophisticated. The island could consider enacting legal reforms to increase cybercrime penalties for attacks on critical infrastructure and government security systems.

Deepening public–private partnerships is also critical for improving Taiwan's cyber resilience capabilities. The Information Sharing and Analysis Centers in Taiwan function to support threat intelligence sharing between entities. The framework needs extension to create permanent institutions that enable time-sensitive data exchange, best practices distribution, and incident response coordination. The development of protective legal frameworks must form the foundation for securing private sector participation through mutual trust. Adoption of the MITRE ATT&CK framework—a globally recognized, open-source knowledge base of adversary tactics and techniques used in real-world cyberattacks—would improve Taiwan's threat modeling and response planning. A unified cyber coordination authority integrating MODA, the Ministry of National Defense, the National Communications Commission, and private sector representatives would strengthen multidomain attack response.

Taiwan's cybersecurity ecosystem relies heavily on civil society networks and public–private partnerships, but this collaborative approach faces several implementation challenges. The DCS supports critical sector development of Information Sharing and Analysis Centers, enabling rapid coordinated threat response (Huang, 2020). However, as these partnerships increasingly incorporate AI-powered autonomous cybersecurity tools, experts advocate modifying civil liability laws to establish proper oversight for AI penetration testing, which is becoming widespread (Wang, 2024). These legal and technological complexities are compounded by fundamental capacity constraints: Taiwan lacks sufficiently skilled cybersecurity personnel and suffers from fragmented agency oversight, while simultaneously confronting evolving threats that merge cyberattacks with disinformation operations.

The development of long-term cybersecurity capabilities requires Taiwan to dedicate substantial funding for workforce growth. Educational organizations are encouraged to establish specialized cybersecurity training programs that receive government certification and can be used in universities, vocational schools, and public service training. Combining academic training with private sector work experience apprenticeships will help bridge the gap between theoretical preparation and real-world readiness. Taiwan's workforce development needs structured changes since it lags Japan and South Korea. Elevating media and digital literacy as policy priorities enhances societal resilience. Programs must deliver training in digital ethics, content verification, and critical thinking skills across all population groups. Educator training can benefit from integrated digital skills, while civic engagement programs would incorporate media literacy training to strengthen democracy.

Taiwan should create a disinformation early warning system that combines social media monitoring with civic alert tools to identify coordinated manipulation schemes in real-time—for instance, a deepfake detection program launched in Taiwan through collaboration among civic technologists, AI researchers, and linguists to develop Mandarin language–specific open-source detection tools for culturally relevant narratives. A nonpartisan board could monitor viral content, particularly during elections. Major social media platforms, such as Meta, Line, and TikTok, would need to sign agreements with Taiwan, demanding both transparency reports and immediate takedown protocols for verified disinformation.

Permanent support for civic tech organizations, including g0v and CoFacts, can be elevated. Creating a fund to invest in digital democracy would provide resources to expand grassroots innovations that develop transparent systems and promote public engagement and service-oriented technological solutions. Pairing civic hackathons with grants enables a community to generate fresh approaches for fighting disinformation and improving e-governance platforms. Taiwan's cyber resilience strategy requires citizen-led innovation as its fundamental foundation.

The digital infrastructure of Taiwan calls for comprehensive protection against both information security threats and physical risks. Critical civilian

and military operations depend on subsea cables and satellite networks, although these systems remain highly exposed to potential threats. MODA should improve its cooperation with the Coast Guard Administration and private operators. The development of satellite-based backup systems and cable repair capabilities requires international cooperation with nations like Japan and South Korea. Working with established providers like SES and Eutelsat could accelerate satellite deployment. Such agreements must defend data sovereignty, guarantee access, and enable joint infrastructure development. The imperative to avoid foreign control during crises, especially Chinese influence, makes trusted vendor selection critical—as demonstrated by Taiwan's excluding Huawei from its 5G networks.

Global cyber competition requires Taiwan to dedicate resources to developing post-quantum cryptography, enhancing trust via understandable (i.e., explainable) AI technologies, and ensuring 6G network integrity and software supply chain security. A diverse range of funders are available to support R&D projects, including government agencies, universities, and private sector leaders. Taiwan's establishment of a cybersecurity innovation hub would serve as a coordination center to manage funding, pilot applications, and accelerate technology commercialization.

Taiwan needs to strengthen international technological cooperation despite diplomatic constraints. MODA has to expand Taiwan's Global Cooperation and Training Framework participation through dedicated tracks on cloud sovereignty, data protection, and disinformation response. Establishing formal bilateral cyber training programs with Taiwan and democratic allies (Japan, Australia, and the Netherlands) should occur as part of regional cybersecurity summits and defense exercises. MODA could also lead the establishment of a digital foreign service corps to deploy cybersecurity specialists in diplomatic missions for technical dialogue, intelligence sharing, and incident response coordination. Taiwan can position itself as a regional leader by providing technical support for Southeast Asian partners regarding digital governance, incident reporting, and cyber hygiene to promote democratic cyber stability in the region.

Finally, Taiwan should create a civilian cyber guard reserve corps, modeled after Estonia's Cyber Defense League. Through this initiative, Taiwan would engage private sector and academic experts to support defense preparedness during emergencies, enabling adaptable and flexible responses. This reserve force would function both as an operational asset and as a potent symbol of citizen unity against cyber threats.

Conclusion

Taiwan is a powerful global actor that unites democratic governance with digital protection as cyber threats escalate worldwide. The island operates an extensive cybersecurity framework defending against continuous politically motivated attacks on data systems, physical facilities, and information integrity. By implementing advanced technological defenses, civic participation, regulatory reform, and international cooperation, Taiwan has created a decentralized cybersecurity framework enabling robust civil society participation. Within this system, media literacy education is a critical component of defense and security. This democratic digital resilience model contrasts sharply with authoritarian approaches, which makes Taiwan an important research subject.

Taiwan's cybersecurity strategy development requires persistent evolution for sustained effectiveness. The development of quantum computing, generative AI, and hybrid warfare demands adaptation beyond traditional firewalls to include predictive defense and cross-sector collaboration. The success of cybersecurity depends on uniting threat intelligence across multiple domains. Taiwan should keep investing in securing its infrastructure and in training a cybersecurity workforce capable of addressing both technical and ethical challenges.

References

Albahri, A. A., Yaseen, M. G., Aljanabi, M., Ali, A. H. A. H., & Kaleel, A. (2024). Securing tomorrow: Navigating the evolving cybersecurity landscape. *Mesopotamian Journal of CyberSecurity*, *4*, 1–3.

An, A. (2024). *Cyberattack on democracy: Escalating cyber threats immediately ahead of Taiwan's 2024 presidential election*.

Bauer, F., & Wilson, K. L. (2022). Reactions to China-linked fake news: Experimental evidence from Taiwan. *The China Quarterly*, *249*, 21–46. doi:10.1017/s030574102100134x

Chang, L. Y. (2024). Taiwan: A battlefield for cyberwar and disinformation. *Melbourne Asia Review*, *2024*, *17*.

Chiang, M. (2023). Taiwan semiconductor manufacturing company: A key chip in the global political economy. *East Asian Policy*, *15*, 36–46. doi:10.1142/S179393052300003X

Chinese vessel cut subsea cable near Taiwan: Report. (2025, January 7). *Taipei Times*.

Chun-hui, Y., & Hetherington, W. (2020, December 28). Presidential office budget for cybersecurity up 50%. *Taipei Times*.

Garcia-Millan, T. (2019). Modernizing Taiwan's legal framework to drive a digital transformation. In B. S. Glaser, M. P. Funaiole (Eds.), *Perspectives on Taiwan: Insights from the 2018 Taiwan-US Policy Program* (pp. 3–9). Rowman & Littlefield.

Ho, M. (2022*). Exploring worldwide democratic innovations: A case study of Taiwan's civic tech movement*. European Democracy Hub.

Hsiao, Y., Lin, S., Tang, A., Narayanan, D., & Sarahe, C. (2018). *vTaiwan: An empirical study of open consultation process in Taiwan*. Center for Open Science. doi:10.31235/osf.io/xyhft

Huang, H. (2020). A collaborative battle in cybersecurity? Threats and opportunities for Taiwan. *Asia Policy, 15*, 101–106. doi:10.1353/asp.2020.0015

Hung, T., & Hung, T. (2022). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies, 7*, ogac016. doi:10.1093/jogss/ogac016

Hung, W. (2024, March 6). *Media literacy education: Taiwan's key to combating disinformation*. Global Taiwan Institute.

International Trade Administration. (2024). *Taiwan - cybersecurity*.

Jacobs, C. S., Ng, L., H. X., & Carley, K. M. (2023). Tracking China's cross-strait bot networks against Taiwan. *16th International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation* [Conference paper] (pp. 115–125). doi:10.48550/arXiv.2310.10851

Jakubczak, W., & Yau, H. (2021). TRENDS IN CYBERSECURITY REGULATIONS OF TAIWAN (REPUBLIC OF CHINA) – Phases of promotion of major cyber security plans and programs in the national cyber security program of Taiwan (2021–2024). *Scientific Papers of the Main School of the Fire Service 1*, 199–216. doi:10.5604/01.3001.0015.6485

Jing, B. (2019). Cybersecurity as a sine qua non of digital economy: Turning Taiwan into a reliable digital nation? In Y. Tatsumi, P. Kennedy, & J. Li (Eds.), *Taiwan Security Brief: Disinformation, Cybersecurity, & Energy Challenges.* (pp. 23–35).

Jing, B. (2021). Cybersecurity is national security: Can Taiwan have the digital cake and eat it too? In Y. Ma (Ed.), *Chinese (Taiwan) yearbook of international law and affairs* (Vol. 38, pp. 120–137). Brill. doi:10.1163/9789004501638_006

Kao, S.-S. (2021). *Taiwan's response to disinformation: A model for coordination to counter a complicated threat.* National Bureau of Asian Research.

Lee, Y. (2025, January 6). Taiwan says Chinese ship broke subsea cable in alleged sabotage. *Insurance Journal*.

Lorci, E. (2024). The nexus of cybersecurity and national security: Taiwan's imperatives amidst escalating cyber threats. *Global Taiwan Institute.*

Ministry of Digital Affairs. (2025, March 13). *The Ministry of Digital Affairs continues to strengthen digital resilience and innovation, establishing a trusted digital economy highway network.*

Office of the President, Republic of China. (2023, September 18). *President Tsai meets US cybersecurity business development mission*.

Po-hsuan, W., & Hetherington, W. (2023, February 26). Nation to launch first low earth orbit satellite in 2025. *Taipei Times.*

Rights CoLab. (2023, September 28). *Cofacts.*

Secretariat, National Security Bureau, Republic of China (Taiwan). (2025). *Analysis on China's cyberattack techniques in 2024*.

Shibuya, Y., Lai, C., Hamm, A., Takagi, S., & Sekimoto, Y. (2022). Do open data impact citizens' behavior? Assessing face mask panic buying behaviors during the covid-19 pandemic. *Scientific Reports, 12*, 17607–y. doi:10.1038/s41598-022-22471-y

TeleGeography (2025). *Submarine cable map*.

US Department of Justice. (2020, June 17). *Team Telecom recommends that the FCC deny Pacific Light Cable Network System's Hong Kong undersea cable connection to the United States*.

Wang, T. (2020). Does fake news matter to election outcomes? The case study of Taiwan's 2018 local elections. *Asian Journal for Public Opinion Research*, *8*, 67–104. doi:10.15206/ajpor.2020.8.2.67

Wang, W. (2024). Legal, policy, and compliance issues in using AI for security: Using Taiwan's cybersecurity management act and penetration testing as examples. *16th International Conference on Cyber Conflict* [Conference paper], 161–176.

Yau, H. (2019). An assessment of cyberpower within the triangular relations of Taiwan–US–China and its implications. *International Journal of Taiwan Studies*, *2*, 264–291.

Yen, W. (2020). Taiwan's COVID-19 management: Developmental state, digital governance, and state-society synergy. *Asian Politics &Policy*, *12*, 455–468. doi:10.1111/aspp.12541

DARIIA TYSHCHENKO

Dariia graduated with highest honors from Lehigh University in May 2025 with a B.S. in computer science and a minor in economics. While at Lehigh, she worked as a teaching assistant, served as the president of the Ukrainian Association, codeveloped an application about sustainability as a Global Social Impact Fellow, and participated in Lehigh's Startup Academy. Additionally, she conducted research on blockchain technology, focusing on zero-knowledge proofs. Dariia is currently working as a software developer and plans to pursue graduate education in technology and policy.