National Chengchi University College of International Affairs Center for Global Military Strategy and Defense Policy Annual Report Academic Year 114

Center Name	Center for Global Military Strategy and Defense Policy
Director	Professor Hong-Yi Lien, Department of Diplomacy
Implementation Period	August 1, 2024–July 31, 2025

Participants	**I. Key Personnel**
	(e.g., Executive Director, Advisors, etc.)
	• **On-campus:**
	  ○ Professor Lien Hong-yi, Department of Diplomacy
	• **Off-campus:**
	  ○ Professor Liou Shiau-shyang, Institute for National Defense and Security Research
	II. Other Personnel
	(e.g., assistants, staff, or contracted personnel)
	• **On-campus:**
	  ○ Huang Chien-hao
	• **Off-campus:**

Report Submission Date	July 31, 2026

Results Report and Future Work Plan

I. Work Achievements for the Academic Year

◉ Focus on National Defense Lecture Series (XII): National Emergency Mechanisms, Resilience Reserves, and International Partnerships *(Held on March 25, 2026)*

The College of International Affairs and the Center for Global Military Strategy and Defense Policy Studies jointly held the twelfth lecture in the *Focus on National Defense* series on March 25, 2026. The lecture focused on **"National Emergency Mechanisms, Resilience Reserves, and International Partnerships."** It was delivered by Lieutenant General Bai Chieh-lung, a senior researcher commissioned by the Institute for National Defense and Security Research, and moderated by Professor Lien Hong-yi, Director of the Executive Master's Program in Strategy and International Affairs in the Department of Diplomacy. The event attracted a large number of faculty members and students and examined Taiwan's current preparations and efforts to respond to national emergencies.

National Emergency Mechanisms: From Constitutional Foundations to Mobilization in Practice

Researcher Bai began by examining the institutional design of national emergency mechanisms, explaining the legal and policy foundations governing Taiwan's response to war or major crises. He noted that when the country faces escalating threats, the president may issue emergency orders in accordance with the Additional Articles of the Constitution of the Republic of China, providing a mechanism for rapid responses under extraordinary circumstances.

Regarding mobilization, Researcher Bai further explained that once mobilization is implemented, the government has broad authority to allocate resources. These powers include requisitioning supplies, regulating transportation and communications, and managing financial and foreign exchange activities. Responsibilities are distributed among the relevant ministries and agencies to ensure the continuity of national operations and meet defense requirements during wartime.

Using the Russia–Ukraine war as an example, Researcher Bai emphasized the importance of determining the appropriate timing and scale of mobilization. Mobilizing too early may trigger economic and social instability, while mobilizing too late may result in missed opportunities for defense. Excessive mobilization may make resources or facilities targets for enemy attacks, whereas insufficient mobilization may fail to protect the country effectively. Ukraine's decision to issue its mobilization order shortly before the outbreak of war illustrates the need for decision-makers to balance strategic judgment against political risks.

Resilience Reserves: Building a Whole-of-Society Defense Capability

In discussing resilience reserves, the speaker stressed that modern national security depends not only on military capabilities but also on society's overall capacity to withstand and recover from disruptions. Taiwan is currently advancing relevant policies through the Whole-of-Society Defense Resilience Committee. Its work covers five major areas: civilian training, the supply of essential goods, energy and infrastructure maintenance, healthcare and evacuation systems, and the security of information, communications, and financial networks.

Overall, the central objective of resilience reserves is to ensure that **preparations made in peacetime can be put to use during wartime**, enabling the country to maintain its basic functions and social order even under extreme circumstances.

International Partnerships: From Supply Chains to Strategic Coordination

Regarding international cooperation, Researcher Bai noted that Taiwan is located along the First Island Chain and faces major-power threats from the Chinese Communist Party. National security cannot be shouldered entirely by any single country; instead, partnerships are needed to complement resources and coordinate tactics.

Using the Russia–Ukraine war as an example, he explained that Ukraine's ability to sustain its resistance has depended in part on international partners, including NATO members, providing weapons, energy, and logistical support. These contributions have enabled Ukraine to maintain its capacity for prolonged operations against a stronger adversary.

He further pointed out that effective international partnerships require stable economic and trade networks and supply-chain cooperation to be established during peacetime. The speaker emphasized that the principle of **"defending one's own country through one's own efforts"** remains fundamental. International cooperation can deliver its greatest benefits only when a country has first established adequate resilience reserves.

Q&A and Discussion: Gray-Zone Threats and Taiwan's Defense Strategy

During the Q&A session, participants raised concerns about Taiwan's challenges in responding to gray-zone operations and safeguarding energy security. Researcher Bai observed that the

international environment remains characterized by power competition and strategic deterrence, with decisions about whether to engage in war shaped by the costs and risks perceived by the parties involved. He also emphasized that Taiwan's strengths lie in its democratic institutions and international legitimacy, and that it should continue strengthening its deterrence capabilities and strategic communication.

In response to questions about domestic mobilization and civilian participation, he noted that Taiwan already has a clear legal and regulatory framework. Going forward, institutional design and policy incentives should be used to encourage businesses and broader social forces to participate in the national defense system.

This event was the twelfth session in the College's *Focus on National Defense* lecture series. By examining national mobilization and resilience-building from institutional, policy, and international perspectives, it deepened faculty members' and students' understanding of modern national security systems. Through Researcher Bai's practical experience and policy analysis, participants gained a more comprehensive understanding of Taiwan's response strategies and development priorities in a complex security environment. The College of International Affairs will continue promoting discussions on related issues to strengthen dialogue and connections between academia and policy practitioners.






聚焦國防系列演講(十二)
國家緊急機制、韌性儲備
與國際友盟運作

⊙ Taiwan Security Forum (XVIII): Focusing on the Digital Battlefield, Supply Chains, and National Security Strategy *(Held on April 18, 2026)*

The College of International Affairs and the Center for Global Military Strategy and Defense Policy Studies held the eighteenth *Taiwan Security Forum* on April 18, 2026. The forum was titled **"Cybersecurity Is National Security: Rethinking Taiwan's Security in an Era of Technological Competition."** It brought together experts and scholars from the Institute for National Defense and Security Research and National Chengchi University to discuss how technology is reshaping national security systems.

The forum was chaired by Dean Lu Yeh-chung of the College of International Affairs. The panelists included Ho Tseng-yuan, Director of the Cybersecurity Research Institute at the Institute for National Defense and Security Research; Wu Tsung-han, Assistant Research Fellow at its Institute for Strategic Studies; Lin Chun-jung, Policy Analyst at its Institute for Strategic Studies; Lin Pi-chao, Emeritus Professor at the College of International Affairs; and Chen Ping-kuei, Director of the Graduate Institute of National Development and Security. Together, they explored new challenges to national security in the digital age, addressing military transformation, the development of cyber warfare, supply-chain risks, and national strategy.

The Transformation of Warfare: From "System Engineering" to "Mission Engineering"

At the beginning of the forum, Ho Tseng-yuan noted that the nature of modern warfare has undergone a fundamental transformation. Traditional military thinking has focused on the performance and development of individual weapons systems. However, this approach is increasingly inadequate for addressing the complex operational requirements of contemporary battlefields.

Ho emphasized that warfare has entered an era of integrated, system-level operations. Military planning is no longer confined to the performance and deployment of individual pieces of equipment; instead, it focuses on integrating capabilities to achieve mission objectives. This shift requires decision-makers to make judgments in increasingly complex information environments. The outcome of a battle now depends more heavily on the ability to integrate information and make timely decisions.

The Rise of Cyber Warfare: Cyberspace as the "First Battlefield"

Wu Tsung-han examined the development of cyber warfare, noting that cyberspace has become a frontline of major-power competition since Russia launched cyberattacks against Estonia in 2007. During the Russia–Ukraine war in 2022, cyberattacks occurred alongside physical military operations, further demonstrating that the battlefield has expanded comprehensively into the digital domain.

Taiwan has also long faced a high level of cyberattacks. Public-sector institutions and educational organizations are among the principal targets. As campus systems are interconnected with government networks, weaknesses in their security defenses may create vulnerabilities that adversaries can exploit to infiltrate these systems.

From Defense to Resilience: A Shift in National Security Governance

In response to an increasingly complex threat environment, the transformation of national security thinking was another major topic of discussion. National security is gradually shifting from a **defense-oriented approach to a resilience-oriented approach**. Wu argued that completely preventing cyberattacks is nearly impossible in the modern digital environment. The critical issue is therefore a system's ability to recover after an attack.

Wu stressed that cybersecurity is no longer merely a specialized technical issue; it is a basic capability that every citizen should possess. Everyday digital activities and the protection of personal data are both closely connected to national security.

Supply-Chain Risks: From the Evolution of Malware to Structural Infiltration

Lin Chun-jung examined cybersecurity from a supply-chain perspective, pointing out that security risks have become deeply embedded in technology production systems. Drawing on the experience of Eastern Europe after the Cold War, she explained that early computer viruses were often expressions of technical showmanship and creativity. As technology evolved and state actors became involved, however, malicious software increasingly developed destructive capabilities and intelligence-gathering functions, alongside more sophisticated mechanisms such as backdoors and remote control.

The Intersection of Technology and Geopolitics: Zero-Trust Architecture and Governance Tools

Lin further noted that supply-chain issues are not merely technical concerns; they are closely related to geopolitics. Some countries, for example, use legal requirements to compel companies to cooperate with intelligence-gathering activities, turning supply chains themselves into instruments of national strategy.

Cybersecurity risks can emerge at multiple stages. These include malicious components introduced during manufacturing, backdoors concealed within operating systems, and infiltration attacks targeting end users. Addressing these challenges requires a comprehensive cybersecurity strategy.

Lin also observed that cybersecurity incidents frequently originate from human error. Education and institutional measures are therefore equally important. Businesses and government agencies should strengthen users' cybersecurity awareness and reduce risks at their source.

The Practical Challenges and Strategic Adjustments of "Non-Red Supply Chains"

Addressing supply-chain security, Chen Ping-kuei noted that completely excluding a particular country from supply chains is difficult to achieve in practice. A more feasible policy approach is to gradually reduce dependence, prioritizing high-risk or highly sensitive areas for enhanced safeguards and adjustments in order to mitigate systemic risks.

Compared with earlier forms of competition centered on military equipment and industrial production capacity, contemporary competition depends more heavily on cross-disciplinary knowledge integration and sustained investment. This creates greater demands on national finances and talent systems.

Chen further emphasized that technological innovation today is driven primarily by the private sector rather than by state institutions. Accordingly, the key to evaluating technological development is not whether a technology has a specific application, but whether it can evolve into a **general-purpose technological framework** that can be widely applied and reused across different industries. Only by doing so can technological achievements accumulate over time and become a

foundation for national competitiveness, thereby supporting the long-term enhancement of national strength.

A National Strategic Perspective: Technological Competition and Institutional Resilience

Lin Pi-chao approached the issue from the perspective of national strategy, noting that technology has become a key means of compensating for disparities in national power amid contemporary international competition. Whereas traditional measures of power emphasized population size and military scale, modern states increasingly rely on information technology and digital capabilities to improve governance and strengthen defense. Technological competition has consequently become an important component of international politics.

He further explained that different political systems exhibit institutional differences in technological development and application. Democratic countries must advance technology governance while safeguarding the rule of law and individual freedoms. Although policy-making processes may be more complex, institutional trust and social integration can strengthen overall stability and effectiveness.

On this basis, Lin emphasized the importance of **resilience** as a concept in national security. The key is to improve the ability of institutions and society to continue functioning when confronted with disruptions, thereby responding to a highly uncertain international security environment.

Finally, he noted that advances in artificial intelligence and digital technology are gradually changing the ways humans interact with machines. These developments make technology governance increasingly complex and demand sustained attention over the long term.

Balancing Technology and National Security

During the Q&A session, participants discussed Taiwan's position in global technological competition. The scholars generally agreed that Taiwan's strengths lie in the flexibility and integration capabilities of its industrial clusters, as well as its ability to play a key role in global supply chains.

However, technological development must be aligned with national security, and the protection and control of critical technologies are equally important. The government must therefore maintain openness and

international cooperation while ensuring that core technologies do not flow overseas excessively, thereby safeguarding Taiwan's long-term strategic interests.

The forum concluded by emphasizing that, in an era shaped by the intersection of digitalization and globalization, cybersecurity has become a concern for society as a whole. Every aspect, from personal data protection to critical national infrastructure, is closely connected to national security.

Only by raising public cybersecurity awareness, strengthening institutional design, and deepening international cooperation can Taiwan establish a stable and resilient national security system capable of addressing the challenges of technological competition and security threats.




大語言當中所潛藏的風險


大語言當中所潛藏的風險