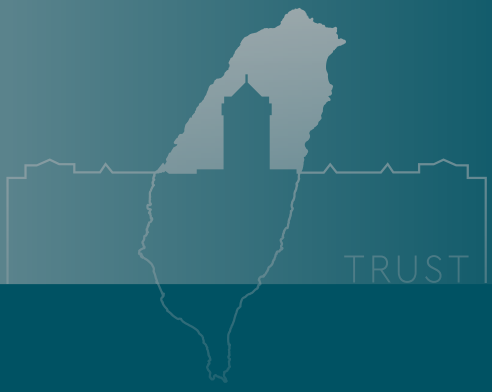
NATIONAL CYBERSECURITY STRATEGY 2025

Cybersecurity is National Security

building a resilient, secure,
and trustworthy smart nation



NATIONAL SECURITY COUNCIL

National Information and
Communication Security Office
April 2025

National Cybersecurity Strategy 2025

Cybersecurity is National Security

PRESIDENT'S FOREWORD

Recent major global events, including the Wuhan pneumonia epidemic, the Russia-Ukraine war, ongoing geopolitical conflicts, the US-China trade tensions, and technological blockades, have shown that democracy, freedom, security, and the development and application of information technology are reaching a critical intersection, which is a major crisis and turning point for both the global democratic coalition and Taiwan. In the changing global situation, the war in the digital domain has already begun. Some countries in the world exploit technology in ways that run counter to universal values. Information technology is used by state power both for domestic surveillance and control of the population, and as a tool of external aggression to attack and infringe on the sovereignty of other countries, with the intention of paralyzing the normal operation of democratic governmental agencies and infrastructure, steal national secrets and corporate intellectual property, expropriate personal assets, violate privacy, and launch sophisticated cognitive warfare. These operations are cloaked in lofty rhetoric to conceal distorted narratives, enhanced by AI-generated content, be it audio, video, graphics or text, designed to obscure the perception of right and wrong, good and evil, and to incite conflict, division, and social unrest.

Taiwan is the best exemplar of freedom, democracy, and prosperity. However, freedom and national security are closely interdependent. Freedom built on a crumbling foundation of national security is inherently fragile. Ignorance and neglect of cybersecurity pose one of the greatest threats to national security. Malicious and hostile foreign forces are exploiting our goodwill and deeply held values of freedom to infiltrate our homes through a digital battlefield, one that is without smoke or bloodshed. Each of us is inevitably a part of this battle. Although the government has made sustained efforts to promote cybersecurity over the years, the rapid pace of technological advancement has dramatically led to a more severe cyber threat landscape. Existing systems, organizations, laws, and regulations are no longer adequate to address or defend against these emerging challenges. Inaction, hesitation, retreat, or appeasement only send the wrong signal. Incremental changes can no longer cope with this urgent crises. At this critical juncture, leading countries

in the global democratic coalition are introducing bold strategic plans and new organizational frameworks, mobilizing industries, businesses, and citizens to strengthen their collective cybersecurity capabilities. The development of Taiwan's *National Cybersecurity Strategy 2025* is firmly rooted in this global context. The real threat emerges when we let our guard down. Only by preparing fully and ahead of time can we deter the growing reach of adversarial forces.

The cost of maintaining freedom and security is necessary and worthwhile. The four pillars, i.e., Whole-of-Society Defense Resilience, Homeland Defense and Critical Infrastructure, Key Industries and Supply Chains, and Application and Security of Artificial Intelligence, are designed not only to strengthen cybersecurity and the capacity of national security, but also to protect the democracy, freedom, stability, and prosperity that our people deeply cherish. More importantly, they aim to safeguard the well-being of future generations. In this effort the role of government is pivotal. We must call on all government agencies, institutions, and public facilities to take initiative and actively fulfill their responsibilities. Strengthening cybersecurity regulations should not be seen as a constraint on freedom, but rather as a protective shield that defends both our liberties and our digital homeland. In addition to the government's full mobilization of talent and technology to strengthen cybersecurity and the capacity of national security, it is equally vital to remind the public that no weapon is more powerful than a citizenry equipped with strong cyber awareness. Building cyber awareness at both personal and organizational levels across daily routines and enterprise operations bolsters the nation's collective ability to resist adversarial threats. Every individual plays a part: through verification, fact-checking, timely reminders, responsible rejection of suspicious content, and digital self-discipline, we can all contribute to enhancing Taiwan's cybersecurity resilience and securing victories in this ongoing digital battle. For instance, businesses should continue to improve cybersecurity management and operational resilience by avoiding the use of questionable information and communications technology (ICT) devices. Individuals should avoid sharing personal information or trusting unverified social media platforms and mobile

apps. They should also not to spread misinformation or disinformation, and resist the temptation to shop on websites that compromise user privacy in exchange for low prices and convenience. All our people of Taiwan, please help your elders, guide your children, and remind your friends to make cybersecurity a daily priority. Let us turn cyber awareness into a shared habit and a way of life. Together, we can foster a culture where cybersecurity is valued and practiced by all. This is the true spirit of building a resilient whole-of-society defense.

As a critical link in the global democracy supply chain and a frontline defender of democracy, Taiwan has long been a primary target of infiltration and cyberattacks by hostile foreign forces. In response cybersecurity has become a strategic focus for advanced democracies and their key partners. For Taiwan this moment also presents a vital opportunity to strengthen and grow our own cyber industry. We must encourage our citizens to remain vigilant and not panicked, cautious but not fearful. Cybersecurity is closely tied to our personal assets, privacy, and even physical safety. We must clearly understand both our adversaries and ourselves. We cannot allow those who seek to undermine our freedom and stability to succeed or shake our collective resolve. This strategy represents more than just a forward-looking plan for national and societal cybersecurity; it is a call for unified cooperation with strategic partners in the democratic world to counter today's increasingly coercive threats. More importantly, it is a firm commitment to protecting our nation, our society, industry, and every individual citizen. The ultimate goal of national security, or the essence of cybersecurity, is to safeguard the values we hold most dear, of freedom, prosperity, openness, and safety. The time to act is now.

THE PRESIDENT Lai, Ching-Te

MARCH 28, 2024

CONTENTS

INTRODUCTION: Incremental changes can no longer cope with urgent crises

Background

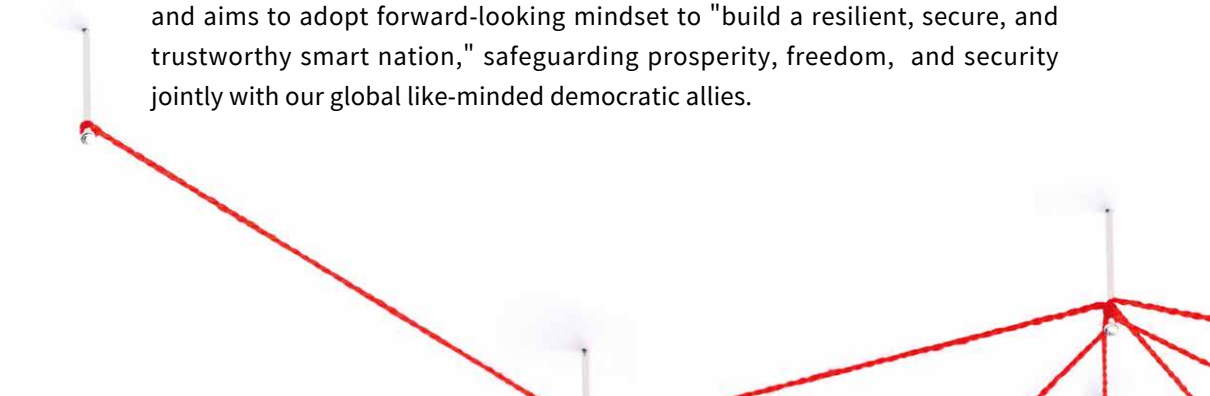
With the deepening of global digitalization and the gradual popularization of emerging technologies, information and communications security, or cybersecurity has ranked among the top ten major risks in the world (World Economic Forum 2024), and has become a crucial component in national security. Hacking and attacks on information and communications systems not only pose a major threat to national security, but also present the characteristics of grey zone conflicts which continue to raise challenges to regional peace and stability.

When the Russia-Ukraine war broke out in 2022, cyberattacks against critical infrastructure became the prelude to large-scale physical military actions. In the same year, Nancy Pelosi, then Speaker of the United States House of Representatives, visited Taiwan, which induced internet intrusions and cyberattacks to websites across Taiwan's public and private sectors. Hackers spread threatening messages through electronic billboards and attempted to paralyze various application services, highlighting the importance of cybersecurity protection in maintaining normal operation of the government and society. In 2023, Microsoft revealed that a state-sponsored hacker group known as Volt Typhoon was trying to take over Guam's critical infrastructure. The intentions behind it triggered high alert in the United States. In 2024, the United States once again revealed that a hacker group known as Salt Typhoon had invaded at least nine telecommunications operators in the United States in an attempt to spy on then-presidential candidate Donald Trump and other high-ranking politicians and to steal national security information. In the same year, remote-controlled explosions of pagers and walkie-talkies occurred in the Middle East, as well as an unexpected software update flaw released by cybersecurity company CrowdStrike, caused millions of computers around the world to crash, exposing the risks hidden in the highly complex and interdependent information and communications supply chain. On the other hand, the rapid development of artificial intelligence (AI) not only brings various innovative applications, but also significantly increases the AI-driven cyber threats. These threats include using automation technology to improve

attack efficacy and expand the scale of attacks, using generative AI to create more realistic audio, video, image and text content to deceive targets, or conduct social engineering attacks. Even the vulnerabilities of the AI system itself have become an emerging target for hackers, bringing unprecedented risks. As for the burgeoning of quantum computers and development of quantum technology, its powerful computing power will pose a fatal threat to the current, widely used public key cryptosystem in the future, which may lead to large-scale leakage of state secrets and exposure of personal privacy. These cases and emerging technologies development trends demonstrate the essence of "cybersecurity is national security" and the urgency of the cyber threat.

Today, China's various actions in cyberspace are arousing high alert in the international community. According to analysis reports from cybersecurity companies and information disclosed by the media, cyberattacks from China have spread all over the world. The United States, the United Kingdom, Japan and other countries have all reported that critical infrastructures and research institutions have been targeted and infiltrated. These behaviors not only threaten regional security, but also challenge the global order, confirming that cyber threats have no borders and are not subject to the existing legal framework. The threat faced by Taiwan is particularly serious. As pointed out by the National Security Bureau (NSB) in "Analysis of Chinese Communist Party's (CCP) Cyber Hacking Techniques in 2024", the average number of daily intrusions on our Government Service Network (GSN) in 2024 was 2.4 million, which is twice of that in 2023- 1.2 million. Most of them were committed by the CCP's cyber force. Although many of them have been detected and effectively blocked, they still highlight that the overall situation of cyberattacks is becoming increasingly severe. In addition, the national security intelligence showed that 906 hacking incidents in both public and private sectors in Taiwan were detected last year. Compared with 752 incidents in 2023, the growth rate reached more than 20%. Among them, government agencies are the highest hacking targets, accounting for more than 80% of the overall total. Analyzing the hacking targets of the CCP's cyber force, we find that the most growth rates occur in the sectors of communication (mainly the telecommunications industry), transportation and defense supply chain, and these sectors have obviously become the focus of the CCP's emerging cyberattacks.

In view of increasingly serious cyber threats, the National Security Council (NSC) proposed Taiwan's first cybersecurity strategy report in 2018: The *National Cybersecurity Strategy Report – Cybersecurity is National Security (hereinafter referred to as Cybersecurity is National Security 1.0*), This led to the establishment of the Cyber Security Department of the Executive Yuan and the promulgation and implementation of the Cybersecurity Management Act. Cybersecurity is National Security Strategy 1.0 focused on building government's organizational infrastructure for cybersecurity policy implementation, advocating intelligence-driven cybersecurity framework and protection mechanism, and promoting international cooperation. In 2021, NSC launched *Cybersecurity is National Security 2.0* to strengthen public-private partnerships, improve protection resilience, build proactive defense capacity, and expand international cooperation. At the same time, it provided an impetus for the establishment of Ministry of Digital Affairs and set up a closely coordinated Six Basic Joint Defense Agencies. As the global landscape changes and emerging technologies continue to develop, various types of cyber threats and risks are growing rapidly. Our democratic allies are allocating more resources and accelerating the adjustment of government organizations and trained personnel to actively respond. Taiwan is located at a geopolitical hub that faces more severe nation-state cyber threats. Incremental changes are no longer able to cope with urgent crises. Comprehensive changes are urgently needed to greatly enhance the capacities and resilience of cybersecurity defense in order to protect the national values and achievements of democracy, freedom and industrial prosperity. Therefore, in order to further ensure and strengthen national security, the NSC proposed the *National Cybersecurity Strategy 2025, which aligns with the vision of President Lai's National Project of Hope: Innovative Economy, Smart Nation*, promoting the development of the Five Trusted Industry Sectors and the Whole-of-Society Defense Resilience, and aims to adopt forward-looking mindset to "build a resilient, secure, and trustworthy smart nation," safeguarding prosperity, freedom, and security jointly with our global like-minded democratic allies.



Threat Landscape and Key Challenges

(As depicted in Figure 1)

I. Rapidly Rising External Threats

First of all, there are nation-state cyber threats. The threat posed by state-sponsored hacker groups is growing day by day, with critical infrastructure and government agencies being the main targets. These hacker groups have abundant resources, and are often professionally trained, capable of using sophisticated tools and techniques to conceal their activities. They often exploit the vulnerabilities of information and communications technology (ICT) supply chain to infiltrate, which greatly increases the difficulty of detection and defense. They usually lurk in the victim's network environment for a long time, waiting for opportunities to steal sensitive information or carry out further actions, for example, by leaking confidential information to media at a critical moment to undermine the government's credibility.

Second, there is the challenge posed by emerging technologies. The rapid development of AI technology is profoundly reshaping the cybersecurity landscape. The powerful computing and analytic capabilities of AI allow hackers to detect vulnerabilities more quickly, automate attack processes, and even generate highly convincing phishing emails and social engineering tactics to break through traditional defense mechanisms. On another front, the advent of quantum computers, although not yet commercially available, will pose additional challenges as their computing power will subvert existing cryptographic protocols. In the future, quantum computing technology may easily crack the current, widely-used cryptographic algorithms, causing unprecedented challenges to the security of communication systems, financial transactions, and state secrets. As technology competition intensifies, how to respond to AI-driven intelligent attacks and quantum computing threats in the future has become a core issue in global cybersecurity strategies.

Finally, cybercrime continues to be rampant. Cybercriminal activities pose

multiple threats to personal, corporate and national security. In particular, ransomware attacks have repeatedly escalated, with hackers encrypting victims' important data and demanding huge ransoms, and even threatening to disclose sensitive information, causing victims' huge economic losses and distrust of cyberspace. At the same time, from compromised business emails to phishing websites, new scams and online fraud techniques keep emerging to hack personal privacy information. What is even more concerning is intellectual property espionage, where hacker groups infiltrate corporations and R&D institutions to steal key technologies and business secrets, causing immeasurable damage to industrial competitiveness and national interests.

II. Internal Challenges to Be Solved Urgently

It is an urgent task to continuously improve the objectives, capabilities, and resilience of incident response. Since the implementation of the *Cyber Security Management Act*, the public sector and critical infrastructure have established a solid foundation for cybersecurity protection to a certain extent. However, in the face of increasingly complex threats, more resources still need to be allocated, and efforts made to strengthen the security and operational resilience. Regulatory compliance and cyber governance measures such as pre-event checking and protection, during-event notification and response, post-event evaluation for continuous improvement, and information sharing must be fully implemented. In addition, to effectively respond to major cyber incidents related to national security, the overall coordination mechanism and collaborative efforts across ministries need to be continuously optimized to ensure that incident response can be more efficient, more effective and more resilient.

Furthermore, as the demands for connectivity and interoperability among Taiwan and its strategic partners continue to increase, cybersecurity has become a key element in solidifying the foundation for cooperation. Effectively preventing data leakage, mitigating insider threats, improving personnel security checks, and establishing secure and trustworthy communication channels among government agencies are all important issues that cannot be ignored. Through cooperation with international partners in public and private sectors in improving

the cybersecurity intelligence sharing and application, we can further strengthen Taiwan's cybersecurity protection capabilities and provide a solid foundation for deepening strategic partnerships.

Finally, proactive defense is also a core strategy of cybersecurity protection. The purpose of proactive defense is to increase the cost of hacker intrusions and maintain an effective deterrent. Relevant measures include blocking attacks in advance through data collection and intelligence analysis, as well as combining continuous threat hunting to proactively identify advanced threats lurking deep within the network. Through attribution methods, public-private partnerships and international cooperation, we can expose hacking schemes and sources, attribute attacks, and hold hackers accountable. Depending on the severity of the incident, necessary actions and measures will be taken in a timely manner. The full implementation of proactive defense requires clear strategic goals, professional technical skills, and sufficient resource investment, and is not only the key to dealing with current cyber threats, but also the cornerstone of future digital resilience.

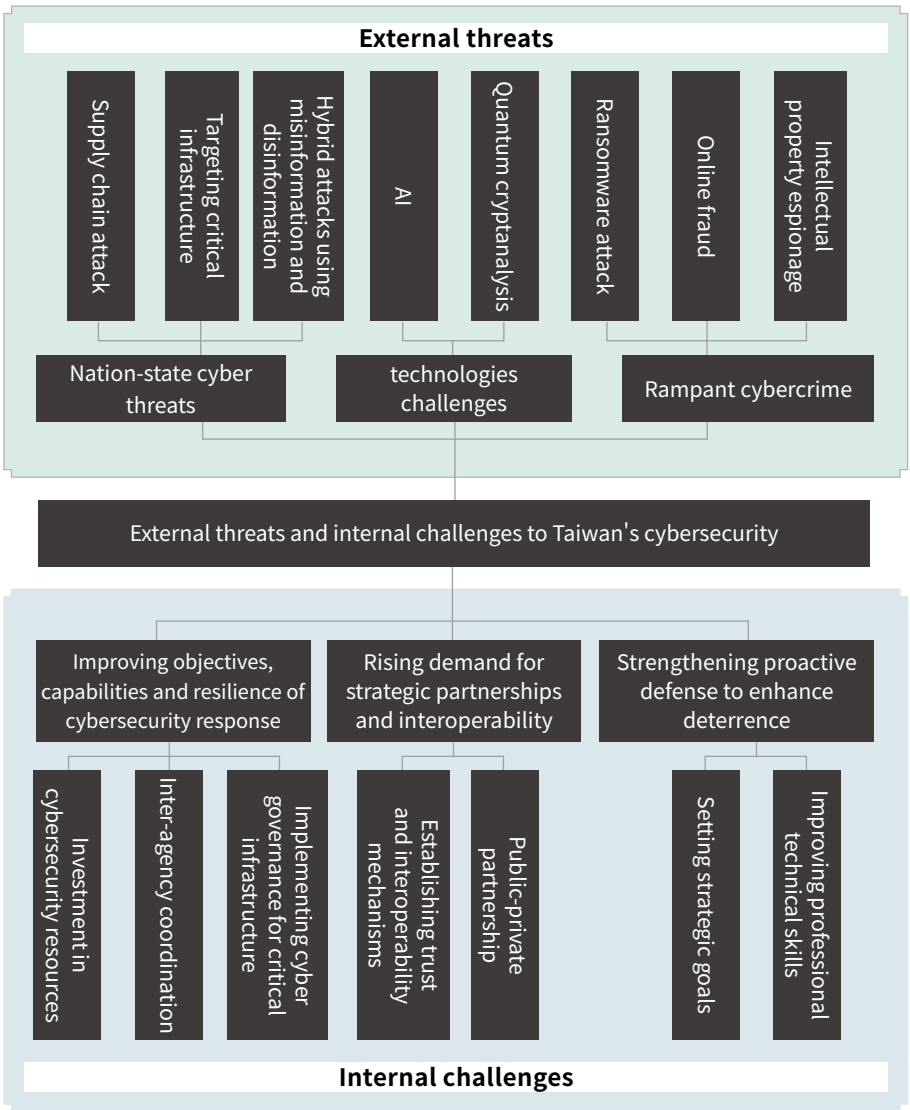


Figure 1. Taiwan's external threats and internal challenges

Strategic Context

I. Strategic Forward-Looking Development

This strategy is consistent with the current governmental policies. In his inauguration speech, President Lai particularly emphasized that in the face of various threats and infiltrations from China, we must demonstrate our determination to protect our country, raise our awareness to protect Taiwan, improve the legal systems of national security, and strengthen democratic resilience. Economically, the *Five Trusted Industry Sectors,* semiconductors, AI, military industry, security control, and next-generation communications, will be comprehensively promoted. President Lai further announced the establishment of the Whole-of-Society Defense Resilience Committee at the press conference on the first month of his inauguration, which will not only promote the expansion of capacity training and utilization of civilian power but also enhance the security of energy and critical infrastructure, as well as the stability of ICT, transportation and financial networks. The Committee seeks to strengthen the resilience of four major elements, national defense, people's livelihood, disaster prevention, and democracy, and build a robust democratic society, comprehensively safeguarding national security.

In addition, Taiwan is the key to the global "democratic supply chains" and must promote industrial AI and utilize AI to enhance national and military power. Premier Cho Jung-tai of Executive Yuan also revealed the contents of the *National Project of Hope* in his policy address, including the *Innovative Economy, Smart Nation*, building a resilient Taiwan, and maintaining security and peace.

II. Continuity of Previous Strategies

In correspondence with the promulgation and implementation of the *Cyber Security Management Act* and the ensuing establishment of the Information, Communications and Electronic Force Command and the Ministry of Digital Affairs, the NSC published the *Cybersecurity is National Security Strategy 1.0* and the Tri-Pillar Cybersecurity Coordination Mechanism in 2018, and subsequently

the *Cybersecurity is National Security Strategy 2.0* and the Six Basic Joint Defense Agencies in 2021, which proposed forward-looking strategic plans for safeguarding national cybersecurity, and established a national security joint defense system that integrates network situation monitoring, cyber incident response, and threat information sharing.

Today, built upon the solid foundation and framework established in the previous stages to cope with the ever-changing cyber threats, it is necessary to invest more resources to improve cybersecurity combat readiness and capabilities, to initiate the thinking of joint defense of the whole society and key industries, and to continue realizing the vision of building a resilient, secure, and trustworthy smart nation.

III. Strategic Response to Global Trends and Emerging Technologies

The World Economic Forum published its Global Risks Report 2024 that reveals growing global risks and crises. Cyber insecurity, misinformation and disinformation, international conflicts, and other issues will rank at the forefront of global risks over the next decade. The Russia-Ukraine war and the conflicts between the United States and China have caused the geopolitical instability, while technological advancement, and particularly the development of AI have also contributed to the escalation of cyber threats. National cybersecurity strategy must be strengthened accordingly as a response to the increase of various risks.

IV. Cybersecurity as the Foundation for Strategic Partnerships

Taiwan is the first gatekeeper of world peace [1] and the most important line of defense for the democratic coalition. Cooperation with our advanced, key strategic partners is crucial. To ensure comprehensive cybersecurity protection for national defense, government agencies, and critical infrastructure, strategic thinking must be first aligned and synchronized with our key partners, and plans, actions, system equipment, education, and personnel training must meet the standards of interoperability. This includes ensuring that systems and protocols are compatible and can exchange information seamlessly, allowing for coordinated responses to threats. Moreover we must implement our partners' forward-looking strategic plans more effectively. Only in this way can mutual trust be built and enhanced and close cooperation relations be maintained.

V. Global Cyber Threat Assessment and Trends of Cyber Strategy

In the planning process of this strategy, in addition to responding to the trends of evolving global cyber threats, we also reference relevant strategies, policies,

[1] Chiang Wei-Shui, *Clinical Lecture Notes— Diagnosis of a Patient named Taiwan*. In *Complete Works of Chiang Wei-Shui*, ed. Xiaobo Wang, Straits Academic Press, Taipei, 2005, pp.3-6.

and regulatory frameworks of various countries to ensure that it is proactive and aligned with international standards and best practices. Taking the United States as an example, the *2023 National Cybersecurity Strategy* advocates the establishment of a more secure and resilient cyberspace that aligns with the values of the United States and its allies. It emphasizes the redistribution of cybersecurity responsibilities to more capable entities, such as large enterprises, suppliers, and cloud operators, rather than allowing small and medium-sized enterprises and end users to bear excessive risks. At the same time, incentives are adjusted to promote long-term security investment to build a more defensive and resilient digital ecosystem in the future. Therefore, the U.S. strategy proposes five pillars, including strengthening infrastructure cyber defense capabilities through public-private partnership such as the Joint Cyber Defense Collaborative (JCDC); comprehensively combating and dismantling cyber threat actors through law enforcement, economic sanctions, and international cooperation; and ensuring that suppliers implement Secure by Design (SbD) principles through legislative regulations. This includes setting mandatory security requirements for Internet of Things (IoT) devices, adopting safer software development standards, and improving software supply chain transparency. The strategy also emphasizes investing in the research and development of advanced cyber security technologies, including AI, Industrial Control Systems, Cloud Computing, Post-Quantum Cryptography, and promoting the introduction of Zero Trust Architecture; and deepening international partnerships.

In 2025, US former President Biden issued the *Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity (EO 14144)*, further naming China as the most active and persistent cyber threat to the United States. President Trump has also emphasized the need for "modern laws to confront modern threats." The initiative aims to strengthen national security, protect critical infrastructure, combat online crimes such as ransomware attacks and data breaches, enhance public-private partnerships, and mandate stricter reporting requirements for cyber incidents.

The UK's *National Cyber Strategy 2022* focuses on five pillars. First, it aims to strengthen the national cyber ecosystem by cultivating a diverse pool of cybersecurity professionals and supporting innovative industries through cooperation among the government, academia, and industry. Second, it seeks to build a resilient and prosperous digital nation by reducing cyber risks and enhancing the cyber awareness and protection capabilities of both enterprises and citizens. Third, it emphasizes leadership in the development of key cyber technologies, advancing the country's competitive edge in science and technology to ensure the security of critical technologies and infrastructure. Fourth, it calls for enhancing global leadership, promoting global cyber governance, supporting a free, open, and secure cyberspace, and strengthening the cybersecurity defense capabilities of international partners. Finally, it underscores the need to detect, combat, and contain malicious activities using a full spectrum of tools to protect national security and respond to nation-state cyberattacks and cybercrimes. On the other hand, officials also pointed out that the most common cyber threats in 2021 came from Russia and China. The UK government also believes that China possesses advanced cyber technology capabilities and has shown a high degree of interest in the UK's commercial secrets. The UK assesses that over the next decade, China's digital development and growing global influence will be one of important considerations in the UK's efforts to strengthen its cybersecurity defenses.

In the *2023-2030 Australian Cyber Security Strategy*, Australia proposed to become a global cybersecurity leader by 2030, adopting six "cyber shields" to protect citizens and businesses from cyber threats and strengthen resilience for rapid response and recovery. The essence includes strengthening the protection capabilities of citizens and businesses, promoting the safe use of emerging technologies, establishing a world-class threat information sharing and blocking mechanism, protecting critical infrastructure, developing local cybersecurity capabilities and talent, and enhancing regional and international cyber resilience and leadership. The strategy is implemented in three phases: 2023-2025 to consolidate the foundation, 2026-2028 to enhance overall cyber maturity, and 2029-2030 to lead the development of global cyber technologies while promoting public-private partnership and legislative reform to realize the vision.

Since the Network and Information Systems Security Directive (NIS2 Directive) came into effect in January 2023, the European Union has continued to strengthen its cybersecurity architecture and introduced several major legislative initiatives and amendments to deal with the increasingly complex cyber threat environment. The NIS2 Directive expands the scope of cybersecurity regulations, strengthens the security standards of critical infrastructure and key sectors, and requires member states to improve notification mechanisms and incident response capabilities. The Cyber Resilience Act focuses on the full life cycle security of digital products, requiring manufacturers to be responsible for the security of their products and to ensure vulnerability remediation and software updates. The Cyber Solidarity Act advocates EU-level threat intelligence sharing and cross-border response support, emphasizing cooperation among member states to respond to major cyber incidents. The revised Cybersecurity Act strengthens the functions of the European Union Agency for Cybersecurity(ENISA) and promotes a unified cybersecurity standard certification framework to enhance the credibility and security of cyber and communication products. In addition, the Artificial Intelligence Act (AI Act) is the world's first legislation specifically addressing AI technology risks and introduces a tiered regulatory framework of AI systems to ensure that high-risk applications comply with requirements for transparency, accountability, and security. Together, these measures form the EU's comprehensive and coordinated cybersecurity and digital governance framework, laying a solid foundation for digital transformation and cyber resilience in the future.

To sum up, nation-state cyber threats are increasing steadily and are closely related to geopolitical developments. Countries around the world are gradually recognizing them as major national security challenges. The cyber strategies of major countries and international organizations such as the United States, the United Kingdom, Australia, and the European Union all reveal several common trends: First, these strategies emphasize critical infrastructure's security and resilience. The ability to respond to nation-state cyber threats, particularly advanced persistent threats (APTs) [2], is regarded as a top priority. Secondly, in the face of risks and opportunities brought by emerging technologies such as AI and quantum computing, these countries have invested in strengthening

technology research and development and risk management. Thirdly, countries have successively adopted stricter regulations and responsibility requirements for the ICT supply chain and related industries to ensure the security and resilience of the overall network ecosystem. Finally, international cooperation and public-private partnerships have become the key to dealing with transnational cyber threats. Countries have established joint defense mechanisms through alliances, cooperation frameworks, and threat intelligence sharing to jointly respond to the challenges of nation-state cyber threats and promote joint operational capabilities in global cybersecurity. These measures show that countries are accelerating the establishment of more comprehensive and resilient cybersecurity systems to confront the growing complexity of the cyber threat landscape.

2 Advanced Persistent Threat, or APT for short, is an advanced form of persistent cyberattack that usually infiltrates specific targets with sophisticated techniques to evade detection and remain dormant for extended periods. APTs often involve a series of staged actions, including infiltration, establishing backdoors, privilege escalation, lateral movement, and data exfiltration. Its main purpose includes stealing sensitive data and disrupting or damaging system operations. It is common in state-sponsored hacking, but may also be launched by well-resourced cybercrime organizations.

Key Elements of the National Cybersecurity Strategy 2025

The *National Cybersecurity Strategy 2025* will comprehensively deploy and strengthen the four pillars of cybersecurity including Whole-of-Society Defense Resilience, Homeland Defense and Critical Infrastructure, Key Industries and Supply Chains, and Application and Security of Artificial Intelligence. These pillars will be guided by two Cross-Pillar Principles: Robust Cybersecurity Governance and Protection, and Strategic Partnerships. Two Cornerstones will be laid: first, Establishing the National Cyber Collaborative Operation Center; second, Strengthening the Role of the National Information and Communication Security Taskforce and Formalizing of the Cybersecurity Budget. These efforts will be supported by Six Basic Joint Defense Agencies, an Inter-agency Joint Defense System, public-private partnerships across industry, academia, and research institutions, as well as international cooperation. Together, these components form a solid foundation to achieve the vision of building a resilient, secure, and trustworthy smart nation (as shown in Figure 2). The strategy is described in detail as follows:(it appears also in the figure)

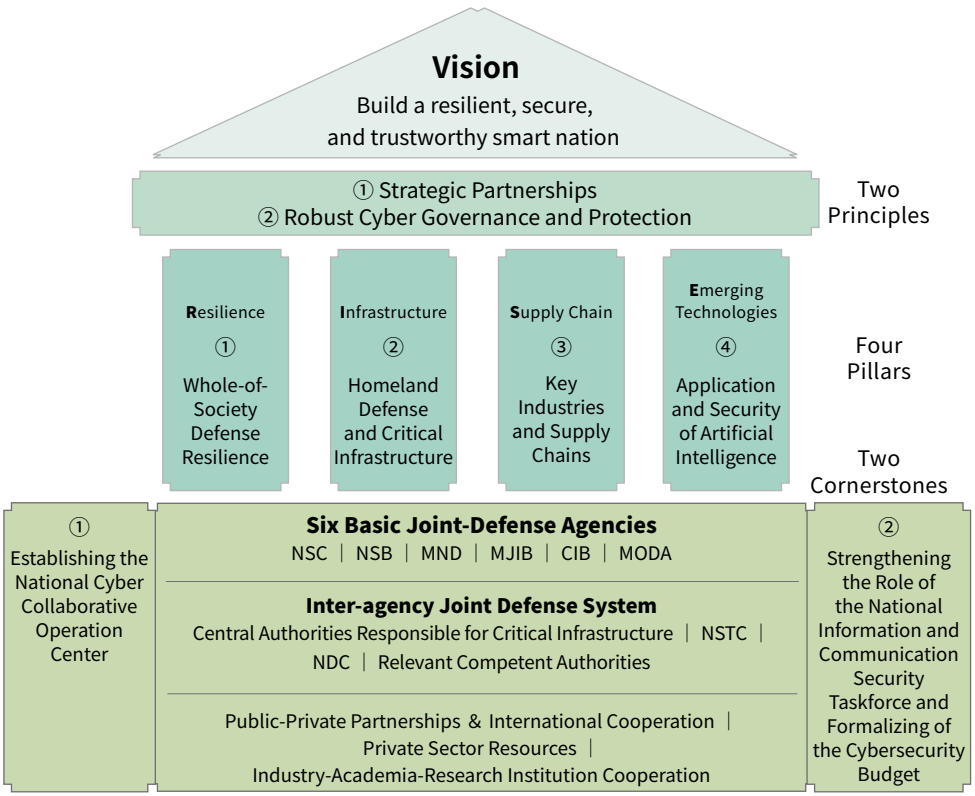


Figure 2. Key Elements of the National Cybersecurity Strategy 2025

Cross-Pillar Principles

I. Robust Cyber Governance and Protection

Cyber governance is the cornerstone of how modern organizations respond to digital risks. In the latest version of the *NIST Cybersecurity Framework (CSF) 2.0*, officially released by the National Institute of Standards and Technology (NIST) in 2024, a new core function titled Govern was introduced to emphasize its key role in cybersecurity. The meaning of governance is to establish clear policies and procedures to ensure that cybersecurity goals are consistent with the organization's business needs, while strengthening the participation and responsibility of its management team. This includes not only risk identification and management, but also the cultivation of a cybersecurity culture to ensure that cybersecurity measures can be effectively implemented across all levels of the organization.

In addition, the zero trust architecture has become an important security approach and an indispensable element of cyber governance in recent years. Through the concept of "never trust, always verify", the zero trust architecture requires continuous authentication and authorization of all users, devices, and resources, effectively limiting the impact of cyberattacks.

In a rapidly changing threat environment, operational resilience is another core element of cyber governance. Resilience emphasizes on an organization's ability to quickly respond to and recover from cyberattacks, operational disruptions, or other uncertainties. Achieving resilience includes promoting the migration of core functions of critical systems towards offshore cloud backup, strengthening the off-site redundancy and fault-tolerant design of infrastructure, and guiding the public and private sectors to gradually transition to post-quantum cryptography standards to address future threats to encryption from quantum computing.

Therefore, this strategy outlines Robust Cyber Governance and Protection as a key cross-pillar principle, driving the implementation of cyber governance, adoption of the zero trust architecture, and strengthening of resilience at the national level. Its main goals are:

1. **To adopt and implement the zero trust architecture to strengthen cyber awareness and culture within organizations in both public and private sectors.**
2. **To implement cyber governance, establish data backups, and effectively protect data in both public and private sectors.**
3. **To develop quantum readiness cybersecurity protection framework and management, and promote accelerated migration to post-quantum cryptography across all sectors.**

In terms of key strategic approaches, first, in accelerating implementation of comprehensive cyber governance and security management systems across all government agencies and critical infrastructures, the concept of zero trust architecture should be promoted to ensure that each entity gains a deeper understanding of the security of data processing, transmission, and storage, followed by adoption of zero trust architecture, with the implementation of its three core principles: explicit verification, least-privilege access, and assumed breach. Organizations in the public and private sectors should be supported in formulating corresponding strategies and implementation plans to establish a more resilient security mechanism. In addition, validation and verification standards and guidelines must be developed to ensure the effectiveness of the zero trust model, with the public sector taking the lead in testing and adjustment to enhance overall defense capabilities. In terms of industrial development, efforts should be made to actively guide and promote the growth of zero-trust-related cyber industries, encourage the development and applications of more innovative solutions, particularly those leveraging AI and machine learning, and further explore emerging technologies, such as quantum-safe security, to strengthen cybersecurity defenses.

At the same time, cooperation with domestic and international cloud service providers should be deepened, and cross-domain establishment of data backup and core function redundancies overseas should be expanded to ensure governments and enterprises can still maintain key business operations in case of major cyber incidents or catastrophic disasters. Digital governance and cross-

border (cloud) data transmission regulations should be continuously reviewed, updated, and refined, when necessary, to support the public and private sectors in accelerating the establishment of backup mechanisms and ensuring the availability of critical data.

In order to strengthen data protection and prevent insider threats, corresponding policies and regulations should be formulated, and necessary resources be in place to ensure that sensitive information is properly protected. Existing laws and regulations related to data encryption and communication protocols should be reviewed and resources continuously allocated to implement encryption schemes to secure both data storage and transmission to reduce the risk of data leakage or theft. In addition, with the development of quantum computing technology, traditional encryption technology faces the risk of being cracked. Thus, through cooperation among industry, academia, and research institutions, the public and private sectors should re-examine and adjust the existing cybersecurity architecture and develop post-quantum cryptographic technologies to ensure that data protection mechanisms still are sufficiently robust, and resistant to quantum attacks, achieving sustained long-term security and reliability.

II. Strategic Partnerships

International cooperation is an indispensable key to strengthening national cybersecurity. Cyber threats respect no borders, and hacker organizations and cybercriminal groups are adept at using springboards, hidden networks, and information and communications supply chains to infiltrate and launch cyberattacks, making the tasks of detection, prevention, defense and attribution much more challenging. Establishing intelligence sharing and joint defense mechanisms through international cooperation can significantly improve the visibility of cyber threats and achieve early warning and rapid response. Furthermore, public cyber attribution and jointly calling for accountability can make hacker organizations and their actions transparent, thereby increasing the costs and risks of their actions and achieving deterrence effects more effectively.

Cybersecurity cooperation is not limited to intelligence sharing and joint defense but also includes assisting other countries to improve their cybersecurity capabilities. In the context of a highly interdependent global economy, the improvement of the cybersecurity capabilities of every partner country in the democratic coalition can contribute to overall protection capacity. The concept of "helping others is protecting ourselves" is the core value of international cybersecurity cooperation, which builds a more solid foundation for the global cyber ecosystem.

In addition, cybersecurity is fundamental to deepening international cooperation because it is an important cornerstone for building mutual trust among partner countries. Facing the trend of rising geopolitical instability and confrontation, countries must work together to consolidate democratic supply chain and ensure the security and resilience of its overall digital infrastructure and key technologies. Taiwan will definitely play a role in this democratic supply chains. Not only is Taiwan an important node in this democratic cybersecurity chain but also an active and responsible participant in international cooperation on cybersecurity. By strengthening our own cybersecurity capabilities and technological innovation, we can further become a key contributor both to the regional and global cyber ecosystem and exert greater impacts.

In line with this, this strategy proposes Strategic Partnerships as another cross-pillar principle. The main goals are as follows:

1. **To comprehensively strengthen national defense and whole-of-government preparedness capabilities using advanced strategic partners as benchmarks.**
2. **To strengthen international cybersecurity cooperation and expand international joint defense efforts.**
3. **To support strategic partners to enhance the collective cybersecurity capabilities.**

To achieve the above goals and strengthen the interoperability and visibility of cybersecurity preparedness, the specific strategic approach is to bolster the foundation of mutual trust with advanced strategic partners, enhance the cybersecurity preparedness of each pillar of this strategy, and facilitate smoother collaboration among different countries and organizations. Continuing to strengthen international government-industry-academia exchanges and encouraging domestic cybersecurity teams to participate in international competitions and forums will help establish closer relations of collaboration in various sectors, which will not only promote best practices sharing but also expand influence in the global cybersecurity arena. In addition, we should continue to draw on the practices of advanced strategic partners and promote build-up and cultivation of cyber talents and technical capabilities in the private sector to strengthen overall cybersecurity capacity.

In terms of data governance, the mechanism for data exchange and sharing among strategic partners should be enhanced to ensure that security audits, physical security, cross-agency communication mechanisms, and related confidentiality operating standards all meet the corresponding levels of confidentiality, thereby laying a solid foundation for cooperation. At the same time, it is necessary to strengthen connections with the international cybersecurity communities and actively participate in global cybersecurity initiatives and drills, thereby improving the situational awareness of foreign cyber threat intelligence and strengthening joint defense mechanisms. We should also actively invest in the international cyber ecosystem, attract international resources to help develop domestic cybersecurity infrastructure and digital ecosystem, and ensure alignment with international standards.

Finally, we should continue to actively share experiences of cybersecurity protection, promotion, and policy formulation, and actively assist strategic partners and allies to cultivate cyber talent, improve their cybersecurity protection capabilities, and deepen the basis for bilateral and multilateral cooperation. In addition, to foster international growth of domestic cyber industry, local enterprises need support to enter the international market and connect with international resources, so that domestic enterprises can access the global market and become

significant players in the international cyber ecosystem, thereby enhancing competitiveness and influence of Taiwan in the global cybersecurity arena.

▼

Four Pillars

Pillar 1: Whole-of-Society Defense Resilience

As President Lai emphasized, with the outbreak of the global pandemic and the Russia-Ukraine war, countries around the world are enhancing their defense resilience. NATO and the European Union, for example, have formulated guidelines for strengthening whole-of-society resilience. This shows that Taiwan is not an exception. Whole-of-Society Defense Resilience is a global issue, and Taiwan's continued efforts in this regard align with the shared expectations of the international community. Cybersecurity is a vital component of Whole-of-Society Defense Resilience. Especially in the digital era, strengthening protection capabilities requires a human-centric approach, which includes two main aspects. On the one hand, cybersecurity is a complex field that requires integration of advanced knowledge, technical skills, and strategic insight, relying heavily on contributions of highly skilled professionals to ensure system security and drive technological innovation. On the other hand, humans remain the greatest source of cybersecurity risks and the most significant vulnerability in cybersecurity. Whether through inadvertently clicking malicious links, leaking sensitive information due to a lack of awareness, or being manipulated by malicious actors, individual actions can pose serious threats.. Therefore, continuous education and ongoing reinforcement of individual cyber awareness are essential to strengthening our overall defense, just like cultivating habits for epidemic prevention via frequent hand washing and wearing masks, which may seem simple but are highly effective in reducing the threat of virus infection. Cultivating personal vigilance, cyber awareness, and responsible online behavior also enhances the public's ability to confront increasingly complex cyber threats, including disinformation, misinformation, and online frauds. Moreover, Whole-of-Society Defense Resilience does not rely solely on individual efforts. It requires strong public- private

partnerships. Both the government and private sector must work collaboratively and invest resources to jointly build a robust and resilient cybersecurity framework that lays a solid foundation for national security in the digital age.

This strategy therefore outlines Whole-of-Society Defense Resilience as the first pillar, with the main objectives as follows:

1. **To expand the training and utilization of civilian power and enrich defense capabilities to respond to cyberattacks, in line with the establishment of the Whole-of-Society Resilience Committee.**
2. **To enhance the capabilities of civilian's cybersecurity defense and data protection, as well as the ability to detect disinformation, misinformation, and fight against cognitive warfare tactics.**
3. **To strengthen public-private partnerships to enhance the cybersecurity defense system and resilience.**

In terms of popularizing cyber awareness, we should provide comprehensive cyber governance resources and basic cybersecurity protection support to enterprises at all levels in Taiwan's economic backbone, and assist enterprises in establishing robust security mechanisms to enhance the overall economic system's risk resistance. To address the increasingly serious problems of cybercrime and online fraud, it is essential to promote robust public-private partnerships and enhance international cooperation. At the same time, regulatory oversight must be strengthened, particularly in data-intensive industries such as e-commerce and social media platforms, a more complete incident warning, notification and verification mechanism be established, and digital forensics and attribution techniques be developed to ensure that relevant risks can be discovered in time and responded to quickly. The promotion of personal identity authentication and verification mechanisms that balance convenience with privacy protection should also be expanded. Such measures can significantly reduce the risk of online impersonation and fraud, while enhancing the credibility of digital transactions and interactions.

To build social consensus and promote the development of cybersecurity, national cybersecurity summits will be convened on a regular basis. These summits aim to foster a shared understanding across society, coordinate cybersecurity efforts across all sectors, and promote the development and innovation of cybersecurity applications. At the same time, robust cyber governance frameworks, as well as incident response and reporting mechanisms, must be established and implemented across both the public and private sectors to ensure timely and effective responses to emerging threats. In addition, we will review, assess and update relevant procurement and budgetary regulations to foster a more secure and enabling environment. This will support the research, development and application of forward-looking technologies across industry, academia and research institutions, while also ensuring the security of telecommunications products throughout their entire life cycle.

Pillar 2: Homeland Defense and Critical Infrastructure

The cybersecurity of critical infrastructure is of paramount importance as these systems form the backbone of a functioning society. Disruptions to essential services, such as energy, water, electricity, telecommunications, transportation, finance, and healthcare care, caused by cyberattacks can lead to a widespread societal paralysis, and inflict severe, incalculable damage on economic activity, public safety, and people's well-being. Such incidents not only endanger national stability, but also erode public trust in the government.

In the realm of national defense, cybersecurity plays a critical role in safeguarding the integrity of the military's combat command and control systems, ensuring that facilities, equipment, communications and decision-making processes remain secure and uninterrupted. Moreover, cybersecurity capabilities represent a vital extension of both national defense and combat strategies. The armed forces must be equipped to effectively counter foreign cyberattacks, aimed at disrupting defense infrastructure, stealing sensitive information, or crippling combat readiness. In this context, cybersecurity serves as a core pillar of homeland security and national defense effectiveness.

This strategy outlines Homeland Defense and Critical Infrastructure as the second pillar. Its main objectives include:

1. **To conduct a comprehensive assessment of potential cybersecurity risks to Homeland Defense and Critical Infrastructure; and to propose targeted countermeasures that strengthen security and enhance the capacity of proactive defense across vital systems.**
2. **To implement cyber governance and enhance cyber defense and resilience across four major domains, national defense, public welfare, disaster prevention, and democratic governance.**
3. **To strengthen cybersecurity and combat readiness to safeguard national security and uphold regional peace and stability.**

As for specific strategies and practices, the establishment of a new National Cyber Collaborative Operation Center is a top priority. This Center will serve as a central hub to monitor national-level cybersecurity risks, strengthen the incident response coordination and personnel deployment, and ensure rapid mobilization of resources to effectively counter major cyber threats. Furthermore, the government should clearly define cybersecurity combat readiness requirements and strategic objectives, particularly for national defense and law enforcement agencies, while concentrating resources on enhancing intelligence gathering, threat attribution, and proactive defense capabilities. These efforts aim to build a more comprehensive and effective national cybersecurity defense system. At the same time, a comprehensive review and management of systems, networks and equipment across key government agencies and critical infrastructure must be undertaken. These assets should be categorized by risk level, and a regular inspection mechanism should be established to ensure the proper implementation of maintenance, management, and upgraded protocols. To further consolidate defense capabilities, both the competent authorities and the central agencies overseeing relevant sectors of critical infrastructure must strengthen their supervisory responsibilities. This includes enforcing cyber incident investigation procedures,

establishing accountability mechanisms, and ensuring that all entities comply with the required standards for cybersecurity risk response.

Building upon the aforementioned considerations, national security and relevant cybersecurity agencies should cooperate with the central authorities overseeing the critical infrastructure sectors, such as energy, communications, transportation, finance, and healthcare, to develop and implement "Cybersecurity Action Plans." These plans aim to bolster system resilience, ensuring the continuity of essential services under extreme conditions. For interdependent infrastructures, elevating cybersecurity standards is crucial to maintaining basic operations during crises. Additionally, formalizing cybersecurity funding for the public sector and critical infrastructure is essential, alongside accelerating the modernization of ICT equipment to safeguard these systems. Establishing a cross-agency joint operating platform can enhance coordination, focusing on strengthening operational resilience during emergencies.

To strengthen cyber defense capabilities, a dedicated cybersecurity protection team should be established to respond to critical infrastructure emergencies. This team should undergo regular training and drills to ensure that personnel are equipped with rapid response and problem-solving skills. In addition, routine technical assessments of key systems within public agencies, the national defense sector, and critical infrastructure should be conducted. Third-party red team exercises and scenario-based tabletop exercises are both essential for testing and validating cyber defense and incident response mechanisms. Drill content should include protocols for responding to data breaches, and the tabletop exercises should be led by senior management and the organization's Chief Information Security Officer (CISO). This leadership involvement ensures that key decision-makers are prepared to respond effectively to cyber incidents. Such coordinated efforts will enable government agencies and critical infrastructure providers to respond swiftly and effectively to cyber threats, thereby strengthening our homeland security and the overall critical infrastructure protection capabilities of Taiwan.

Pillar 3: Key Industries and Supply Chains

Domestic key industries, including the *Five Trusted Industry Sectors*, i.e., semiconductors, artificial intelligence (AI), military, security and surveillance, and next-generation communications, form the backbone of economic prosperity and development. Alongside core service sectors, such as finance, healthcare, and communications, which are vital for societal operations, these industries must prioritize cybersecurity to protect intellectual property and ensure operational resilience. Given the increasing interdependence of global supply chains, safeguarding these sectors and their interconnected networks is paramount. Cyber threats targeting key industries and their supply chains pose significant risks to both national and economic security. Therefore, fortifying cybersecurity protection measures is essential to maintain Taiwan's strategic position in global supply chains, and to protect its economic and national interests. For the international community, enhancing the cybersecurity of key industries is equally critical to reinforcing the democratic supply chains. This ensures that global cooperation is built on secure, trustworthy technologies, and resilient industrial ecosystems, safeguarding shared values and mutual interests.

To further strengthen the cybersecurity protection of key domestic industries and supply chains, it is imperative to cultivate a robust domestic cybersecurity ecosystem. Supporting local cybersecurity innovation not only enhances Taiwan's indigenous technological capabilities, but also enables Taiwan to exert greater influence on the international stage. A vibrant cybersecurity industry not only meets local market needs, but also promotes technological exports, facilitates industrial upgrades, and attracts top-tier cyber talent, infusing new momentum into growth. Only by integrating the promotion of cybersecurity in key industries and supply chains with the innovative development of the cybersecurity sector can Taiwan establish a comprehensive and resilient cybersecurity framework. This holistic approach ensures readiness to address the challenges posed by geopolitics and digitalization, safeguarding national security and economic interests. Therefore, the third pillar of this strategy is Key Industries and Supply Chains, with the following main objectives:

1. **To review and strengthen the cybersecurity frameworks in key domestic industries (such as the *Five Trusted Industry Sectors* as well as data-intensive industries such as finance, communications, and healthcare) to fortify democratic supply chains.**
2. **To implement Business Continuity Management (BCM) in key industries to mitigate cybersecurity risks.**
3. **To expand investment in cybersecurity and foster startups.**

To enhance supply chain security, the strategy calls for close cooperation with industry associations and leading enterprises to conduct a comprehensive assessment of key industries, critical enterprises, supply chains and their essential resources. A risk management registry should be established to ensure greater visibility and security across the entire supply chain. Building on this foundation, targeted "Cybersecurity Action Plans" should be implemented to meet the specific needs of key industries, with phased expansion to progressively strengthen national cyber governance capabilities. In addition, government procurement processes as well as the labeling and certification systems for related cybersecurity products must be improved, along with strengthened cybersecurity standards, governing the acquisition of software, hardware, and services by government agencies and key industry supply chains. Furthermore, key or high-risk suppliers and designated product categories should be given particular attention to proactively mitigate cybersecurity risks at the source.

To strengthen the cybersecurity capabilities of key industries, it is essential to promote communication and collaboration among enterprises, while enhancing cyber awareness and technical expertise through regular personnel training and the systematic sharing of major vulnerabilities. These efforts will contribute to safeguarding data security across sectors. At the same time, all key industries, and their associated supply chains (including the defense-related supply chains) should be encouraged to establish joint defense mechanisms to improve cybersecurity coordination and enhance collective resilience against cyber threats. In addition, cybersecurity governance measures should be implemented

across these industries, and their defense and response capabilities should be rigorously tested through red team exercises to ensure preparedness and the ability to effectively respond to cyber incidents.

To promote the autonomous development of Taiwan's cybersecurity industry, it is essential to strengthen regulatory requirements for both the public and private sectors, and foster a supportive and healthy environment for industry growth. Cybersecurity governance and protection capabilities should be improved through regular evaluations and the implementation of incentive mechanisms. These may include expanding tax deductions for cybersecurity investments such as Bug Bounty Programs, encouraging the adoption of third-party assessments, integrating cybersecurity requirements into government procurement contracts, and establishing frameworks for evaluating both domestic and international cybersecurity firms. Such measures will help stimulate the development of a robust domestic cybersecurity industry. Furthermore, increased investment and targeted guidance should be provided to support cybersecurity startups, facilitate industry scaling and internationalization, and establish a comprehensive talent ecosystem that aligns cybersecurity human resource supply with market demand. These efforts will strengthen Taiwan's competitiveness of cybersecurity industry, and reinforce the resilience and security of its supply chain in the global market.

Pillar 4: Application and Security of Artificial Intelligence

As the fourth pillar of this strategy, the Application and Security of Artificial Intelligence should be advanced through coordinated efforts in three key areas: technology, talents, and systems. First, the government must work collaboratively with the private sector to increase investment in the research and development of AI security technologies and applications, ensuring a joint response to the threats posed by emerging technologies. At the same time, it is also imperative to cultivate a large-scale talent pipeline in both cybersecurity and AI to ensure that the nation possesses sufficient technical expertise and human resources necessary to meet future challenges. Improving institutional framework and regulatory systems will also help facilitate safe deployment and applications of AI technologies, and foster responsible international cooperation, maximizing the potential benefits of AI applications and mitigating associated

risks. The main objectives and strategic approaches of this pillar are twofold:

1. **To apply AI technologies to enhance cybersecurity capabilities across the domains of Whole-of-Society Defense Resilience, Homeland Defense and Critical Infrastructure, and Key Industries and Supply Chains, while simultaneously fostering a robust and innovative cybersecurity industry ecosystem.**

2. **To ensure the security, reliability, and trustworthiness of AI technologies themselves by embedding safety, ethical, and governance frameworks throughout their development and deployment.**

To advance the applications of AI in the field of cybersecurity and strengthen overall security resilience, several strategic measures should be implemented. These include: enhancing collaboration between public and private sectors, as well as across industries, in the research and development of AI technologies, and strengthening the cybersecurity defense capabilities through the adoption of automated cybersecurity management and governance, such as deploying AI to detect system vulnerabilities and recommend timely countermeasures. In addition, hosting relevant competitions can help stimulate innovative research and accelerate the development and practical application of AI technologies, encouraging enterprises and research institutions to engage in this domain. To further improve the overall technological standards of cybersecurity, we should also devote efforts to focus on promoting AI integration into the cybersecurity field through the establishment of a "Cybersecurity Technology Park." This initiative would aim to attract top domestic and international talent and enterprises, foster industrial clustering and drive the growth of a robust cybersecurity ecosystem.

To establish an autonomous, inclusive and competitive cybersecurity ecosystem and ensure full integration of the cybersecurity industry with market demand, AI technologies should serve as a central pillar connecting the upstream, midstream, and downstream sectors. This includes aligning cybersecurity service providers with the needs of key industries, critical infrastructure, and government agencies. By doing so, a virtuous cycle of supply and demand can be

cultivated, driving the holistic development of the cybersecurity industry. From a technical governance perspective, the Secure by Design (SbD) priniciples, and the safety and trustworthiness of AI systems must be actively promoted. Embedding risk management mechanisms at the design and development stages will help mitigate potential cybersecurity risks at the source, ensuring that AI technologies contribute to a secure digital environment.

On the other hand, international AI-related standards should be developed, while encouraging enterprises in the private sector to develop technologies that align with these standards This approach will help lay a solid foundation for the sustainable development of the AI security industry. To ensure the safe and responsible application of AI technologies, a comprehensive review of existing regulations should be undertaken, accompanied by the promotion of widespread AI adoption and the establishment of a robust cyber governance framework. These measures will help maintain high standards of cybersecurity management in an AI-driven environment. Furthermore, to strengthen the whole-of-society defense resilience, it is critical to build the capacity to detect, assess, and respond to emerging risks such as cognitive warfare and cyber-enabled fraud. In doing so, the advancement of AI technologies does not pose new cybersecurity risks, but rather becomes a key enabler in bolstering national cybersecurity and enhancing societal resilience.

▼

Two Cornerstones

I. Establishing the National Cyber Collaborative Operation Center

To achieve the vision of this strategy of building a resilient, secure, and trustworthy smart nation and to consolidate the four pillars, a National Cyber Collaborative Operation Center should be established. This Center must be supported by sufficient investment in funding, personnel and other essential resources. Its core mandate will be to integrate and coordinate key functions, including the collection, analysis, and sharing of cybersecurity intelligence, joint

defense operations, and the provision of support in response to major cyber incidents. The key tasks include:

1. **To develop a national cybersecurity risk map to accurately assess and visualize cybersecurity risks at the national level.**
2. **To expand the collection of cybersecurity monitoring intelligence across public and private sectors, critical industries, and international partners to enhance situational awareness of threat visibility.**
3. **To coordinate and support the response to major cyber incidents, including the formulation of operational guidelines and standardized procedures to enhance the efficiency and effectiveness of integrated incident response.**

II. Strengthening the Role of the National Information and Communication Security Taskforce and Formalizing the Cybersecurity Budget

To effectively support this strategy, the role of the National Information and Communication Security Taskforce under the Executive Yuan should be further strengthened, solidifying its position as the central coordinating and supervisory body for national cybersecurity affairs. Key responsibilities include:

1. **To coordinate and supervise interagency cybersecurity efforts, promoting necessary regulatory adjustments. and ensuring robust legal compliance across all levels of government.**
2. **To ensure that government agencies and operators of critical infrastructure be equipped with sufficient cybersecurity budgets and personnel, while regularly evaluating the effectiveness of their cybersecurity implementation and protection measures.**
3. **To expand engagement with the private sector by promoting public-private partnerships that foster collective cybersecurity responsibilities and innovation.**

Cross-Pillar Foundation

I. Six Basic Joint Defense Agencies (Six Basics)

Building upon the foundation of the original Six Basic Joint Defense Agencies, and guided by the national security-centered core strategy, a coordinated framework is established to integrate the efforts of the six key agencies: the National Security Council (NSC), the Ministry of National Defense (MND), the National Security Bureau (NSB), the Ministry of Justice Investigation Bureau (MJIB), the Criminal Investigation Bureau (CIB), and the Ministry of Digital Affairs (MODA). This joint mechanism is tasked with ensuring the comprehensive planning, effective execution, and robust management of fundamental cybersecurity protection measures. Within this joint defense framework, each agency plays a distinct and critical role: MND is responsible for cybersecurity and proactive defense operations within the military sector; NSB oversees cybersecurity protection, intelligence gathering, and analysis for intelligence agencies; MODA is responsible for strengthening digital resilience across government, implementing cybersecurity laws and regulations, and enhancing cybersecurity within industries, as well as promoting national cyber awareness; MJIB and CIB serve as the principal entities of digital forensics, traceability, cybercrime investigation and law enforcement.

II. Inter-agency Joint Defense System (Grand Alliance)

In line with the elevated notion of "Cyber Security is National Security," the Interagency Joint Defense System, or referred to as the Grand Alliance, should integrate key government agencies and the entities under their jurisdiction or supervision. This includes subordinate non-departmental public bodies, critical infrastructure, key industries, and their associated supply chains. (as depicted in Figure 3). The core responsibilities of the Grand Alliance encompass the strategic allocation of resources and the integration of capabilities across industry, academia and research institutions to promote scientific innovation and industrial development; cyber governance of critical infrastructure, including budget planning, oversight, implementation, and the safeguarding of vital data

and systems; promotion of advance deployments; and the strengthening of cybersecurity diplomacy and international cooperation, etc.

III. International Cooperation of Strategic Partners

Taiwan stands at the forefront of the global democratic coalition. This strategy seeks to deepen collaboration with advanced strategic partners and like-minded democratic nations by actively engaging in international organizations, global cybersecurity communities, and fostering partnerships across industry, academia, and research institutions. Through robust public-private partnerships and international cooperation, Taiwan aims to enhance its cybersecurity protections and expand its influence on the global stage.

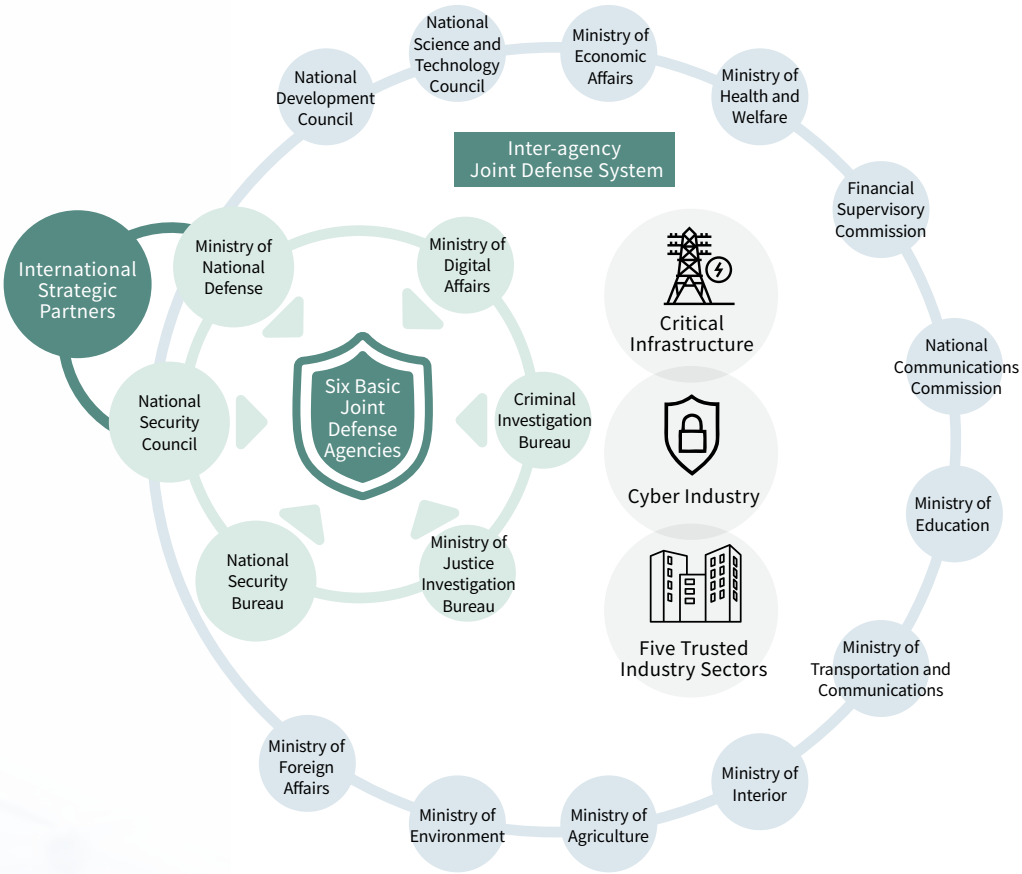


Figure 3. Cross-pillar base and public-private partnership team

CONCLUSION: Building a resilient, secure, and trustworthy smart nation

Cybersecurity is integral to national security. In the face of escalating and evolving cyber threats and challenges, Taiwan must demonstrate unified national resolve, comprehensive resource allocation, and decisive top-down leadership to strengthen its cybersecurity resilience, safeguarding democracy, freedom and industrial prosperity. Today's cyber threats go far beyond technical issues; they directly impact national security, economic and social stability, and the continuity of governmental operations. State-sponsored cyberattacks, AI-driven hybrid threats and vulnerabilities in supply chain are becoming increasingly pervasive. Positioned as a geopolitical nexus and a significant partner in global supply chains, Taiwan finds itself at the forefront of the global cybersecurity battleground. This strategic position necessitates an unwavering commitment to enhancing cybersecurity capabilities, and safeguarding national interests.

Consequently the *National Cybersecurity Strategy 2025* sets forth a vision of building a resilient, secure, and trustworthy smart nation and proposes a strategic layout with four core pillars, such as Whole-of-Society Defense Resilience, et al., emphasizing broad-based national engagement in cybersecurity. Key initiatives include implementing Zero Trust Architecture to fortify access controls, constructing proactive defense capabilities to anticipate and mitigate threats, enhancing international joint defense collaboration to strengthen global partnerships, and ensuring the security of AI applications to safeguard against emerging technological risks. These strategies not only require comprehensive technological advancements, policies and regulatory reforms, but also demand the participation of the whole society from government agencies to enterprises, to academia and to the private sector, to form a community of cybersecurity protection, and to unite every effort to meet future challenges.

Public participation is essential to effective cybersecurity protection. The government must take the lead and demonstrate top-down commitment through increased resource investment and accelerated institutional transformation. From threat assessment and regulatory development to resource allocation, and strengthening operational mechanisms, the government will prioritize the establishment of a robust cyber governance framework as its core policy objective, aimed at securing critical infrastructure

and enhancing the protection resilience of the public sector. At the same time, deepening international collaboration across both public and private sectors is imperative to bolster intelligence sharing and joint defense capabilities, thereby solidifying Taiwan's role within the global cybersecurity ecosystem. Furthermore, cultivation and recruitment of cybersecurity talent must be vigorously promoted, along with the advancement of industrial innovation to achieve greater cybersecurity autonomy. By adopting targeted incentive measures, enterprises can be encouraged to enhance their cyber governance practices, fostering a virtuous self-sustaining cycle of industrial development and resilience.

Cybersecurity challenges know no borders. Only by national unity, integrated resource mobilization, and unwavering commitment can Taiwan safeguard its security and sustain its development amid global digital competition. It is imperative to confront cyber threats with foresight and decisive action, protect our freedom, democracy, and industrial prosperity with strong determination and comprehensive planning, and build a smart nation that is resilient, secure, and trustworthy for all citizens. In the future, through unremitting efforts and timely transformations, Taiwan will gain a firm foothold on the global cybersecurity stage and emerge as a leading model of cyber resilience.

Acknowledgments

We would like to extend our sincere gratitude to all experts, scholars, and representatives from public associations who contributed to the formulation of the *National Cybersecurity Strategy 2025 – Cybersecurity is National Security*. Your professional insights and valuable suggestions have laid a stronger foundation for national cybersecurity policy and enhanced the overall capacities for cyber defense.

Special thanks：

Hao-Wei Chen	Founder, Taiwan International Foundation
Shi Chen	Assistant Professor, Department and Institute of Banking and Finance, Chinese Culture University
Mars Cheng	Executive Director, Association of Hackers in Taiwan
Shin-Ming Cheng	Professor, Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology
Robert Chin	Chairman, Taiwan Chief Information Security Officer Alliance
Chen-Yu Dai	Director, Association of Hackers in Taiwan Board Member, Office of the President Whole-Of-Society Defense Resilience Committee
Yun Hsia	Researcher, National Institute of Cyber Security
Kenny Huang	Chairman, Taiwan Network Information Center
Alan Lee	Executive Director, Association of Hackers in Taiwan
Der-Tsai Lee	Academician & Distinguished Visiting Chair, Institute of Information Science, and Research Center for Information Technology Innovation, Academia Sinica
Hahn-Ming Lee	Distinguished Professor, Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology
Jung-Shian Li	Professor, Department of Electrical Engineering, National Cheng Kung University
Ying-Dar Lin	Chair Professor, Department of Computer Science, National Yang Ming Chiao Tung University
Allen Own	Chairman, Association of Hackers in Taiwan
Bo-Yen Shen	Chairman, Taiwan Innovative Software and Services Association.
Yeali Sun	Professor, Department and Institute of Information Management, National Taiwan University
Tzong-Chen Wu	Distinguished Professor, Department of Information Management, National Taiwan University of Science and Technology
Benson Wu	Director, Taiwan Innovative Software and Services Association(CISA), and Chairman, Cyber Resilience Committee, of CISA

(Sort by the number of strokes of surnames)

Title
National Cybersecurity Strategy 2025 –
Cybersecurity is National Security

Copyright Holder
National Security Council

Distributor
Joseph Wu, Secretary General, National Security Council

Author
National Information and Communication Security Office,
National Security Council

Consulting Editor
Yuh-Jye Lee, Senior Advisor, National Security Council

Der-Tsai Lee, Academician, Institute of Information Science,
Academia Sinica

Hahn-Ming Lee, Distinguished Professor, Department of Computer
Science and Information Engineering, National Taiwan University
of Science and Technology

Publisher
National Information and Communication Security Office,
National Security Council

Published: April 2025
ISBN：978-626-7688-05-2
GPN：1011400414

國家安全會議
NATIONAL SECURITY COUNCIL

Download Strategy

NATIONAL CYBERSECURITY STRATEGY 2025

Cybersecurity is National Security

building a resilient, secure,
and trustworthy smart nation

National Information and
Communication Security Office