Cybersecurity Analysis in Thailand: Trends, Challenges, and Policy Insights from Case Studies of SMEs, Mobile Banking, and Port Infrastructure

Academic Article

Chanin Taeratanachai[1] and Rawida Wiriyakitjar[2]
Business School, University of Thai Chamber of Commerce,
Bangkok, Thailand 10400[1-2]
E-mail: chanin_tae@utcc.ac.th[1] (Corresponding Author) and rawida_wir@utcc.ac.th[2]

Abstract

This academic article analyzes the emerging trends and challenges in cybersecurity within the context of Thailand, focusing on three key sectoral case studies: small and medium-sized enterprises (SMEs), mobile banking, and port infrastructure. Amid the rapid transformation toward a digital economy, these sectors face growing cyber risks that could undermine the country's economic security. The article advocates for the adoption of Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), to enhance threat detection, incident response, and predictive risk analytics. Nonetheless, Thailand continues to encounter critical obstacles, including limited technical readiness, fragmented governance, and a relatively low rate of AI adoption. The article concludes by proposing strategic policy recommendations to strengthen national cyber resilience through the integration of regulatory frameworks, technological innovations, and multi-stakeholder collaboration-ensuring a sustainable and secure cybersecurity environment for Thailand's digital future.

Keywords: Cybersecurity, Artificial Intelligence, Digital Economy, Critical Infrastructure, Threat Detection

Received : May 26, 2025 Revised : June 5, 2025 Accepted : June 13, 2025

1. Introduction

1.1 Importance of Cybersecurity in the Digital Age

The rapid evolution of internet technologies has reshaped social, economic, and political landscapes across the globe. Digital systems now underpin critical sectors such as communication, commerce, education, healthcare, and governance (Yeasmin, 2024, p.53-67). As digital transformation continues to accelerate, the interconnectedness of devices, systems, and users has expanded the attack surface, exposing vulnerabilities that can be exploited by cybercriminals, hacktivists, and even state-sponsored actors. Key contributing factors include software vulnerabilities, insecure network protocols, device proliferation, and complex IT architectures (Mallick & Nath, 2024, p.1-69). Despite the significant efficiency and productivity gains brought by digitalization, these advancements have introduced corresponding risks that must be addressed through effective cybersecurity measures. Cybersecurity, therefore, plays a foundational role in ensuring trust, stability, and the continued functionality of digital ecosystems (Kumar et al., 2024, p.1-10). It involves not only the implementation of protective technologies, but also regulatory compliance, risk governance, and public awareness.

1.2 Linkages with National Security

In today's interconnected world, cybersecurity has evolved beyond the boundaries of traditional IT systems and emerged as a cornerstone of national resilience. The increasing interdependence of digital infrastructures, communication systems, and societal functions creates new vulnerabilities that require coordinated national and international strategies. Rather than relying solely on conventional protection mechanisms, countries must adopt a maturity-based approach that promotes cyber resilience—encompassing strategic planning, capability assessments, and cross-sectoral collaboration between public and private stakeholders (Sharkov, 2020, p.5-24). The rising frequency and sophistication of cyber threats underscore the urgent need for robust and adaptive security frameworks (Firmansyah, 2024, p.280-320). Such incidents often result in financial losses, reputational damage, privacy violations, and threats to national security. Developing effective strategies requires a nuanced understanding of the evolving threat landscape to bolster resilience, foster cross-sector collaboration, and maintain public trust (Salman & Alsajri, 2023, p.73-85).

In the digital age, cybersecurity is a critical enabler of national resilience, safeguarding sensitive data, critical infrastructure, and essential services amid rising threats (Basak, 2024, p.1361-1382). As sectors like energy, healthcare, transportation, and telecommunications become increasingly digitized, their vulnerability to sophisticated attacks-often by state actors or organized cybercriminals-intensifies. Countries like Thailand, undergoing rapid digital integration, must adopt adaptive and collaborative cybersecurity strategies to protect vital sectors such as mobile banking, SMEs, and port infrastructure, ensuring both economic stability and national security (Bellamkonda, 2020, p.273-280).

1.3 Objectives of the Article

This article aims to analyze the evolving cybersecurity landscape in Thailand by focusing on three sectoral case studies: SMEs, mobile banking, and port infrastructure. These sectors were selected based on their vital roles in the Thai digital economy and their high exposure to cyber risks. SMEs are a key driver of global economic growth, particularly in developing nations like Thailand, where they contribute more than one-third of the national GDP. Despite their importance, these enterprises often suffer from chronic underinvestment in cybersecurity, leaving them increasingly vulnerable to digital threats (Thamrongthanakit, 2023). Mobile banking, a cornerstone of Thailand's financial inclusion policy, sees widespread daily use but poses substantial privacy and fraud risks, particularly among digitally vulnerable populations (Limna et al., 2023, p.1133-1151; Thetlek et al., 2024, p.264-272). Maritime ports, essential for international trade, have rapidly digitized logistics systems but remain susceptible to targeted cyberattacks due to aging infrastructure and fragmented governance (Senarak, 2021, p.20-36; Office of National Economic and Social Development Council [NESDC], 2024; Janmethakulwat & Thanasopon, 2024, p.157-166).

The article also explores the application of Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), in enhancing threat detection, predictive risk analysis, and automated response capabilities. It identifies technical and policy challenges, including low AI adoption, fragmented governance, and limited cyber literacy. Finally, it offers strategic recommendations across national, organizational, societal, and international levels to improve cyber resilience and ensure sustainable digital development in Thailand.

To contextualize the analysis of cybersecurity challenges, the following section delves into three selected sectors-SMEs, mobile banking, and port infrastructure-based on their significant economic relevance, increasing digitization, and heightened vulnerability to cyber threats. These sectors also illustrate the diversity of challenges across enterprise scale, user trust, and critical infrastructure. The goal is to draw lessons from these case studies to inform targeted, practical, and sector-specific policy recommendations.

2. Cybersecurity and cybercrime in Thailand

Thailand ranks among the top ten countries globally for average daily internet usage, with users spending over eight hours online each day (Walderich, 2023). This extensive online engagement has fueled the rapid expansion of Thailand's e-commerce sector, while simultaneously exposing users to significant cybersecurity threats. Common attacks include phishing through mobile applications, SMS, and fraudulent websites aimed at extracting personal and financial information. Online fraud cases, such as non-delivery of goods, illicit loan applications, Ponzi schemes, and investment scams, are increasingly prevalent, affecting both individuals and institutions (Walderich, 2023).

Institutional cybersecurity vulnerabilities have also escalated. In 2023, the Thailand Computer Emergency Response Team (ThaiCERT) addressed over 1,000 website hacking incidents, while ransomware attacks, though less frequent, posed substantial threats (Walderich, 2024b).

According to the National Cyber Security Agency (NCSA), a total of 295 cyber incidents targeted public and private organizations, with educational institutions accounting for the highest number of attacks, followed by other government agencies (Walderich, 2024a). These patterns highlight critical weaknesses within key sectors and underscore the urgent need for a coordinated and adaptive national cybersecurity strategy.

Within the business sector, cybersecurity preparedness remains uneven. Although some firms are investing in cybersecurity solutions, many continue to suffer from limited awareness, inadequate infrastructure, and a shortage of skilled cybersecurity professionals (Thamrongthanakit, 2023). Compared to regional peers such as Singapore and Malaysia, Thailand's cybersecurity market remains underdeveloped (Tran, 2024). Initiatives by the Digital Economy Promotion Agency (DEPA), including partnerships to enhance digital skills in cybersecurity, cloud computing, and data science, represent important steps toward addressing these gaps (Walderich, 2023).

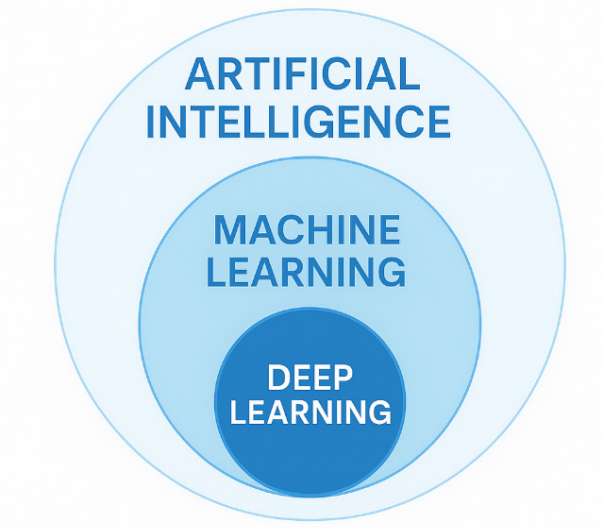
Despite governmental and private sector efforts, the evolving nature of cyber threats demands a more proactive, adaptive, and collaborative approach to cybersecurity management in Thailand. Building national resilience will require not only technological innovation but also legal reforms, education initiatives, and sustained cross-sectoral cooperation.

3. AI-Driven Cybersecurity Trends

The increasing sophistication of cyber threats—particularly Advanced Persistent Threats (APTs) and zero-day vulnerabilities—has revealed the limitations of traditional signature-based detection. APTs refer to prolonged, targeted attacks where an intruder gains unauthorized access to a system, often with the intent of stealing sensitive information or compromising system integrity over time. Zero-day vulnerabilities, on the other hand, are security flaws in software or hardware that are exploited by attackers before the vendor or developer has had a chance to address them with a patch. In response to these complex threats, cybersecurity strategies are increasingly integrating AI, ML, and DL technologies to enhance threat detection and improve response capabilities (Durgaraju et al., 2025, p.117-123). Figure 1 illustrates the nested relationship among these technologies—DL is a subset of ML, which in turn is a subset of AI. This hierarchy reflects the increasing complexity and specificity of each technique used in cybersecurity solutions.

Figure 1

Hierarchical relationship among AI, ML, and DL



Note: Adapted From Artificial Intelligence (AI), Machine Learning (ML) & Deep Learning (DL): A Comprehensive Overview on Techniques, Applications and Research Directions, by S. M. Mian, M. S. Khan, M. Shawez, and A. Kaur, In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (p.1404-1409), 2024, IEEE.

While countries such as Singapore and EU have introduced AI governance frameworks tied to cybersecurity—such as Singapore's Model AI Governance Framework and EU's Ethical Guidelines for Trustworthy AI (Personal Data Protection Commission [PDPC], 2020; Hickman & Petrin, 2021, p.593-625)—Thailand's regulatory landscape remains in its formative stages. These disparities underscore the need for ethical adaptation rather than wholesale adoption, particularly in a context where AI systems may be deployed without adequate transparency or bias mitigation mechanisms (Akinrinola et al., 2024, p.050-058).

3.1 AI Integration with Security Frameworks

AI is transforming traditional tools like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) by enabling real-time log analysis, anomaly detection, and automated responses (Muhammad et al., 2023, p.1406-1405). Automation reduces repetitive tasks, freeing analysts to focus on proactive threat hunting and strategic planning (Ramalingam et al., 2025, p.75-94).

3.2 Machine Learning for Threat Detection

ML improves cyber defense through both supervised and unsupervised learning. Supervised models classify threats using labeled data, while unsupervised techniques detect anomalies and zero-day attacks in unlabeled datasets. Clustering algorithms expose subtle deviations in network traffic (Paul, 2024). Reinforcement Learning (RL), especially when combined with DL, enhances real-time, adaptive decision-making in dynamic and adversarial environments (Nguyen & Reddi, 2021, p.3779-3795).

3.3 Deep Learning Applications in Cybersecurity

DL architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Generative Adversarial Networks (GANs) strengthen threat detection. CNNs identify malware via binary code analysis; RNNs and LSTMs interpret sequential data like system logs; GANs simulate attack scenarios to enrich training datasets and improve detection accuracy against adversarial threats (Sarker, 2021, p.154).

3.4 Real-Time Defense and Strategic Value

AI enables real-time behavioral analysis, endpoint monitoring, and threat intelligence. It detects anomalies like abnormal logins or lateral movements, supporting systems like Endpoint Detection and Response (EDR) (Aminu et al., 2024, p.11-27). Beyond detection, AI-driven models continuously evolve, prioritize vulnerabilities, automate patching, and support proactive risk mitigation. Ultimately, AI has become a strategic enabler of cyber resilience and operational continuity (Saad & Aslam, 2023).

3.5 Limitations and Technical Constraints of AI in Cybersecurity

Despite the growing integration of AI in cybersecurity, several technical limitations remain critical to its operational reliability and trustworthiness. Three key challenges are explainability, model drift, and ethical bias.

Explainability is a significant constraint, especially in complex AI models like deep neural networks, which function as *"black boxes"* with limited transparency. This lack of interpretability impedes human understanding of how specific decisions are made, reducing trust and complicating incident response (Zhang et al., 2022, p.93104-93139; Capuano et al., 2022, p.93575-93600). Although explainable AI (XAI) methods have been proposed, they often involve trade-offs between accuracy and interpretability and are still limited in real-time cybersecurity contexts (Hosain et al., 2024).

Model drift is another technical hurdle. AI models trained on static datasets are prone to degradation over time as data distributions evolve—particularly in dynamic threat landscapes. Without effective detection mechanisms, drift can lead to reduced model accuracy and increased false positives or negatives (Lee et al., 2023; Patchipala, 2023, p.1198-1209). Addressing this requires continuous monitoring and adaptive retraining, which remains resource-intensive.

Ethical bias arises when training data reflect social or systemic biases, which are then perpetuated in automated decisions. In cybersecurity, this can lead to disproportionate threat profiling or access control errors (González et al., 2024, p.38-54; Kaushik et al., 2024, p.437-470). Mitigating such bias requires rigorous data curation and ethical auditing, which are not yet standard practice in most AI development pipelines.

These technical constraints highlight the need for not only robust AI design but also ongoing oversight and interdisciplinary collaboration to ensure secure and equitable deployment.

4. Challenges of Cybersecurity

The rapid advancement of digital technologies—including cloud computing, AI integration, and the proliferation of IoT—has introduced complex, rapidly evolving cybersecurity threats across all sectors (Sarker, 2024; Salama & Al-Turjman, 2025, p.86-95). Concurrently, attackers are employing more sophisticated techniques such as APTs, zero-day exploits, and multi-vector attacks that evade conventional defenses (Durgaraju et al., 2025, p.117-123). While these innovations enhance efficiency, they also dramatically expand the attack surface and outpace traditional safeguards. Addressing modern cyber risks demands proactive, multi-layered strategies that incorporate not just technical solutions but also regulatory adaptation and human-centric awareness (Akhtar & Rawol, 2024, p.50-67). This section outlines four critical areas of concern: advanced attack strategies, vulnerabilities in IoT ecosystems, AI-driven threats, and cloud-specific security challenges.

4.1 Advanced Cyberattack Strategies

Modern cyberattacks increasingly rely on APTs-long-term, targeted intrusions often orchestrated by state actors-designed to infiltrate high-value systems while avoiding detection. Zero-day vulnerabilities, which exploit unknown security flaws before a patch is available, are often used in combination with polymorphic malware and multi-vector tactics to bypass traditional defenses (Durgaraju et al., 2025, p.117-123).

Recent activity from APTs shows that many of these attacks are driven by geopolitical and financial motives. For example, some APT groups have targeted countries involved in China's *"One Belt, One Road"* initiative or areas with rising tensions, such as the Korean Peninsula. This suggests that cyberattacks are increasingly influenced by real-world political conflicts. At the same time, financially motivated APT actors-such as DeathStalker and North Korean state-backed groups like Lazarus and BlueNoroff-have launched ransomware attacks and other financially driven campaigns aimed at critical infrastructure and financial institutions. In recent years, Southeast Asia has become a major hotspot for these operations, alongside the Middle East and regions targeted by Chinese-speaking APT groups (Burita & Le, 2021, p.1-7).

These evolving trends underscore the urgent need for AI-enhanced anomaly detection and predictive analytics, supported by real-time behavioral monitoring and continuous patch management.

4.2 Vulnerabilities in IoT Ecosystems

The rapid growth of IoT has significantly expanded the digital attack surface. Many devices still lack essential protections such as strong authentication, encryption, and timely firmware updates, leaving them highly vulnerable. Common threats include spoofing, DoS attacks, and data breaches, often enabled by unsecured protocols and weak access controls (Shafiq et al., 2022). For example, attackers have exploited vulnerabilities in voice assistants like Google Assistant and Amazon Echo to eavesdrop on conversations and steal user credentials through phishing-based app manipulation. Similarly, baby monitoring cameras have been remotely accessed due to default passwords and unencrypted video streams, compromising both privacy and physical safety.

On a larger scale, botnets such as Mirai have infected hundreds of thousands of unsecured IoT devices to launch massive DDoS attacks, crippling enterprise networks and critical infrastructure. These cases reveal that consumer IoT vulnerabilities are not limited to personal privacy breaches, but can also be leveraged for broader infrastructure-level cyberattacks (Xenofontos et al., 2021, p.199-221).

These evolving threats highlight the growing necessity of AI-driven security frameworks for IoT systems, including real-time anomaly detection, behavior-based threat modeling, and adaptive response mechanisms-to mitigate risks stemming from large-scale device compromise and privacy intrusion.

4.3 Artificial Intelligence–Driven Threats

AI presents dual-use challenges: while it enhances threat detection and response, attackers also leverage AI to automate and adapt cyberattacks. Techniques like AI-generated deepfakes compromise biometric authentication, while AI-enhanced botnets can execute large-scale intrusions. Defending against these requires ethical, adaptive, and resilient AI systems (Sarker, 2024).

These AI-driven cyber threats are not only sophisticated but also carry severe real-world consequences. For instance, deepfake technologies —particularly those based on GANs—can fabricate hyper-realistic videos and audio clips that mimic individuals with uncanny accuracy. Such synthetic media have been weaponized for identity theft, political misinformation, extortion, and even character assassination. One infamous case involved a fabricated video of a political leader that incited widespread public unrest, illustrating how AI-generated content can destabilize trust in digital communications and pose national security risks. Moreover, deepfake pornography and voice spoofing have led to psychological trauma and reputational damage for individuals, especially public figures and vulnerable groups (Patel et al., 2023, p.143296-143323). These incidents highlight the growing severity and sophistication of AI-enabled cyberattacks and emphasize the urgent need for robust detection frameworks and legal countermeasures.

4.4 Challenges in Cloud Security

Cloud platforms offer scalability and efficiency but also raise concerns around data breaches, insecure APIs, and misconfigurations. Reliance on third-party providers expands the attack surface and reduces control. Key mitigations include RBAC, continuous monitoring, AI-driven detection tools, and strong cloud governance policies (Salama & Al-Turjman, 2025, p.86-95). However, the consequences of these vulnerabilities can be severe. Cloud-based cyberattacks—especially those targeting mobile and distributed cloud architectures—have already led to large-scale data breaches, service disruptions, and the compromise of critical infrastructure. For instance, peer-to-peer (P2P) and mobile cloud systems, while offering cost-efficient scalability, can expose sensitive user data to unauthorized access due to decentralized control and weak enforcement of access policies (Lo'ai & Saldamli, 2021, p.810-819).

One particularly alarming trend involves ransomware attacks that exploit cloud storage vulnerabilities and spread laterally across multi-tenant environments. Moreover, advanced side-channel exploits such as Spectre and

Meltdown have demonstrated the possibility of extracting sensitive information from shared cloud hardware. These threats are exacerbated by the growing reliance on cloud-based analytics services, where unencrypted or poorly partitioned datasets can lead to inadvertent data leakage or malicious inference attacks. According to Lo'ai and Saldamli (2021, p.810-814), even widely used services such as Big Data as a Service (BDaaS) and cloud-based AI analytics must now incorporate sophisticated protections—such as homomorphic encryption, secure multi-party computation, and format-preserving encryption—to mitigate these increasingly complex threats. Without such protections, cloud environments remain highly attractive targets for adversaries seeking to exploit systemic weaknesses on a massive scale.

5. Sector-Specific Challenges in Thailand

Thailand's cybersecurity landscape varies widely across sectors, reflecting differences in scale, digital maturity, regulatory exposure, and systemic importance. This section analyzes three critical sectors-SMEs, mobile banking, and port infrastructure -selected for their economic significance, heightened cyber risk exposure, and potential spillover effects on national stability. Each sector illustrates unique vulnerabilities while also offering insights into shared systemic challenges that policy must address holistically.

While each sector faces distinct challenges, these vulnerabilities are often interconnected. For instance, a cyberattack on maritime port infrastructure could disrupt digital supply chains, directly impacting SMEs reliant on import–export flows. Similarly, security breaches in mobile banking systems can erode consumer trust in digital payments, indirectly harming SMEs that depend on online transactions. Conversely, poor data governance among SMEs could lead to user data exposure, which attackers may exploit for fraud in banking systems. These interdependencies underscore the need for integrated cybersecurity strategies that transcend sectoral silos.

5.1 Cybersecurity Gaps in SMEs

SMEs constitute a major pillar of economic development globally, with particular significance in developing economies such as Thailand, where they account for more than one-third of the country's GDP (Thamrongthanakit, 2023). Despite this economic weight, SMEs remain disproportionately underprepared for cyber threats. A 2024 report revealed that nearly 25% of Thai SMEs have no cybersecurity tools and lack even basic digital protection policies (Komsan Tortermvasana, 2024). Common barriers include limited budgets, unclear return on investment (ROI), and lack of in-house expertise (Prasopdee & Srisa-An, 2024, p.40-44).

While threats like ransomware (30%), malware (20%), and web attacks (15%) are prevalent (Jonathan & Thamrongthanakit, 2024), most SMEs rely on basic antivirus programs and have no incident response plans. Crucially, many employees lack cybersecurity training, and few SMEs participate in national threat intelligence networks.

To address this gap, cybersecurity must be framed as a strategic enabler rather than a technical afterthought. Government policies should

support AI-powered solutions tailored to SME constraints—such as low-cost behavior-based detection tools and centralized threat analytics hubs. Financial incentives like tax credits and public-private digital literacy campaigns will be critical to bridge the awareness and capability divide.

5.2 Mobile Banking and Financial Technology Risks

Thailand's shift toward a cashless society -driven by mobile banking and digital platforms-offers expanded financial access but also increases cybersecurity and digital inclusion risks. Individuals with limited digital literacy or access face exclusion, underscoring the need for targeted digital education and alternative access strategies (Thetlek et al., 2024, p.264-272). To ensure fairness and consumer protection, robust regulatory frameworks must support both traditional and virtual banking ecosystems.

As mobile banking grows, enhancing user cybersecurity awareness is crucial. Educating users on secure practices—like avoiding credential sharing and using verified apps—can reduce malware and fraud risks. Financial institutions must align cybersecurity strategies with evolving threats and user behavior to build trust and promote safe financial engagement (Limna et al., 2023, p.1133-1151).

AI integration is key to addressing these challenges. Real-time threat detection, behavioral analytics, and adaptive risk assessment powered by AI can significantly enhance fraud prevention. Regulators like the Bank of Thailand should ensure ethical AI use, data privacy, and compliance with global standards. Public-private partnerships must expand access to threat intelligence, digital literacy, and protection for vulnerable users. Embedding AI in mobile banking, alongside user-centered awareness efforts, will be essential to securing and democratizing Thailand's digital financial landscape.

5.3 Vulnerabilities in Maritime Port Infrastructure

As a major maritime nation, Thailand relies heavily on port operations for economic growth and global trade (NESDC, 2024). With global ports embracing digitalization, Thailand must adopt smart technologies to stay competitive. This digital shift, however, brings increased cybersecurity risks. Regulatory updates and financial incentives—such as subsidies and tax breaks—are needed to support secure digital adoption (Janmethakulwat & Thanasopon, 2024, p.157-166).

Digitized port systems, while efficient, are vulnerable to cyber threats from hacktivists, cybercriminals, and state-sponsored actors. Common risks stem from outdated infrastructure, weak protocols, and low employee awareness. To address these, ports must implement strong access controls, regular staff training, and comply with international standards like the ISPS Code (Senarak, 2021, p.20-36).

A national, coordinated response is essential. Government leadership should promote aligned regulations, public-private partnerships, and international cooperation. Integrating AI-driven cybersecurity tools—such as real-time monitoring, anomaly detection, and predictive threat modeling—can significantly enhance resilience. Embedding AI into port systems will strengthen Thailand's digital security and solidify its role in global maritime logistics.

Table 1

Cross-Sector Comparison of Cybersecurity Risks, Systemic Issues, AI Applications, and Policy Recommendations in Thailand

Sector	Key Risks	Systemic Issues	AI Applications	Policy Recommendations
SMEs	Ransomware, malware, web attacks	Limited budget, low awareness, lack of in-house expertise	Lightweight ML-based behavior detection, centralized threat intelligence	Tax credits, subsidized SME-tailored AI tools, public-private literacy campaigns
Mobile Banking	Phishing, fraud, credential theft	Digital inclusion gap, low user cybersecurity literacy	Deep learning for real-time fraud detection, behavioral risk scoring	National user education, AI ethics oversight, secure access design for vulnerable users
Port Infrastructure	System intrusion, data disruption, state-sponsored threats	Legacy digital systems, weak access protocols, low staff awareness	AI-driven anomaly detection, real-time monitoring, predictive threat modeling	ISPS Code compliance, AI R&D subsidies, mandatory staff cyber training

To better contextualize the cybersecurity posture and governance needs across Thailand's key sectors, Table 1 presents a comparative overview of key cyber risks, systemic vulnerabilities, AI-based mitigation strategies, and policy recommendations for SMEs, mobile banking, and port infrastructure. This mapping enables more coherent, targeted, and AI-informed cybersecurity policymaking.

6. Policy Recommendations for Cybersecurity in Thailand

Thailand's cybersecurity landscape demands a coordinated and future-facing policy framework that addresses diverse sectoral needs while promoting technological innovation. Drawing from the sector-specific vulnerabilities analyzed in Section 5—namely, those of SMEs, mobile banking, and port infrastructure—this section outlines integrated policy recommendations across four dimensions: national, organizational, societal, and international. These recommendations aim not only to mitigate present-day risks but also to foster long-term resilience through the strategic use of AI, ML, and DL technologies.

6.1 National-Level: Legal Reform and Strategic Investment

National cybersecurity policy must begin with the refinement of the Cybersecurity Act to ensure a balance between national security enforcement and civil liberties. Greater judicial oversight, clearer definitions of enforcement authority, and enhanced transparency mechanisms will build public trust and promote lawful use of digital surveillance powers.

To support technological advancement, a national innovation fund should be established to catalyze the development of AI-based cybersecurity tools. For example, ML algorithms can be developed to detect anomalies in SME systems, while DL architectures can model complex attack vectors in critical infrastructure such as port logistics. Such a fund should prioritize tools that are open-access, scalable, and tailored to Thai economic contexts, particularly low-cost solutions for SMEs and intelligent monitoring for port systems.

Moreover, Thailand should create a centralized national incident response center that integrates AI-powered threat intelligence and provides real-time alerts across sectors. This is especially critical for mobile banking and port infrastructure, where early detection can prevent cascading impacts across financial and trade networks. These reforms provide the institutional foundation necessary for coordinated, cross-sector cybersecurity readiness.

6.2 Organizational-Level: Adoption Incentives and Workforce Development

Organizational readiness is often hindered by resource constraints, particularly in SMEs and state-operated logistics hubs. The government should offer tax incentives and procurement advantages for organizations that adopt certified cybersecurity platforms integrating ML and DL capabilities. For SMEs, supervised ML can provide low-maintenance fraud detection, while ports may benefit from unsupervised learning systems that recognize unusual equipment behaviors.

Mobile banking institutions should undergo mandatory AI-readiness audits and adopt DL-based risk scoring mechanisms to enhance fraud prevention. Additionally, tailored training programs should be launched to upskill different workforce segments: SME operators, cybersecurity auditors, banking fraud analysts, and port IT personnel. These programs must include both foundational and advanced modules on AI-driven cybersecurity to bridge Thailand's persistent skills gap.

6.3 Societal-Level: Public Literacy and Digital Hygiene

Cybersecurity must be democratized through inclusive awareness initiatives that empower citizens with practical knowledge. National campaigns should target digitally vulnerable groups—including seniors, rural populations, and low-income earners—with accessible content on safe mobile banking practices, phishing avoidance, and data privacy.

To promote sustainable resilience, cybersecurity literacy and ethical AI education should be integrated into school and university curricula. This initiative is particularly relevant for communities adopting mobile finance and IoT-based services, where human error remains a primary vector for cyber threats. By normalizing concepts such as AI-generated fraud and behavioral biometrics, the public can become an active line of defense against evolving threats.

Private sector actors, especially in fintech and telecommunications, should collaborate with government agencies to disseminate behavioral AI literacy—helping end users understand how ML-based systems monitor anomalies and protect their accounts. These joint efforts reinforce trust in digital systems while extending protection beyond institutional boundaries.

6.4 Regional and International Level: Strategic Alignment and AI Diplomacy

Given the transnational nature of cyber threats, Thailand must strengthen its cooperation with ASEAN neighbors and global partners. Harmonization with the ASEAN Digital Economy Framework Agreement will enhance regulatory consistency and facilitate cross-border threat response—particularly vital for logistics hubs and digital finance platforms.

Thailand should also take a leading role in AI diplomacy, advocating for global norms in ethical AI deployment within cybersecurity. This includes support for explainable AI, robust data governance, and human rights–based AI policies. As AI becomes embedded in digital infrastructure, Thailand's position as a regional logistics and fintech hub requires the country to lead, not just follow, in shaping responsible AI applications.

Cross-border participation in cyber drills, AI model-sharing for anomaly detection, and regulatory sandboxes for fintech security innovation will not only strengthen Thailand's domestic defenses but also elevate its status as a trusted digital trade partner in the Asia-Pacific region.

Despite the promise of AI, its integration into national cybersecurity systems also raises ethical concerns—particularly in contexts like Thailand, where data governance and regulatory maturity remain limited. Issues such as algorithmic bias, lack of transparency, and the risk of surveillance overreach must be critically addressed. Countries like Singapore and the European Union have adopted AI governance frameworks that emphasize explainability, accountability, and rights-based protections (PDPC, 2020; Hickman & Petrin, 2021, p.593-625). Thailand should consider adapting similar principles to ensure that AI deployment in cybersecurity aligns with democratic values and public trust.

Table 2

Multi-Level Policy Integration Framework for Cybersecurity in Thailand

Policy Level	Recommended Policies	Target Groups	Relevant Sectors	Key Technologies
National	• Introduce judicial oversight and transparency into the Cybersecurity Act • Establish a national AI fund for open-access cybersecurity innovation • Develop a centralized AI-driven national incident response center	Government agencies, regulators	All sectors	AI, ML, DL, National SIEM

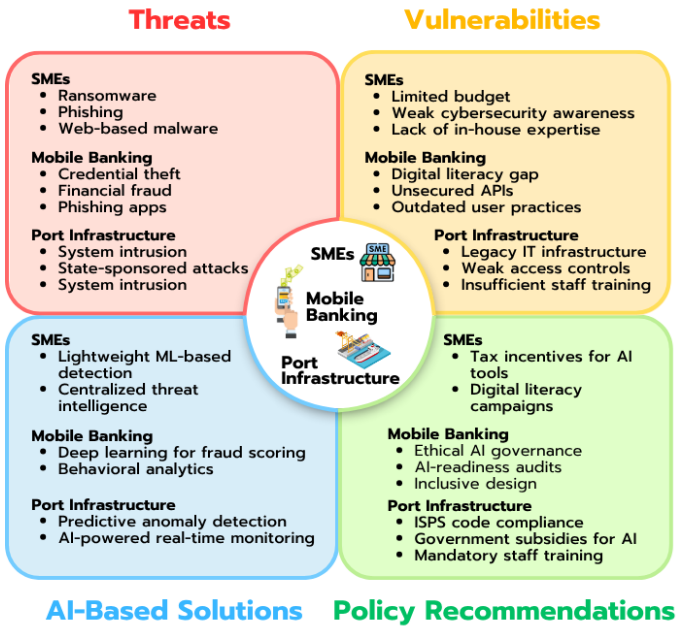
Organizational	• Incentivize certified AI platforms via tax and procurement benefits • Require AI-readiness audits for banks • Provide specialized AI cybersecurity training	SMEs, banks, port operators, cybersecurity staff	SMEs, Banking, Logistics/Ports	ML (supervised & unsupervised), DL, IDS/EDR
Societal	• Launch public campaigns on digital hygiene and phishing prevention • Integrate AI ethics and cybersecurity into curricula • Promote behavioral AI literacy via public-private partnerships	General public, students, vulnerable populations	Mobile banking, IoT-based services	AI literacy, Behavioral biometrics
International	• Align with ASEAN Digital Economy Framework • Lead in AI diplomacy and ethical AI standards • Participate in cross-border cyber drills and sandboxes	Regulators, digital trade partners	Ports, Fintech, Cross-border systems	Explainable AI, Shared anomaly detection models

Table 2 outlines a multi-level policy framework integrating national, organizational, societal, and international strategies. This structure fosters coherent, synchronized actions across institutions and stakeholder groups, and is vital for building sustainable, AI-enabled cyber resilience in an increasingly complex threat landscape.

To synthesize the interrelated cyber risks, sector-specific vulnerabilities, AI applications, and multi-tiered policy implications, Figure 2 presents a conceptual map of Thailand's cybersecurity landscape. This visual framework illustrates how SMEs, mobile banking, and port infrastructure—three critical digital sectors—are centrally situated and dynamically interconnected with four systemic dimensions: threats, vulnerabilities, AI-based solutions, and policy interventions.

Figure 2

Cybersecurity Landscape Map of Thailand's Key Sectors and Systemic Dimensions



7. Conclusion

This article has examined Thailand's evolving cybersecurity landscape across three critical sectors—SMEs, mobile banking, and port infrastructure—and identified systemic vulnerabilities, ranging from limited AI adoption and fragmented governance to disparities in digital literacy. It also analyzed the potential of AI, ML, and DL to enhance national cyber resilience, while acknowledging structural and implementation constraints. The policy recommendations in Section 6 can be operationalized through a tiered approach to support strategic planning and policy execution:

- **Immediate Priorities:** These include refining the National Cybersecurity Act, establishing a centralized incident response center, and launching public awareness campaigns targeting SMEs and mobile banking users. These interventions address governance deficiencies and end-user vulnerabilities identified in Section 5.
- **Long-Term Collaborations:** These encompass the development of an AI-literate cybersecurity workforce, integration of cybersecurity education into national curricula, and participation in cross-border cybersecurity frameworks such as ASEAN's digital initiatives. These measures are critical for securing port infrastructure and scaling AI deployment ethically and sustainably.
- **Stakeholder-Sensitive Measures:** This category includes incentive programs for SMEs, ethical AI audits for financial institutions, and inclusive digital literacy initiatives. These strategies must account for sectoral disparities in technological

readiness and ensure equitable access across all groups.

By organizing the roadmap in this manner, the article emphasizes that effective cybersecurity governance demands synchronized efforts across technical, regulatory, educational, and international domains. This multi-dimensional perspective, supported by cross-referenced findings in Sections 3 to 6, constitutes a core academic contribution.

8. Future Research Directions

Further studies can extend this framework in several directions. First, researchers may develop empirical metrics to assess the effectiveness of AI-driven cybersecurity interventions across different sectors. Second, behavioral studies could investigate how SMEs, financial institutions, and port authorities perceive and adapt to AI-enabled security solutions. Third, cross-disciplinary analyses may explore the ethical, legal, and social implications of algorithmic surveillance, especially in regulatory-light environments. Finally, longitudinal studies can track the impact of AI-based reforms on resilience outcomes and sectoral innovation.

In conclusion, Thailand's cybersecurity future hinges on strategic investments in AI capacity, human capital, inclusive governance, and ethical innovation. The findings presented here offer a coherent roadmap to navigate these complexities and position Thailand as a regional leader in AI-driven cybersecurity resilience.

References

Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT Journal Research and Development, 9*(1), 50-67.

Akinrinola, O., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability. *GSC Advanced Research and Reviews, 18*(3), 050-058.

Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research, 13*(8), 11-27.

Basak, B. (2024). The Impact of Cybersecurity Threats on National Security: Strategies. *International Journal of Humanities Social Science and Management (IJHSSM), 4*(2), 1361-1382.

Bellamkonda, S. (2020). Cybersecurity in critical infrastructure: Protecting the foundations of modern society. *International Journal of Communication Networks and Information Security, 12,* 273-280.

Burita, L., & Le, D. T. (2021). Cyber security and APT groups. In *2021 Communication and Information Technologies (KIT)* (pp. 1-7). IEEE.

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access, 10,* 93575-93600.

Durgaraju, S., Vel, D. V. T., & Madathala, H. (2025). The evolution of cyber threats and defenses: A review of innovations and challenges. In *Proceedings of the 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 117–123). IEEE.

Firmansyah, B. (2024). Cybersecurity Fundamentals. In *Challenges in Large Language Model Development and AI Ethics* (pp. 280-320). IGI Global.

González, A. L., Moreno, M., Román, A. C. M., Fernández, Y. H., & Pérez, N. C. (2024). Ethics in artificial intelligence: An approach to cybersecurity. *Inteligencia Artificial, 27*(73), 38-54.

Hickman, E., & Petrin, M. (2021). Trustworthy AI and corporate governance: the EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective. *European Business Organization Law Review, 22,* 593-625.

Hosain, M. T., Jim, J. R., Mridha, M. F., & Kabir, M. M. (2024). Explainable AI approaches in deep learning: Advancements, applications and challenges. *Computers and electrical engineering, 117,* Articel 109246.

Janmethakulwat, A., & Thanasopon, B. (2024). Digital technology adoption and institutionalization in Thai maritime industry: An exploratory study of the Thai shipowners. *The Asian Journal of Shipping and Logistics, 40*(3), 157-166.

Jonathan, G., & Thamrongthanakit, T. (2024). Cybersecurity Management Practices in Thai SMEs. In *MWAIS 2024 Proceedings.* AIS Electronic Library (AISeL).

Kaushik, K., Khan, A., Kumari, A., Sharma, I., & Dubey, R. (2024). Ethical considerations in AI-based cybersecurity. In *Next-generation cybersecurity: AI, ML, and Blockchain* (pp. 437-470). Singapore: Springer Nature Singapore.

Komsan Tortermvasana. (2024, December 17). Project aims to fortify firms' cyber defence. *Bangkok Post.* https://www.bangkokpost.com/business/general/2921177/project-aims-to-fortify-firms-cyber-defence

Kumar, V. A., Bhardwaj, S., & Lather, M. (2024). Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms. *Productivity, 65*(1), 1-10.

Lee, Y., Lee, Y., Lee, E., & Lee, T. (2023). Explainable Artificial Intelligence-Based Model Drift Detection Applicable to Unsupervised Environments. *Computers, Materials & Continua, 76*(2).

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The relationship between cyber security knowledge, awareness and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research, 7,* 1133-1151.

Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University-Computer and Information Sciences, 33*(7), 810-819.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News, 190*(1), 1-69.

Mian, S. M., Khan, M. S., Shawez, M., & Kaur, A. (2024). Artificial Intelligence (AI), Machine Learning (ML) & Deep Learning (DL): A Comprehensive Overview on Techniques, Applications and Research Directions. In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (pp. 1404-1409). IEEE.

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). Integrated security information and event management (siem) with intrusion detection system (ids) for live analysis based on machine learning. *Procedia Computer Science, 217,* 1406-1415.

Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems, 34*(8), 3779-3795.

Office of National Economic and Social Development Council. (2024). *Thailand's Logistics Report 2023.*

Patchipala, S. (2023). Tackling data and model drift in AI: Strategies for maintaining accuracy during ML model inference. *International Journal of Science and Research Archive, 10*(2), 1198-1209.

Patel, Y., Tanwar, S., Gupta, R., Bhattacharya, P., Davidson, I. E., Nyameko, R., Srinivas, A., & Vimal, V. (2023). Deepfake generation and detection: Case study and challenges. *IEEE Access, 11,* 143296-143323.

Paul, J. (2024). *Comparative Analysis of Supervised vs. Unsupervised Learning in API Threat Detection*.

Personal Data Protection Commission. (2020). *Singapore's Model AI Governance Framework.*

Prasopdee, N., & Srisa-An, C. (2024). Strategies for Cyber Risk Assessment and Mitigation in Small and Medium-Sized Enterprises in Thailand. In *2024 8th International Conference on Information Technology (InCIT)* (pp. 40-44). IEEE.

Ramalingam, R., Arthi, K., Bhavani, M. M., & Sunitha, T. (2025). AI-Enhanced Security Information and Event Management (SIEM) System. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 75-94). IGI Global Scientific Publishing.

Saad, W., & Aslam, M. (2023). *The Role of Artificial Intelligence in Remediation and Risk Mitigation for Cybersecurity.*

Salama, R., & Al-Turjman, F. (2025). Addressing Cybersecurity Vulnerabilities with Cloud Security. *NEU Journal for Artificial Intelligence and Internet of Things, 4*(1), 86-95.

Salman, H. A., & Alsajri, A. (2023). The Evolution of Cybersecurity Threats and Strategies for Effective Protection. *SHIFRA,* 2023, 73-85.

Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science, 2*(3), 154.

Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence. In *cyber automation, intelligent decision-making and explainability.* Springer Cham.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics, 37*(1), 20-36.

Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., & Hamam, H. (2022). The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks. *Wireless Communications and Mobile Computing, 2022*(1), Articel 8669348.

Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal, 19*(4), 5-24.

Thamrongthanakit, T. (2023). *Impacts of cybersecurity practices on cyberattack damage and protection among small and medium enterprises in Thailand* [Master's thesis, Stockholm University]. https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-219680

Thetlek, R., Kraiwanit, T., Limna, P., Shaengchart, Y., & Moolngearn, P. (2024). The strategy of virtual banking adoption in the digital economy [Special issue]. *Corporate & Business Strategy Review, 5*(1), 264-272.

Tran, K.. (2024, September 18). *Largest cybersecurity markets in the Asia-Pacific region in 2022, by revenue.* Statista. https://www.statista.com/forecasts/1400787/apac-largest-cybersecurity-markets-by-revenue

Walderich, A. (2023, December 20). *Cybersecurity and cybercrime in Thailand – Statistics & facts*. Statista. https://www.statista.com/topics/11439/cybersecurity-and-cybercrime-in-thailand/

Walderich, A. (2024a, October 4). *Number of cyber threats against public and private entities in Thailand 2023, by type of organization.* Statista. https://www.statista.com/statistics/1202802/thailand-number-of-cyber-threats-by-type-of-organization/

Walderich, A. (2024b, October 14). *Number of cyber threats detected and settled by ThaiCERT in Thailand in 2023, by type of threat.* Statista. https://www.statista.com/statistics/1154735/thailand-number-of-cyber-threats-by-type-of-threat/

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet of Things Journal, 9*(1), 199-221.

Yeasmin, F. (2024). The impact of digital transformation on society: unraveling trends, challenges, and opportunities. *Eunomia–Rozwój Zrównoważony–Sustainable Development, 2*(108), 53-67.

Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access, 10,* 93104-93139.