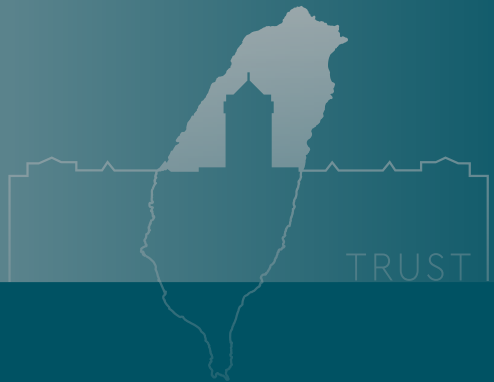


NATIONAL CYBERSECURITY STRATEGY 2025

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 crisis. 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 cyber security 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



MARCH 28, 2024



CONTENTS

08

Introduction: Incremental changes can no longer cope with urgent crisis

09 Background

12 Threat Landscape and Key Challenges

12 I. External Threats

13 II. Internal Challenges

16 Strategic Context

16 I. Strategic National Forward-Looking Development

16 II. Continuity of Earlier Strategic Plan

18 III. Strategic Response to Global Trends and Emerging Technologies

18 IV. Cybersecurity as the Foundation for Strategic Partnerships

18 V. Global Cyber Threat Assessment and Trends of Cyber Strategy

24

Key Elements of the National Cybersecurity Strategy 2025

26 Cross-Pillar Principles

26 I. Robust Cyber Governance and Protection

28 II. Strategic Partnerships

30 Four Pillars

30 Pillar 1: Whole-of-Society Defense Resilience

34 Pillar 2: Homeland Defense and Critical Infrastructure

36 Pillar 3: Key Industries and Supply Chains

38 Pillar 4: Application and Security of Artificial Intelligence

40 Two Cornerstones

40 I. Establish the National Cyber Collaborative Operation Center

41 II. Strengthen the Role of the National Information and Communication Security Taskforce and Formalize the Cybersecurity Budget

41 Cross-Pillar Foundation


41 I. Six Basic Joint Defense Agencies (Six Basics)

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

42 III. International Cooperation of Strategic Partners

44

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

The background features a dark teal vertical stripe on the left and a lighter teal vertical stripe on the right. Scattered across the dark teal area are several vertical columns of small, light-colored dots. The text is centered in the dark teal section.

INTRODUCTION:

Incremental changes can no longer cope with urgent crisis



Background

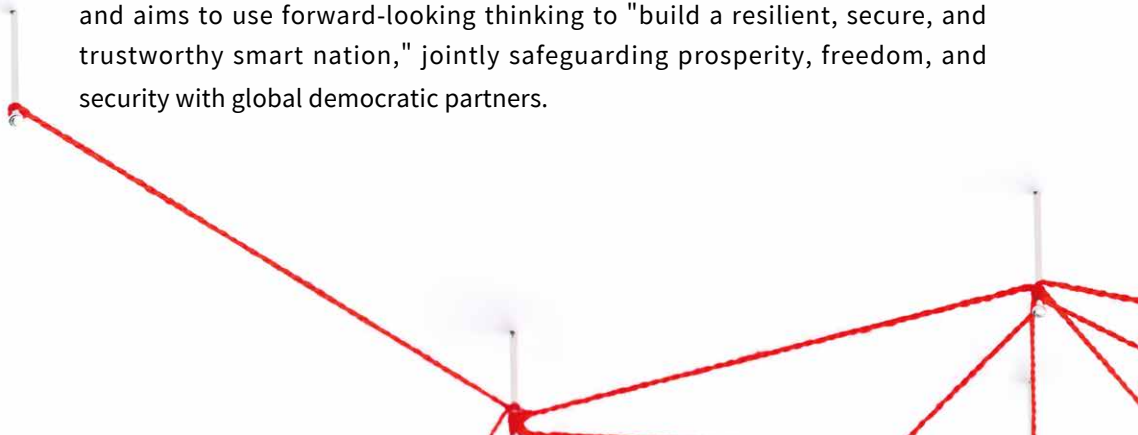
With the deepening of global digitization and the increasing prevalence of emerging technologies, information and communications security, or cybersecurity has ranked among the top ten major risks in the world (World Economic Forum 2024), and has become a crucial component in national security. Hacking and attacks on information and communication technologies (ICTs) not only pose a major threat to national security but also exhibit the characteristics of grey zone conflicts, continuously challenging 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, triggering internet intrusions 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 the normal operation of the country and society. In 2023, Microsoft revealed that a state-sponsored hacking group known as Volt Typhoon was attempting to infiltrate Guam's critical infrastructure, raising high alert in the United States. In 2024, U.S. authorities again identified a state-sponsored hacking group known as Salt Typhoon had invaded at least nine telecommunications operators in the United States with the intent to spy on then-presidential candidate Donald Trump and other high-level 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 by cybersecurity company CrowdStrike, which caused millions of computers worldwide to crash, exposing the risks inherent in the highly complex and interdependent information and communications supply chains. On the other hand, the rapid development of artificial intelligence (AI) not only brings various innovative applications but also significantly increases AI-driven cyber threats. These threats include using automation technology to improve attack efficiency and expand the scale of attacks, using generative AI to create

more realistic audio, video, images, and text content to confuse targets or conduct social engineering attacks. Even the vulnerabilities of AI systems themselves have become an emerging target for hackers, posing unprecedented risks. As for developing quantum computing, its powerful capabilities will pose a fatal threat to the currently widespread public key cryptography technology in the future, which could potentially lead large-scale leakage of state secrets and exposure of personal privacy. These cases and emerging technological trends demonstrate the essence of "cybersecurity is national security" and the urgency of the threat.

Today, China's various actions in cyberspace are raising 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 threats faced by Taiwan are particularly serious. The National Security Bureau (NSB) pointed out in the Analysis of the Chinese Communist Party's (CCP) Cyber Hacking Techniques in 2024 that the average daily number of intrusions on our Government Service Network (GSN) in 2024 reached 2.4 million, more than double the 2023 daily average of 1.2 million. Most of them were committed by the CCP's cyber army. Although many of them have been effectively detected and blocked, they still highlight the increasingly severe cyber intrusion landscape. In addition, the national security intelligence team detected 906 hacking cases across government and private sectors last year. Compared to 752 cases in 2023, this represents an increase of over 20%. Government agencies accounted for the largest share, making up over 80% of the total. An analysis of the CCP's cyber army targets revealed the most significant increases in the communications sector (mainly telecommunications), transportation, and the defense supply chain. It is obvious that these fields have become the focus of the CCP's emerging cyberattacks.

Given 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 Department of Cybersecurity under the Executive Yuan and the promulgation and implementation of the *Cybersecurity Management Act*. *Cybersecurity is National Security Strategy 1.0* focused on building the internal momentum for government policy implementation, advocating cybersecurity policies externally, 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 capacities, and expand international cooperation. At the same time, it promoted the establishment of the Ministry of Digital Affairs and the development of a closely coordinated Six Basic Joint Defense Agencies. As the global landscape evolves and emerging technologies continue to develop, various types of cyber threats and risks are rapidly increasing. Democratic partner countries are allocating more resources and accelerating government restructuring and talent development to actively respond. Our country is located at a geopolitical hub and faces more severe state-sponsored cyberattacks. Incremental changes can no longer cope with this urgent crisis. Comprehensive changes are urgently needed to greatly enhance the capacities and resilience of cyber defense to safeguard the achievements of national democracy, freedom, and industrial prosperity. Therefore, to further ensure and strengthen national security, the NSC proposed the *National Cybersecurity Strategy 2025* building upon existing foundations, which aligns with the vision of President Lai's *National Project of Hope: Innovative Economy, Smart Nation*, promotes the development of the *Five Trusted Industry Sectors* and the *Whole-of-Society Defense Resilience*, and aims to use forward-looking thinking to "build a resilient, secure, and trustworthy smart nation," jointly safeguarding prosperity, freedom, and security with global democratic partners.





Threat Landscape and Key Challenges

(As shown in Figure 1)

I. Rapidly rising external threats

First, there are nation-state cyber threats. The threat posed by state-sponsored hacker groups is growing steadily, with critical infrastructure and government units as their primary targets. These hacker organizations are resource-rich, use sophisticated techniques, and are skilled at concealing their actions. They often exploit the information and communications supply chain to infiltrate, which greatly increases the difficulty of detection and defense. They usually remain dormant within the victim's network for extended periods, waiting for the right moment to steal sensitive information and launch further operations, for example, leaking confidential information at a precise moment and manipulating media coverage 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 cyber landscape. The powerful computational and analytical capabilities of AI allow hackers to detect vulnerabilities more quickly, automate attack processes, and even generate highly convincing phishing emails and social engineering tactics that bypass traditional defense mechanisms. On the other hand, although quantum computers are not yet commercially available, their potential computing power will subvert existing encryption technologies. In the future, quantum computing may easily crack the currently widely used public key encryption algorithms, posing unprecedented challenges to the security of communication systems, financial transactions, and state secrets. As the technological race intensifies, how to address AI-driven intelligent attacks and quantum computing threats in the future has become a core issue in global cybersecurity strategies.

Third, cybercrime continues to be rampant. Cybercriminal activities pose multiple threats to individuals, businesses, and national security. In particular, ransomware attacks have escalated repeatedly, with hackers encrypting victims' important data and demanding huge ransoms, and even threatening to disclose sensitive information, causing huge economic losses to victims and a crisis of

trust in cyberspace. At the same time, from fake corporate emails to phishing websites, new online fraud techniques keep emerging to hack personal privacy information. What is even more concerning is intellectual espionage, where hacker organizations infiltrate corporations and Research and Development institutions to steal key technologies and business secrets, causing immeasurable damage to industrial competitiveness and national interests.

II. Internal challenges that need to be solved urgently

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

Furthermore, as the demand for connectivity and interoperability between Taiwan and its strategic partners continues to grow, cybersecurity has become a key element in strengthening the foundation for cooperation. Effectively preventing data leakage, mitigating internal threats, improving personnel security vetting, and establishing secure and trustworthy communication channels among government agencies are all critical issues that must not be overlooked are all important issues that cannot be ignored. Through cooperation with international public and private sector partners, improving the sharing and application of cybersecurity intelligence can further strengthen Taiwan's cybersecurity protection capabilities, providing 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 raise the cost of hacker intrusions and create an

effective deterrent effect. 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 techniques, public-private partnerships, and international cooperation, we can expose hacking methods and sources, attribute attacks, and hold hackers accountable. Based on the severity of the incident, necessary actions and measures will be taken in a timely manner.

The full implementation of active defense requires clear strategic goals, professional technical capabilities, and sufficient resource investment. The implementation of proactive defense is not only key to addressing current cyber threats, but also the cornerstone of future digital resilience.



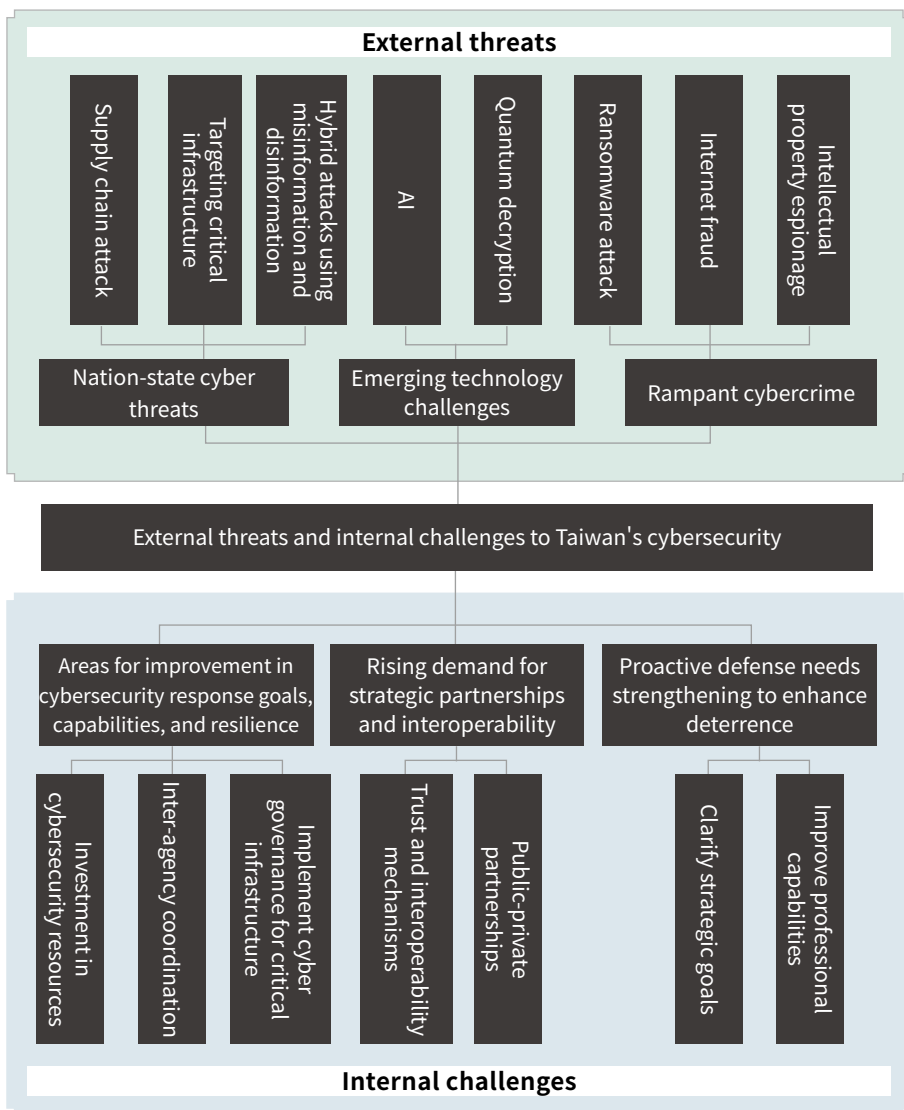


Figure 1. Taiwan's external threats and internal challenges



Strategic Context

I. Strategic National 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 the awareness of all people to protect it, improve the legal systems of national security, and strengthen democratic resilience. Economically, the *Five Trusted Industry Sectors* of 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 training and utilization of civilian wisdom and efforts but also cover the security of energy and critical infrastructure, as well as the stability of ICT, transportation and financial networks. The Committee seeks to enhance resilience in four key areas: national defense, people's livelihood, disaster prevention, and democracy, to build a robust democratic society and comprehensively safeguard national security.

In addition, Taiwan is the key to the global "democratic supply chains" and must promote industrial AI and use AI to enhance national and military power. Executive Yuan President Cho Jung-tai 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 Earlier Strategic Plan

In response to the promulgation and implementation of the *Cyber Security Management Act* and the successive establishment of the Information, Communications and Electronic Force Command and the Ministry of Digital Affairs, the NSC proposed the *Cybersecurity is National Security Strategy 1.0* and the Cybersecurity Iron Triangle Mechanism in 2018, and the *Cybersecurity*

is *National Security Strategy 2.0* and the Six Basic Joint Defense Agencies to be followed in 2021, all 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 intelligence sharing.

Today, building on the solid foundation and structure established in the early stage, in order to cope with the ever-changing cyber threats, it is necessary to devote more resources, enhance cybersecurity preparedness of joint defense of the whole society and key industries, and continue working toward the vision of building a resilient, secure, and trustworthy smart nation.



III. Strategic Response to Global Trends and Emerging Technologies

The World Economic Forum's 2024 Global Risks Report reveals that global risks and crises continue to rise. 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 competition between the United States and China have increased geopolitical instability, while technological progress and the development of AI have also contributed to the escalation of cyber threats. The national cybersecurity strategy must adjust and strengthen its strategic posture as various risks increase.

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 advanced strategic partners is crucial. The strategic thinking of cybersecurity protection must be aligned and synchronized with advanced strategic partners. The protection plans, actions, system equipment, education, and training of national defense, government agencies and critical infrastructure must also meet the standards of interoperability with our advanced strategic partners. Moreover we must be aligned with the partners' forward-looking plans and actions to ensure more effective implementation. Only in this way can mutual trust be enhanced and close cooperative relations maintained.

V. Global Cyber Threat Assessment and Trends of Cyber Strategy

In the planning process of this strategy, in addition to responding to the development trends of global cyber threats, we also refer to relevant strategies, policies, and regulatory documents of various countries to ensure that it is

¹ Wei-Shui Chiang, Clinical Handouts.

forward-looking and in line with international standards. 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 service providers, rather than allowing small and medium-sized enterprises and end users to bear disproportionate risks. At the same time, it adjusts incentive structures to encourage long-term security investments, to build a more defensive and resilient future digital ecosystem. Therefore, the U.S. strategy outlines five pillars. These include strengthening the cybersecurity defense capabilities of critical infrastructure through public-private partnerships 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 enhancing transparency in the software supply chain. The strategy also emphasizes investing in advanced cybersecurity technologies, such as AI, Industrial Control Systems (ICS), cloud computing, and Post-Quantum Cryptography (PQC), and promoting the adoption of zero trust architecture. Finally, it calls for deepening international partnerships to further strengthen collective cyber resilience.

In 2025, former US President Joe 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 technology, 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 2 (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 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 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. Third, 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.

■ 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-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, the Establishing of the National Cyber Collaborative Operation Center; second, the Strengthening of the Role of the National Information and Communication Security Taskforce and the Formalization of the Cybersecurity Budget. These efforts will be supported by the Six Basic Joint Defense Agencies, an Inter-agency Joint Defense System, public-private partnerships across industry, academia, and research sectors, 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:

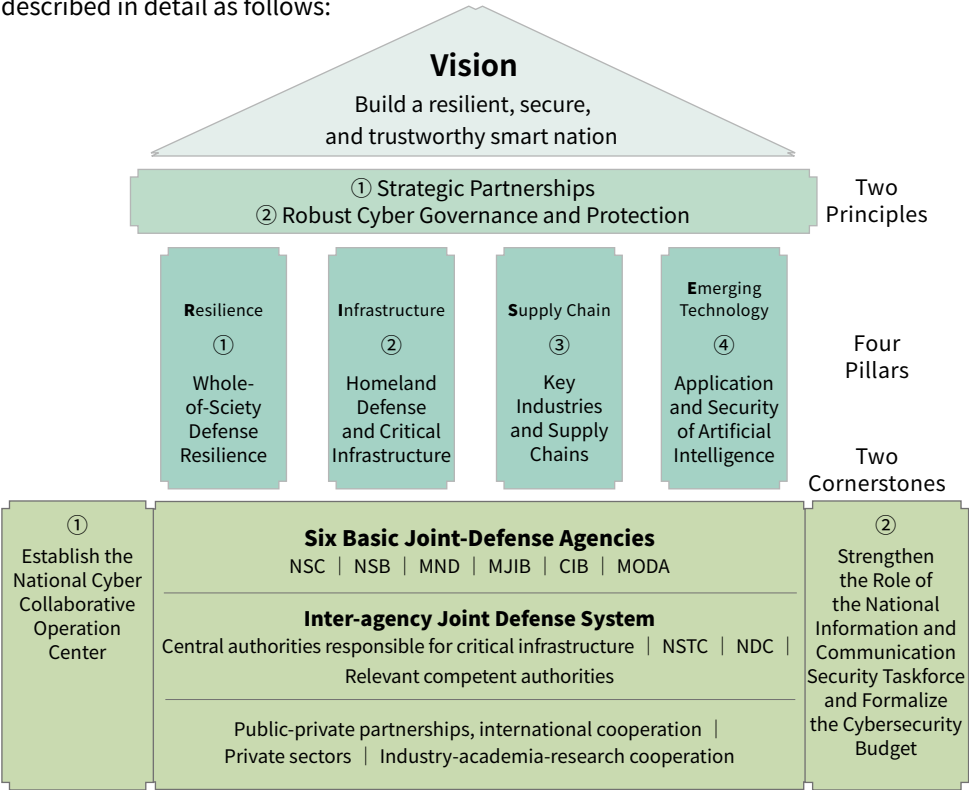


Figure 2. Key elements of the National Cybersecurity Strategy 2025



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 highlight its critical role in cybersecurity. Governance refers to the establishment of clear policies and procedures to ensure that cybersecurity objectives align with the organization's business needs, while also reinforcing leadership involvement and accountability. It encompasses not only risk identification and management but also the cultivation of a cybersecurity culture, ensuring that protective measures are effectively implemented across all levels of the organization.

In addition, the zero trust architecture has become 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 evolving threat landscape, operational resilience is another core component of cyber governance. Resilience emphasizes an organization's ability to respond quickly and recover effectively from cyberattacks, operational disruptions, or other uncertainties. Building resilience includes promoting the migration of critical system functions to offshore cloud backups, enhancing off-site redundancy and fault-tolerant infrastructure design, and guiding the public and private sectors in gradually transitioning to post-quantum cryptography to address future threats to encryption technologies.

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

- ① **Implement a cross-pillar zero trust architecture to strengthen cyber awareness and culture within public and private sector organizations.**
- ② **Implement cyber governance, establish data backups, and effectively protect data in both the public and private sectors.**
- ③ **Develop the cybersecurity protection architecture and management of post-quantum cryptography and promote its accelerated adoption across the public and private sectors.**

In terms of key strategic approaches, first, in the process of accelerating the implementation of comprehensive cyber governance and systems across public sectors and critical infrastructure, 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. This should be followed by broader promotion and adoption of zero trust architecture, with the implementation of its three core principles: identity authentication, device authentication, and trust inference. Public and private sector organizations should be supported in formulating corresponding strategies and implementation plans to establish a more resilient security mechanism. In addition, verification standards and guidelines must be developed to ensure the effectiveness of the zero trust mechanism, 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 application of new solutions, and further expand the adoption of innovative technologies to strengthen cybersecurity defenses.

At the same time, cooperation with domestic and foreign cloud service providers should be deepened, and cross-field establishment of overseas data backup and core function redundancies should be expanded to ensure that governments and enterprises can still maintain key business operations in the face of major cyber incidents or disasters. Digital governance and cross-border (cloud) transmission regulations should be continuously reviewed,

updated, and refined 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 internal threats, corresponding policies and regulations should be formulated, and necessary resources devoted to ensure that sensitive information is properly protected. Existing laws and regulations related to data encryption and communication transmission protocols should be reviewed and resources should be continuously devoted to implement encrypted data storage and secure transmission to reduce the risk of sensitive information being leaked or stolen. In addition, with the development of quantum computing technology, traditional encryption technology faces the risk of being cracked. Therefore, through cooperation between industry, academia, and research, the public and private sectors should be encouraged to re-examine and adjust the existing cybersecurity architecture and introduce post-quantum cryptography technology to ensure that future data protection mechanisms still have 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 cyber and communication supply chains to penetrate and attack, increasing the challenges in detection, defense, and attribution of causes. 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. Further incident attribution and joint accountability can make hacker organizations and their actions transparent, thereby increasing their operating costs and achieving effective deterrence effects.

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. The concept of helping others is protecting ourselves is the core value of international cybersecurity cooperation and establishing 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 countries. Facing the trend of rising geopolitical instability and confrontation, countries must work together to consolidate democratic supply chains and ensure the security and resilience of digital infrastructure and key technologies. Taiwan is at the forefront of this democratic supply chains and it is not only an important node in global cybersecurity but also should actively participate in international cooperation on cybersecurity. By strengthening our own cybersecurity protection and technological innovation, we can further become a key contributor to the regional and global cyber ecosystem and exert greater protective effects.

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

- ① **Comprehensively strengthen national defense and government preparedness capabilities using advanced strategic partners as benchmarks.**
- ② **Strengthen international cybersecurity cooperation and expand international joint defense efforts.**

③ **Support strategic partners in enhancing their cybersecurity capacity.**

To achieve the above goals and strengthen the interoperability and visibility of cybersecurity preparedness, the specific strategic approach is to strengthen the foundation of mutual trust with advanced strategic partners, enhance the cybersecurity preparedness of each pillar of this strategy, and facilitate smoother

collaboration between different countries and organizations. Continuing to strengthen international industry-government-academia exchanges and encourage domestic cybersecurity teams to participate in international competitions and forums will help establish closer relations of business collaboration, which will not only promote experience sharing but also expand influence in the global cybersecurity field. In addition, we should continue to draw on the practices of advanced strategic partners and promote the accumulation of private-sector cyber talent and technical capabilities, thereby strengthening 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 confidentiality levels, thereby laying a solid foundation for cooperation. At the same time, it is necessary to strengthen connections with the international cybersecurity community and actively participate in global cybersecurity cooperation and drills, thereby improving the situational awareness of foreign cyber threat intelligence and strengthening joint defense mechanisms. We should also actively invest in the development of the international cyber ecosystem, strive to attract international resources into the domestic cyber industry, further improve its development, and ensure alignment with international standards.

Finally, we should continue to actively share experiences of cybersecurity protection, policy formulation, and promotion, 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 promote the international development of the domestic cyber industry, local enterprises must be supported to span the international market and link up with international resources, so that domestic enterprises can access the global market and become important players in the international cyber ecosystem, thereby enhancing competitiveness and influence of Taiwan in the global cybersecurity field.



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 people-centric approach, which includes two main aspects. On the one hand, cybersecurity is a combination of advanced knowledge, skills, and insight, relying on the involvement of highly skilled professionals to maintain system security and drive technological innovation. On the other hand, people remain the greatest source of cybersecurity risks. Whether through inadvertently clicking malicious links or leaking sensitive information due to a lack of awareness, individuals can trigger serious threats. Therefore, continuous cybersecurity education and the enhancement of individual cyber awareness are essential. Just like developing epidemic prevention habits such as frequent handwashing and wearing masks, these practices are simple yet effective in reducing the threat of viral infection. Cultivating personal awareness and responsible online habits also strengthens the public's ability to face complex cyber threats, including disinformation, misinformation, and fraud. Moreover, Whole-of-Society Defense Resilience does not rely solely on individual efforts. It requires robust public-private partnerships. The government and private sector must work hand in hand to allocate resources and jointly build a resilient and defensive cybersecurity framework that lays a solid foundation for 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 In line with the establishment of the Whole-of-Society Defense Resilience Committee, expand the training and utilization of civilian resources and enhance response defense capacities.**
- ② Enhance public cybersecurity and data protection awareness, as well as the ability to detect disinformation, misinformation, and cognitive warfare tactics.**
- ③ Strengthen public-private partnerships to enhance the resilience and defense of the cybersecurity defense system.**

In terms of expanding the training and utilization of civilian wisdom and efforts, the specific strategy is to prioritize the establishment of an elite team of cybersecurity professionals and cooperate with public associations, academic societies, and related institutions to ensure that the capabilities of cybersecurity professionals continue to improve through regular exchanges, training, and drills, thereby enhancing the overall defensive capacity. We should actively expand the recruitment of international cyber talent to fill the current talent gap, and at the same time enhance the employment conditions for cyber professionals in the public sector and critical infrastructure fields to attract and retain outstanding professionals. On the other hand, cyber talent circulation channels and collaboration mechanisms between public and private sectors should be expanded to promote cross-domain resource sharing and improve overall cyber defense effectiveness.

In terms of popularizing cyber awareness, comprehensive cyber governance resources and basic cybersecurity protection support should be provided to enterprises at all levels in Taiwan's economic backbone, and enterprises should be assisted in establishing complete security mechanisms to enhance the risk resistance of the overall economic system. In order to deal with the increasingly serious problems of cybercrimes and fraud, public-private partnership and international cooperation should be promoted, security supervision of data-intensive industries such as e-commerce and social platforms should be strengthened, and a more complete warning, notification, and verification mechanism should be established, such as the application of digital forensics and

attribution techniques, to ensure that relevant risks can be discovered in time and responded to quickly. The promotion of personal identity authentication and verification mechanisms that combine convenience and privacy protection should also be expanded to reduce the risk of online impersonation fraud and enhance the credibility of online transactions and digital interactions.

In order to build social consensus and advance cybersecurity development, national cybersecurity summits will be held regularly to align efforts across sectors, consolidate actions, and foster innovation in cybersecurity applications. At the same time, cyber governance, incident response, and reporting mechanisms in the public and private sectors should be implemented to ensure that they can respond effectively when facing threats. Furthermore, we will review and update relevant procurement and budgeting regulations to foster a more secure and favorable digital environment. This will support industry, academia, and research institutions in the development and application of forward-looking technologies, and ensure the security of information and communications products throughout their life cycle.



Pillar 2: Homeland Defense and Critical Infrastructure

The cybersecurity of critical infrastructure is vital since these systems are at the core of keeping society functioning. When infrastructure such as oil, water, electricity, communications, transportation, finance, and healthcare is disrupted by cyberattacks, it can lead to a social shutdown, cause incalculable damage to economic activities, public security, and people's lives, and further weaken the country's stability and the public's trust in the government.

In the field of national defense, the importance of cybersecurity is reflected in maintaining the security of the national military's combat command and control system, ensuring that facilities, equipment, communications, and decision-making are not interfered with. In addition, cybersecurity capabilities are an important extension of national defense strategy and combat strategies. The military must possess the capability to effectively counter foreign cyberattacks, to prevent adversaries from sabotaging defense systems, stealing sensitive information, or paralyzing combat capabilities. In this regard, cybersecurity serves as the cornerstone of homeland security and the effectiveness of national defense.

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

- ① **Comprehensive review of potential cybersecurity risks in homeland defense and critical infrastructure and propose countermeasures to enhance the security and proactive defense capacity of critical infrastructure.**
- ② **Implement cyber governance and improve cyber defense and resilience in the four major fields of national defense, people's livelihood, disaster prevention, and democracy.**
- ③ **Strengthen cybersecurity preparedness to safeguard national security and uphold regional peace and stability.**

In terms of specific strategies and practices, we should first establish the new National Cyber Collaborative Operation Center to comprehensively grasp national-level cybersecurity risks, enhance the coordination of incidents and manpower, and ensure that resources can be quickly mobilized and effectively deployed when facing significant cyber threats. Furthermore, the government should clearly formulate cybersecurity readiness requirements and strategic objectives, covering national defense and law enforcement agencies, and focus resources on enhancing intelligence gathering, attribution, and proactive defense capabilities to establish a more robust cybersecurity readiness system. At the same time, a comprehensive checking and management of the systems, networks, and equipment of important government agencies and critical infrastructure should be conducted based on risk levels, and a regular inspection mechanism should be established to ensure the implementation of management, maintenance, and upgrade protocols. In order to continue to consolidate defense capabilities, the competent authorities and the central authorities in charge of relevant industries should strengthen their supervision responsibilities over critical infrastructure, implement cyber incident investigation and accountability mechanisms, and ensure that all units meet the required standards for responding to cybersecurity risks.

Based on the above, relevant national security and cybersecurity agencies should cooperate with the central authorities responsible for critical infrastructure to formulate and implement "Cybersecurity Action Plans" for critical infrastructure sectors such as energy, communications, transportation, finance, and healthcare, to strengthen their system network resilience. For critical infrastructure with system dependencies, cyber defense standards should be elevated to ensure that basic operations can still be maintained under extreme conditions. Moreover, the cybersecurity budget for the public sector and critical infrastructure should be formalized, and the replacement and upgrading of ICT equipment should be accelerated to ensure the continued safe operation of systems. A cross-agency government operations platform should also be established to focus on strengthening operational resilience during emergencies.

In order to strengthen cyber defense capabilities, a dedicated cybersecurity protection team should be established to respond to critical infrastructure emergencies through regular training and drills to ensure that cyber talent has the capability for immediate response and effective problem-solving. In addition, technical testing of key systems within public agencies, national defense, and critical infrastructure should be implemented, and third-party red team exercises and tabletop exercises should be promoted to test and verify cyber defense and response mechanisms. The content of the drill should cover response measures for data leakage, and the tabletop exercise should be led by the organization's senior management and the Chief Information Security Officer (CISO) to ensure that decision-makers are capable of effectively handling cyber incidents. These efforts will enable the government and critical infrastructure providers to respond quickly and preventively to various cyber threats, and further strengthening Taiwan's homeland security and the protection of its critical infrastructure.

Pillar 3: Key Industries and Supply Chains

Domestic key industries, including the *Five Trusted Industry Sectors*, form the foundation of economic prosperity and development. Along with core service industries such as communications, finance, and healthcare that sustain societal operations, both groups must ensure cybersecurity, protect intellectual property, and build resilience for continued operations. Therefore, for national and economic development, key industries and supply chain security are critical priorities for cybersecurity protection. Especially in the era of globalization of the supply chain, preventing cyber threats targeting key industries and their supply chains is the primary task of safeguarding national and economic interests. For the international community, strengthening the cybersecurity of key industries is also a crucial element in reinforcing the democratic supply chains, ensuring that global cooperation is based on secure and trustworthy technology and an industrial ecosystem.

In addition, in order to continue the strengthening of cybersecurity protection of key domestic industries and supply chains, it is also important to

foster the development of domestic cyber industries and startups. Supporting local cybersecurity innovation not only enhances indigenous technological capabilities but also enables Taiwan to exert greater influence on the international stage. The vigor of cyberindustry development not only meets the needs of the local market, but also promotes technological exports, facilitates industrial upgrade, and attracts more cyber talents to join, thereby injecting new momentum into economic growth. Only by combining the promotion of cybersecurity in key industries and supply chains with the innovative development of the cyber industry can Taiwan's cybersecurity capabilities take root comprehensively and effectively respond to the challenges of geopolitics and digitalization. Therefore, the third pillar of this strategy would be: Key Industries and Supply Chains, with the following main objectives:

- ① **Review and strengthen the cybersecurity frameworks of key domestic industries (such as the *Five Trusted Industry Sectors* and data-intensive industries such as finance, communications, and healthcare) to consolidate local cyber industry.**
- ② **Promote the reduction of cybersecurity risks and the implementation of Business Continuity Management (BCM) in key industries.**
- ③ **Expand investment in the cyber industry and foster innovation and startups.**

In order to strengthen supply chain security, a specific strategy involves cooperation with industry associations and leading enterprises, to conduct a comprehensive assessment of key industries, important enterprises, supply chains, and their key resources, and to establish a risk management list to ensure supply chain visibility and security. On such basis, we should also initiate Cybersecurity Action Plans to meet the needs of key industries, while expanding the scope of implementation step by step to enhance the overall capability of cyber governance. In addition, the labeling and certification systems for government procurement and cybersecurity-related products should be improved, and cybersecurity standards should be strengthened for

the procurement of software, hardware, and services by the government and critical industry supply chains. By establishing robust labeling and certification mechanisms for suppliers and products, supply chain security can be ensured. Furthermore, key government suppliers and designated product projects should be specifically reinforced to prioritize the reduction of cybersecurity risks from the government procurement side.

To improve the cybersecurity capabilities of key industries, communication and exchanges between enterprises should be promoted. Moreover, regular training programs and the sharing of major vulnerabilities should be implemented to reinforce cyber awareness, technical capacity, and data security. At the same time, all key industries, and their supply chains, including the defense supply chains, are encouraged to establish joint defense mechanisms to strengthen cybersecurity coordination and enhance overall resilience to cyber threats. In addition, cyber governance measures should be implemented in key industries, and their defense and response capabilities should be verified through red team exercises to ensure an effective response to cyber incidents.

To facilitate the autonomous development of the cyber industry, regulatory requirements for both the public and private sectors should be enhanced, and a healthy environment for industry development should be established. Regular reviews and the introduction of incentive measures, including expanding tax deductions for cybersecurity investments such as bug bounty programs and third-party assessments, tightening requirements in government procurement contracts, and evaluating both domestic and foreign cybersecurity companies, are measures that should be implemented to enhance enterprises' cyber governance, strengthen protection capabilities, and drive the development of Taiwan's cyber industry. In addition, investment in and support for various cybersecurity startups should be expanded to promote industrial scale and international development, establish a comprehensive cybersecurity human resources supply-demand ecosystem, strengthen the competitiveness of the cyber industry in Taiwan, and ensure the security and resilience of our 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 promoted through three aspects: technology, talents, and systems. First, the government should work with the private sector to devote more resources to the research and development of AI security technologies and applications, to jointly respond to the threats posed by rapidly evolving emerging technologies. At the same time, it is also necessary to cultivate large numbers of professionals in both cybersecurity and AI to ensure that the country has sufficient technological and human resources to meet the challenges. Improving systems and regulations helps facilitate safe AI application and international cooperation, maximize AI's potential, and reduce associated risks. The main objectives and strategic approaches of this pillar include:

- ① Apply AI technology to enhance cybersecurity protection in Whole-of-Society Defense Resilience, Homeland Defense and Critical Infrastructure, and Key Industries and Supply Chains, while fostering an industrial ecosystem.**
- ② Ensure the security and trustworthiness of AI technologies themselves.**

In order to promote AI application in the cybersecurity field, and to strengthen overall security resilience, specific strategies include: enhancing cooperation across public and private sectors and industries in AI research and development, and strengthening the cybersecurity defense capabilities through automated cybersecurity management and governance, such as using AI to find vulnerabilities and provide solutions. In addition, relevant competitions can be held to facilitate research, development, and application of technology, and encourage enterprises and research institutions to invest in the development of AI technology. To further improve the overall technological standards of cybersecurity, we should also promote AI integration into the cybersecurity field by establishing a cybersecurity technology park, complete with incubation mechanisms, to attract outstanding domestic and foreign talents and companies, forming an industrial cluster.

In order to build an autonomous, inclusive, and competitive cybersecurity ecosystem, and promote the full integration of the cyber industry with market demand, AI technology should be used as the core to connect cybersecurity service providers across the upstream, midstream, and downstream sectors, along with the demand side, including key industries, critical infrastructure, and government agencies. This will promote a close integration between the cyber industry and market demand, establish a virtuous cycle, and drive the overall development of the industry. In terms of technical governance, the secure-by-design (SbD) principles, safety, and trustworthiness of AI systems should be actively promoted to ensure that AI technology incorporates risk management mechanisms at the source, thereby reducing potential cybersecurity risks.

On the other hand, international AI-related standards should be developed and aligned, while encouraging companies in the private sector to develop technologies that comply with international standards, thereby laying the foundation for the long-term development of the AI security industry. In order to ensure the secure application of AI technology, we should comprehensively review current regulations, promote the widespread adoption and application of forward-looking AI technologies, and develop a robust cyber governance mechanism to maintain high standards of cybersecurity management in an AI-driven environment. To enhance the defense resilience of the whole society, it is also important to strengthen the capacity to address and investigate risks such as cognitive warfare and cyber fraud, ensuring that AI development won't become a cybersecurity vulnerability, but a key driving force for security improvement.



Two Cornerstones

I. Establish the National Cyber Collaborative Operation Center

In order to achieve the vision of this strategy of building a resilient, secure, and trustworthy smart nation and consolidate the four pillars, a National Cyber

Collaborative Operation Center should be established with sufficient investment in funding, talent, and other resources, to integrate collaborative operations such as collection, analysis, and sharing of cyber threat intelligence, joint defense, and support for major cyber incidents. The key tasks include:

- ① **Develop a national cybersecurity risk map to accurately assess cybersecurity risks at the national level.**
- ② **Expand the collection of cybersecurity monitoring intelligence across public and private sectors, industries, and international partners to enhance threat visibility.**
- ③ **Coordinate and jointly handle and support major cyber incidents, formulate operating guidelines and work guidelines, and improve integrated response efficiency.**

II. Strengthen the Role of the National Information and Communication Security Taskforce and Formalize the Cybersecurity Budget

Strengthen the existing function of the National Information and Communication Security Taskforce under the Executive Yuan as the central coordinating and supervisory body for this strategy and government cybersecurity affairs, by further enhancing its role and capacity. Important tasks include:

- ① **Coordinate and supervise inter-agency cybersecurity affairs, promote regulatory adaptation, and ensure effective legal compliance.**
- ② **Ensure that government agencies and critical infrastructure have adequate cybersecurity budgets and manpower, and assess the effectiveness of their implementation of cybersecurity protection.**
- ③ **Expand private sector participation and promote public-private partnerships.**



Cross-Pillar Foundation

I. Six Basic Joint Defense Agencies (Six Basics)

Based on the previous Six Basic Joint Defense Agencies, and with national security as the core strategy, we connect the six key agencies of 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). Its primary task is to ensure the planning, implementation, and oversight of basic protection measures related to cybersecurity. Among them, MND is responsible for cybersecurity and proactive defense of the military sector; NSB is responsible for cybersecurity protection and intelligence collection and analysis of the intelligence agencies; MODA is responsible for strengthening the governmental digital resilience, implementing cybersecurity laws and regulations, and enhancing the cybersecurity of industries and public cyber awareness; MJIB and CIB are the main forces for digital forensics, attribution, and law enforcement of cybercrime.

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

In line with the continuous upgrading of *Cybersecurity is National Security*, we will include subordinate non-departmental public bodies, and the critical infrastructure, key industries, and their supply chains that fall under its jurisdiction or supervision (as shown in Figure 3). Important tasks include resource allocation, combining the capacities of private industry, academia, and research, and promoting scientific research and industrial development. Other key tasks are cyber governance of critical infrastructure, budget allocation, supervision and execution, protection of important data and systems, promotion and advanced deployment, cyber diplomacy cooperation, etc.

III. International Cooperation of Strategic Partners

Taiwan stands at the front line of the world's democratic coalition. The aim of this strategy focuses on cooperating with advanced strategic partners and like-minded friendly countries and actively participating in the affairs of international organizations, cybersecurity professional communities, and industry-academia-research collaboration. Through public-private partnerships and international cooperation, Cybersecurity protection will be effectively improved, and influence will be expanded.

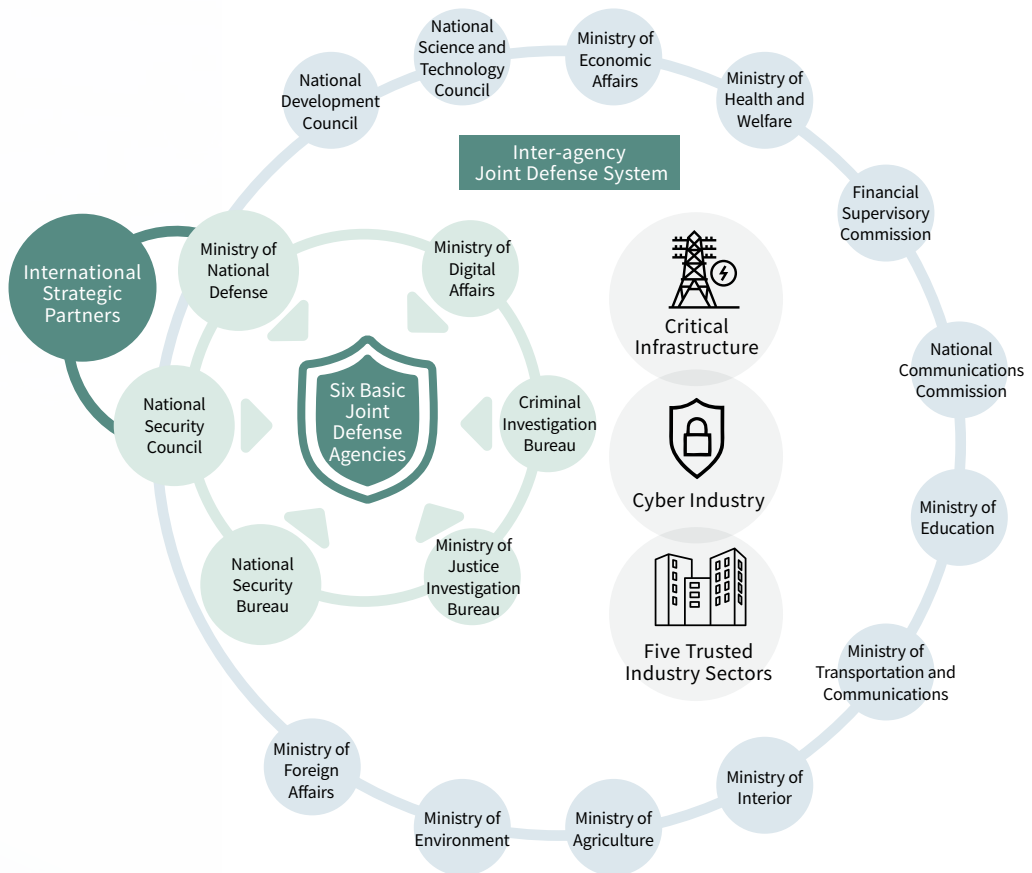


Figure 3. Cross-pillar base and public-private partnership team

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



Cybersecurity is national security. In the face of increasingly escalating cyber threats and challenges, Taiwan must demonstrate whole-of-society participation, comprehensive investment of resources, and top-down commitment to effectively strengthen the country's cyber resilience and protect democracy, freedom, and industrial prosperity. Current cyber threats are no longer limited to the technical level, they have far-reaching implications for national security, economic and social stability, and government operations. National hacker organizations, AI-driven hybrid attacks, and supply chain security risks continue to emerge. As a geopolitical hub and an important partner in the international supply chain, Taiwan is at the forefront of global cybersecurity and bears undeniable responsibility.

Against this background, the *National Cybersecurity Strategy 2025* highlights building a resilient, secure, and trustworthy smart nation as its ultimate vision, and proposes a strategic framework with four pillars, such as Whole-of-Society Defense Resilience at its core, and includes key initiatives such as the implementation of a zero trust architecture, the development of proactive defense capabilities, the deepening of international joint defense, ensuring the security of AI applications. These strategies require not only a comprehensive upgrade of technology, policies and regulations, but also full participation of society, including government, enterprises, academia, and the private sector, to create a cybersecurity protection community that unites every effort to meet future challenges.

Public participation is the key to cybersecurity protection. The government should take the lead in investing more resources, showing top-down commitment, and accelerating transformation. From threat assessment and policy formulation to resource allocation and strengthening mechanisms, the government will focus on implementing a robust cyber governance framework as its core policy, enhancing the resilience and protection of the public sector and critical infrastructure. At the same time, it is necessary to deepen cooperation with international public and private sectors, strengthen intelligence sharing and joint defense capabilities, and ensure Taiwan plays a more significant role in the global cybersecurity ecosystem. In addition, we

must vigorously cultivate and recruit cyber talents, foster industrial innovation, achieve cybersecurity democracy, and adopt incentive measures to encourage enterprises to strengthen cyber governance, creating a self-sustaining cycle of industry-driven improvement.

Cybersecurity challenges transcend borders. Only by uniting the nation, integrating resources, and fully committing to their efforts can Taiwan's security and development be ensured in the global digital competition. We need to respond to cyber threats with foresight and action, protect the country's freedom, democracy, and industrial prosperity with determination and strategy, and build a smart nation that is resilient, secure, and trustworthy for all citizens. In the future, through continuous efforts and reforms, we will gain a firm foothold on the international stage of cybersecurity and become a global 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 :

Tzong-Chen Wu	Distinguished Professor, Department of Information Management, National Taiwan University of Science and Technology
Benson Wu	Director, Information Service Industry Association of R.O.C. And Chairman, Cybersecurity Resilience Promotion Association
Jung-Shian Li	Professor, Department of Electrical Engineering, National Cheng Kung University
Alan Lee	Executive Director, Association of Hackers in Taiwan
Hahn-Ming Lee	Distinguished Professor, Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology
Der-Tsai Lee	Academician, Institute of Information Science, Academia Sinica
Bo-Yen, Shen	Chairman, Information Service Industry Association of R.O.C.
Ying-Dar Lin	Chair Professor, Department of Computer Science, National Yang Ming Chiao Tung University
Robert Chin	Chairman, Taiwan Chief Information Security Officer Alliance
Yun Hsia	Researcher, National Institute of Cybersecurity
Yeali S. Sun	Professor, Department and Institute of Information Management, National Taiwan University
Allen Own	Chairman, Association of Hackers in Taiwan
Hao-Wei Chen	Founder, Taiwan International Foundation
Shi Chen	Assistant Professor, Department and Institute of Banking and Finance, Chinese Culture University
Kenny Huang	Chairman, Taiwan Network Information Center
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
Chen-Yu Dai	Director, Association of Hackers in Taiwan Member, Office of the President Whole-Of-Society Defence Resilience Committee

(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



Download Strategy

NATIONAL CYBERSECURITY STRATEGY 2025

Cybersecurity is National Security

building a resilient, secure,
and trustworthy smart nation



National Information and
Communication Security Office