A Cybersecurity Governance Maturity Framework for Mitigating Cross-Domain Attacks in 5G Private Networks

Hung-Cheng Yang, I-Long Lin, Yueh Lin, Chorng-Ming Chen*

Department of Computer Science and Information Engineering, Tatung University, Taiwan
yangyeh5046@gmail.com, cyberpaul@gm.ttu.edu.tw, yuehlin@gmail.com, avenchentw@gmail.com

Abstract

With the increasing deployment of 5G private networks in smart manufacturing, transportation, and IoT environments, the high performance of these networks has also introduced new cybersecurity challenges. The convergence of Information Technology (IT), Operational Technology (OT), and Communication Technology (CT) significantly expands the attack surface and exposes systems to cross-domain threats such as rogue base station infiltration, distributed denial-of-service (DDoS) attacks, and lateral movement. These attacks threaten data integrity, service continuity, and user privacy. To address these issues, this study applies the MITRE FiGHT threat model to depict representative attack stages—including reconnaissance, intrusion, lateral propagation, and service disruption—and integrates CVSS 3.1 scoring with corresponding mitigation strategies. Based on these components, we construct an analytical workflow capable of quantifying risks, identifying governance deficiencies, and guiding targeted improvements. A prototype Cybersecurity Governance Maturity Model (CSGMM) tailored for 5G private networks is subsequently proposed.

The proposed framework incorporates six governance domains—policy, asset management, risk defense, incident response, control practices, and supply chain management—and formalizes a three-tier structure covering strategic, tactical, and operational layers. It also defines twenty-five practice objectives aligned with international standards such as ISO/IEC 27002 and NIST CSF 2.0, improving both applicability and interoperability.

Experimental validation was conducted using a Free5GC and UERANSIM testbed to simulate practical attack scenarios, including traffic-based DDoS and endpoint-level exploitation. The results show that the implementation of the governance framework, together with FiGHT-based mitigation strategies, leads to a measurable reduction in CVSS risk scores and attack success probability. These findings demonstrate that integrating governance mechanisms with technical defense measures enhances incident response, strengthens network resilience, and supports continuous security management throughout the lifecycle of 5G private network deployment.

The proposed model provides a structured reference for both industry and government seeking to advance 5G cybersecurity strategies. It offers practical value for smart manufacturing and other mission-critical applications, supporting organizations in addressing increasingly complex cyber threats in the era of digital transformation.

Keywords: 5G private networks, Cybersecurity Governance Maturity Framework (CSGMM), Cross-domain attacks, Risk quantification

1 Introduction

The rapid proliferation of Fifth-Generation (5G) mobile communication technology has driven governments and industries worldwide to deploy private networks. These networks have emerged as essential technological foundations for high-performance applications in domains such as smart manufacturing, intelligent healthcare, and automated transportation [1]. By leveraging technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and network slicing, 5G private networks provide superior bandwidth, ultra-low latency, and massive connectivity compared with public networks. This architectural flexibility enables highly customized deployments, positioning 5G private networks as critical infrastructures for the emerging intelligent industry ecosystem [2].

However, the practical deployment of 5G private networks is accompanied by increasingly complex cybersecurity risks. The primary challenge arises from the deep integration of heterogeneous Information Technology (IT), Operational Technology (OT), and Communication Technology (CT) domains. While this convergence enhances data fluidity and intelligent automation, it simultaneously dissolves traditional security perimeters and exponentially increases system complexity, creating new vectors for lateral movement by malicious actors. As noted by Maleh (2021), the transition toward Industry 4.0 has exposed OT systems to severe cyber threats, wherein adversaries exploit unsegmented networks, default configurations, and remote access vulnerabilities to compromise critical control systems [3]. Such cross-domain attacks can result in data manipulation, service disruption, and loss of asset control, ultimately jeopardizing business continuity and user privacy. Moreover, as Yassine Maleh et al. (2021) emphasize, organizations lacking institutionalized governance frameworks often struggle to

*Corresponding Author: I-Long Lin; Email: cyberpaul@gm.ttu.edu.tw
DOI: https://doi.org/10.70003/160792642026032702009

promptly identify and respond to security incidents within such converged architectures [4].

Although existing cybersecurity standards provide fundamental guidelines for establishing information security management systems, they often lack the practical effectiveness and governance breadth required for highly virtualized and modular 5G environments. The 5G Alliance for Connected Industries and Automation (5G-ACIA) underscores in its white paper that cybersecurity governance for industrial 5G must be holistically addressed across strategic planning, technical implementation, and operational monitoring levels [2]. Consequently, reliance solely on conventional security tools or single-layer vulnerability assessments is insufficient to mitigate the systemic, dynamic, and cross-domain threats intrinsic to 5G private networks.

Within the domain of cybersecurity governance, Maleh et al. (2021) proposed the Cybersecurity Governance Maturity Model (CSGMM), which employs tiered governance structures and Control Practices and Objectives (CPOs) to assess the effectiveness of an organization's security management framework [4]. However, this model was designed for general enterprise contexts and does not explicitly address the distinctive risks associated with 5G private networks, particularly those arising from the intricate integration of IT, OT, and CT systems.

To bridge this research gap, this study proposes a prototype CSGMM specifically tailored for the 5G cross-domain environment. The proposed approach integrates the MITRE ATT&CK® framework to model threats relevant to 5G private networks, constructing plausible attack scenarios encompassing reconnaissance, initial access, lateral movement, and denial-of-service [5]. By mapping these threats to corresponding mitigation strategies and employing the Common Vulnerability Scoring System (CVSS) v3.1 for quantitative risk evaluation, the proposed framework establishes a comprehensive methodology for security assessment and governance. Ultimately, this work seeks to enhance the defensive posture of 5G private networks against cross-domain attacks and to advance organizational governance maturity and cyber resilience.

2 Literature Review

2.1 5G Private Network Architecture

The evolution of Fifth-Generation (5G) mobile communication technology has established private network architectures as fundamental enablers for enhanced performance and security. According to Kalhoro et al. (2024) [6], 3rd Generation Partnership Project (3GPP) standards [7], 5G systems are designed with inherent flexibility and scalability to accommodate diverse application requirements and market scenarios. As industries accelerate digital transformation, 5G private networks have become cornerstones of intelligent systems by offering high bandwidth, low latency, and massive connectivity. Unlike public mobile networks, a 5G private network is a dedicated and secure communication infrastructure provisioned for a specific enterprise or vertical. It is engineered to satisfy specialized requirements in production and security management while supporting emerging applications such as smart cities, the Internet of Things (IoT), and ultra-high-definition video delivery. These networks can attain peak data rates approaching 10 Gbps and commonly employ small-cell base stations and massive Multiple-Input Multiple-Output (MIMO) to increase connection density and reliability [6].

To satisfy stringent throughput and latency requirements while preserving cyber resilience, 5G private network design must strike a balance between performance optimization and security hardening. Ahmad et al. [8] decompose the 5G architecture into three principal domains: the core network, the access network, and the edge computing layer. Key enabling technologies include Software-Defined Networking (SDN), Network Function Virtualization (NFV), and cloud-native platforms. The Taiwan Association of Information and Communication Standards [9] further enumerates constituent elements of 5G private deployments, including core network components, access network elements (e.g., base stations), user equipment (UE), and management and orchestration systems.

The 5G Alliance for Connected Industries and Automation (5G-ACIA) classifies industrial 5G deployments into four deployment models according to the degree of integration with public networks. These models, summarized in Table 1, range from standalone non-public networks (NPNs) to fully integrated public-network-assisted NPNs. This typology highlights that 5G private networks can be configured to meet distinct security, privacy, and operational isolation requirements, with direct implications for data protection and process segregation.

Table 1. 5G NPN Deployment type (Source: Adapted from 5G-ACIA [2])

Deployment type	3GPP classification	Scope of resource sharing
Shared Radio Access Network NPN	Standalone Non-Public Network (SNPN)	Shares only the Radio Access Network (RAN)
Fully Isolated Non-Public Network (SNPN)	Standalone Non-Public Network (SNPN)	Completely isolated from the public network
Shared Radio and Control Plane NPN	Public Network Integrated NPN (PNI-NPN)	Shares both the Radio Access Network (RAN) and the Control Plane
Shared Radio, Control, and User Plane NPN	Public Network Integrated NPN (PNI-NPN)	Shares the Radio Access Network (RAN), Control Plane, and User Plane

2.2 Cybersecurity Threats in 5G Private Networks

While the advanced architecture of 5G enables unprecedented capabilities, it simultaneously introduces a broader and more complex threat landscape. The converged nature of 5G private networks—particularly the integration of Information Technology (IT), Operational Technology (OT), and Communication Technology (CT)—renders them attractive targets for sophisticated, cross-domain cyberattacks. Previous studies confirm that these threats can compromise data integrity, system availability, and user privacy, potentially leading to network-wide disruptions [5].

Kalhoro et al. [6] classified cybersecurity threats to 5G private networks by targeted domains, identifying vulnerabilities across user equipment, access networks, and core networks, as shown in Figure 1.

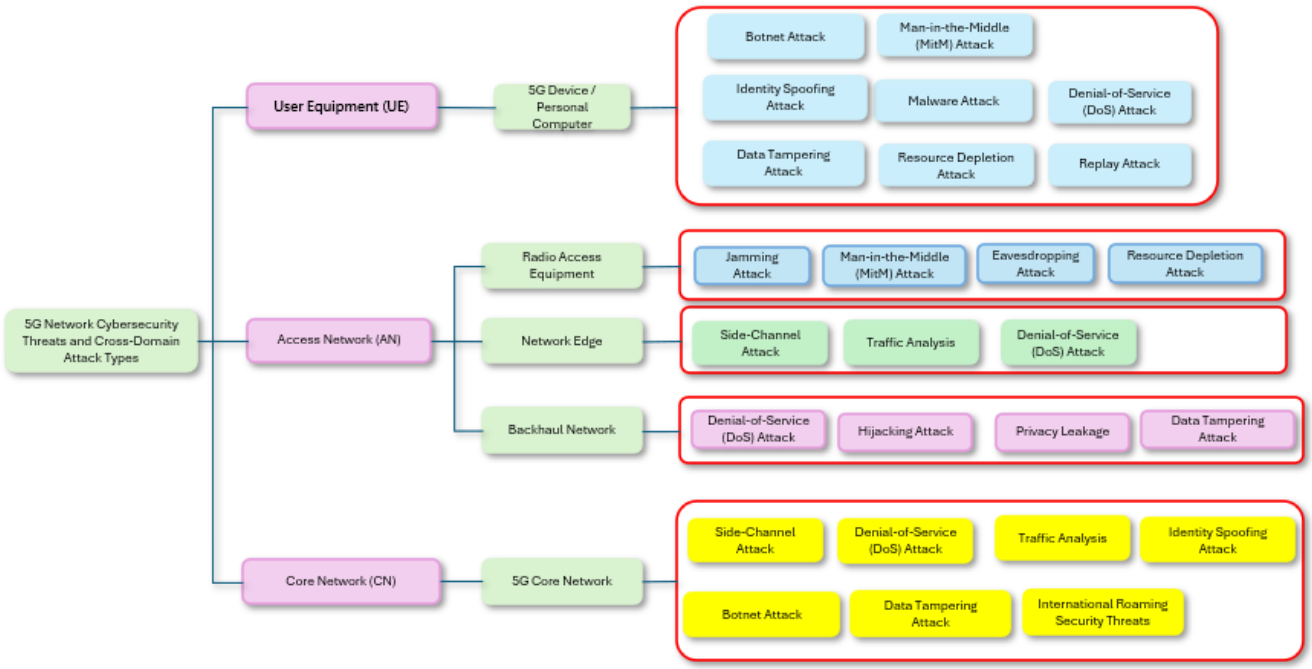

Figure 1. 5G Cybersecurity threat and attack domain (Source: Adapted from Kalhoro et al. [6]; compiled by the authors)

A study on a campus-based 5G private network by Djuitcheu et al. [10] further identified both internal attacks originating from within the network and external attacks from adjacent networks. Common attack vectors include Denial-of-Service (DoS), jamming, and Man-in-the-Middle (MitM) attacks. Cross-domain attacks are particularly critical, as they exploit vulnerabilities across network segments to gain unauthorized access, resulting in data exfiltration or system failure.

To better model such threats, the MITRE Corporation introduced the 5G Hierarchy of Threats (FiGHT™) framework in 2022. This framework complements the traditional MITRE ATT&CK® matrix by addressing the unique architectural features and diverse attack patterns specific to 5G environments [11]. As Vanderveen emphasizes, the FiGHT™ framework operationalizes threat intelligence and supports key cybersecurity activities such as adversary emulation and defense gap assessments, making it a vital reference for developing comprehensive 5G security strategies [5].

2.3 Cybersecurity Governance and Management

Cybersecurity governance maturity reflects an organization's ability to manage risks, align security with business objectives, and institutionalize defense mechanisms through continuous improvement. Effective governance integrates risk management, threat defense, incident response, and continuous monitoring into the overall organizational strategy, thereby elevating cybersecurity from an operational function to a strategic element of corporate governance.

By contrast, information security management, as defined by the ISO/IEC 27000 series [12], focuses on implementing policies, procedures, and controls to safeguard information assets in support of business operations. ISO/IEC 27001 [13] provides a structured framework for establishing an Information Security Management System (ISMS) that ensures confidentiality, integrity, and availability (CIA).

While ISO 27001 emphasizes operational implementation, ISO/IEC 27014 [14] offers explicit guidance for cybersecurity governance, outlining principles for senior leadership to drive strategic security decisions. Similarly, ISO 38500 [19] establishes an "Evaluate–Direct–Monitor" model to ensure strategic alignment and risk oversight within IT governance.

Leading international bodies have underscored the criticality of governance. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines five key pillars of effective cyber governance [15], while NIST SP 800-100 promotes a risk-based approach aligning cybersecurity with business strategy [16]. Likewise, the UK National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) [17]

recommends establishing governance structures that integrate cybersecurity into overall management through standardized, risk-based methods.

In the latest update, the "Govern" function was added as the strategic core of the NIST Cybersecurity Framework (CSF) 2.0 [18], complementing the existing Identify, Protect, Detect, Respond, and Recover functions. This inclusion highlights the necessity of defining clear policies, roles, and oversight mechanisms for all cybersecurity activities. The distinctions between governance and management functions are summarized in Table 2.

Effective cybersecurity governance provides a structured mechanism for defining frameworks, selecting controls, and responding to internal and external incidents, as conceptualized in Figure. 2.

Table 2. Comparison of cybersecurity governance and management

Aspect	Cybersecurity governance	Cybersecurity management
Definition	Focuses on the strategic level of cybersecurity by establishing policies, principles, and organizational direction.	Concentrates on day-to-day operations and the execution of specific cybersecurity measures.
Objective	Ensures alignment between organizational objectives and information security strategies.	Protects information systems and manages operational cybersecurity risks.
Primary activities	Formulating long-term objectives, conducting risk assessments, and overseeing regulatory compliance.	Implementing technical controls, conducting staff training, and performing continuous monitoring.
Level of involvement	Senior management and executive decision-makers.	Cybersecurity professionals and operational personnel.
Compliance requirements	Ensures adherence to laws, regulations, and recognized standards.	Ensures that technical controls comply with governance frameworks and policies.
Success indicators	Degree of organizational commitment to cybersecurity and the establishment of a security-oriented culture.	Security, stability, and reliable operation of information systems.
Scope	Encompasses organization-wide cybersecurity policies and strategic planning.	Encompasses specific technical implementations and operational procedures.

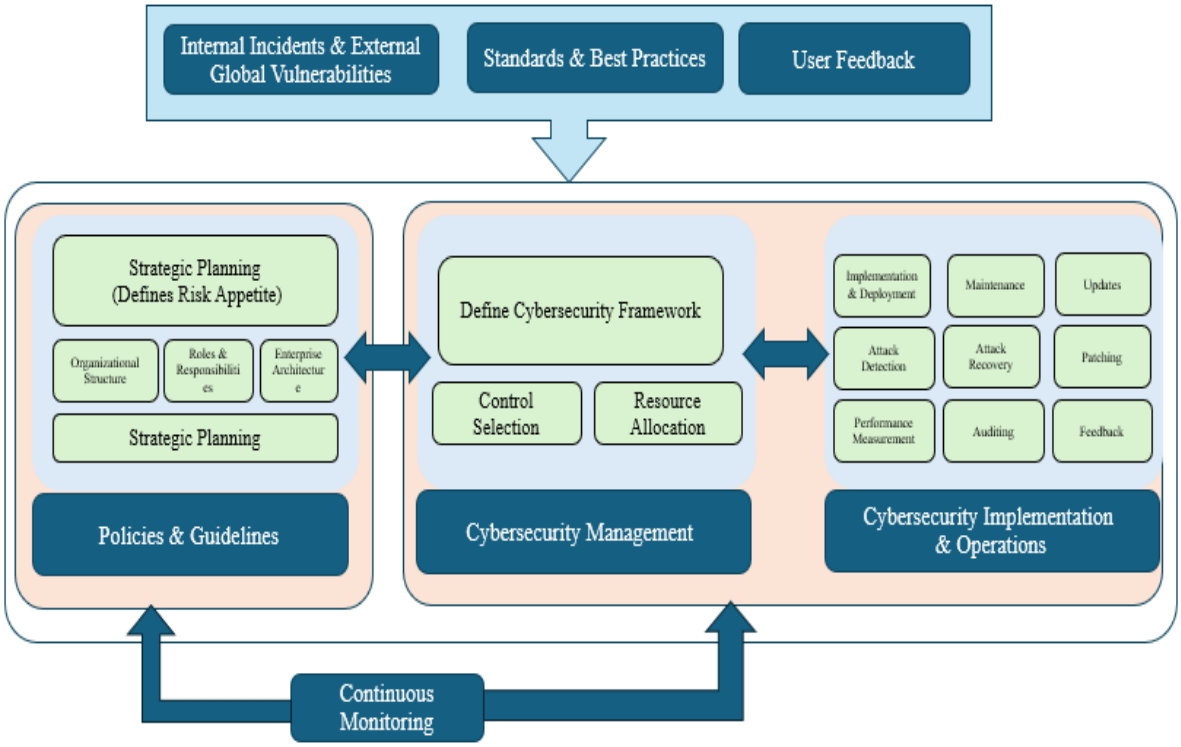

Figure 2. Framework for isms stabilization through governance, management, and operation (Source: Author's own representation)

2.4 Existing Cybersecurity Governance Maturity Frameworks

Amid increasing digitalization and escalating cyber threats, Maleh et al. (2021) proposed the CYBERGOV information security governance maturity framework to help organizations strengthen governance across five core areas: information security strategy, asset protection, infrastructure management, risk response, and third-party/cloud control. The framework employs key indicators to monitor governance effectiveness and prioritizes the allocation of resources toward high-risk areas to enhance organizational foresight and resilience.

When combined with frameworks such as the ISACA COBIT maturity model [20] and the EU Cybersecurity Education Maturity Assessment (2024) [21], organizations can integrate governance mechanisms aligned with international standards (e.g., ISO 27014 [14], ISO 38500 [19], and NIST CSF [18]) and advance from Level 1 (Initial) to Level 5 (Optimized). This hierarchical progression not only assesses the implementation of risk management practices but also reflects the maturity of supply chain and internal control strategies, offering a structured pathway toward comprehensive governance enhancement [22].

2.5 Toward an Integrated Governance Framework for 5G Private Networks

The preceding analysis demonstrates that while robust IT governance frameworks exist, they are insufficient for the converged IT-OT-CT environment of 5G private networks. An integrated solution must combine the strategic oversight principles of ISO 38500 [19] and ISO 27014 [14], the management system structure of ISO 27001 [13] and ISO 27002 [23], and the operational functionality of NIST CSF 2.0 [18]. The resulting three-tiered (strategic, tactical, and operational) governance maturity framework is summarized in Table 3.

2.6 5G Cybersecurity Maturity Assessment Level Design

The design of a corresponding maturity assessment system should draw from established tiered models, such as those from ENISA [21] and COBIT [20]. Such models enable organizations to benchmark governance performance against defined control objectives and best practices, providing a structured roadmap for continuous improvement. The proposed maturity levels are presented in Table 4.

2.7 Establishing an Integrated 5G Cybersecurity Maturity Framework Prototype

Based on the synthesis of existing standards and frameworks, this study develops an Integrated Cybersecurity Maturity Framework Prototype. As shown in Figure 3, it combines ISO 38500, ISO 27014, ISO 27001, and NIST CSF 2.0 principles with MITRE FiGHT™ threat-modeling capabilities and the governance requirements identified by Maleh et al. [24]. The prototype comprises three governance tiers (strategic, tactical, and operational), six governance domains, and twenty-five security practice objectives, ensuring cohesive alignment across all organizational levels.

Table 3. Proposed 5G cybersecurity governance framework (Source: Author's own representation)

Six integrated governance dimensions	ISO/IEC 27014	ISO/IEC 38500	ISO/IEC 27001	NIST CSF 2.0	MITRE FiGHT
Governance Policy (G1)	Governance responsibilities and policies	Board governance principles	Security policies and organizational structure	ID.GV (Governance)	Reconnaissance and initial access
Asset Management (G2)	Asset management and risk	Resource and asset contro	Asset identification and protection	ID.AM (Asset Management)	Resource discovery and system exploration
Risk Assessment (G3)	Risk assessment and quantification	Risk governance framework	Risk assessment procedures	ID.RA (Risk Assessment)	Detection and threat modeling
Control Measures (G4)	Control design and implementation	Control strategies and measures	Technical and operational controls	PR.AC (Access Control)	Targeted threat defense
Incident Response (G5)	Incident response and recovery	Disaster recovery planning	Incident management procedures	RS (Response)	Response and incident management
External Supply Chain (G6)	External collaboration and risk	Supply chain governance	Third-party security agreements	ID.SC (Supply Chain)	Supply chain risk management

Table 4. 5G Cybersecurity governance maturity assessment levels (Source: Author's own representation)

Maturity level	Score	Description	Key elements	Evaluation indicators	Practice directions
Level 1 – Initial	0-20	The organization has limited awareness of 5G private network security and lacks formal strategies and procedures.	Risk Awareness: Low, insufficient recognition of security threats in 5G private networks.	Probability of Attack Success: High	Establish basic security awareness and formulate preliminary cybersecurity policies for 5G private networks.
Level 2 – Repeatable	21-40	The organization has begun implementing certain 5G private network security measures, but these are typically reactive and lack unified management.	Risk Assessment: Initiation of informal risk assessments.	System Response Time: Long	Formally establish a security organization dedicated to 5G private network security affairs.
Level 3 – Defined	41-60	The organization has established formal 5G private network security strategies and procedures, integrating them into business processes.	Threat Defense: Implementation of standardized security controls, such as network slicing security.	Resource Consumption: High	Strengthen cross-departmental collaboration to ensure effective execution of 5G private network security strategies.
Level 4 – Quantitatively Managed	61-80	The organization can quantify the effectiveness of 5G private network security measures and continuously improve based on data analysis.	ncident Response: Establish incident response plans and conduct regular exercises.	Monitoring Programs: Plan and maintain stakeholder feedback, measure progress toward objectives, and ensure strategic goals remain effective and aligned with business needs	Establish quantitative evaluation indicators, regularly monitor and assess the effectiveness of 5G private network security measures, and adjust based on results.
Level 5 – Optimized	81-100	The organization's 5G private network security measures have reached best-practice levels and can proactively address emerging threats.	Continuous Monitoring: Implement automated monitoring and analysis to detect and respond to security incidents in real time.	Effectiveness of Mitigation Strategies: High	Threat Defense: Define how security procedures enable the organization to resist security threats.

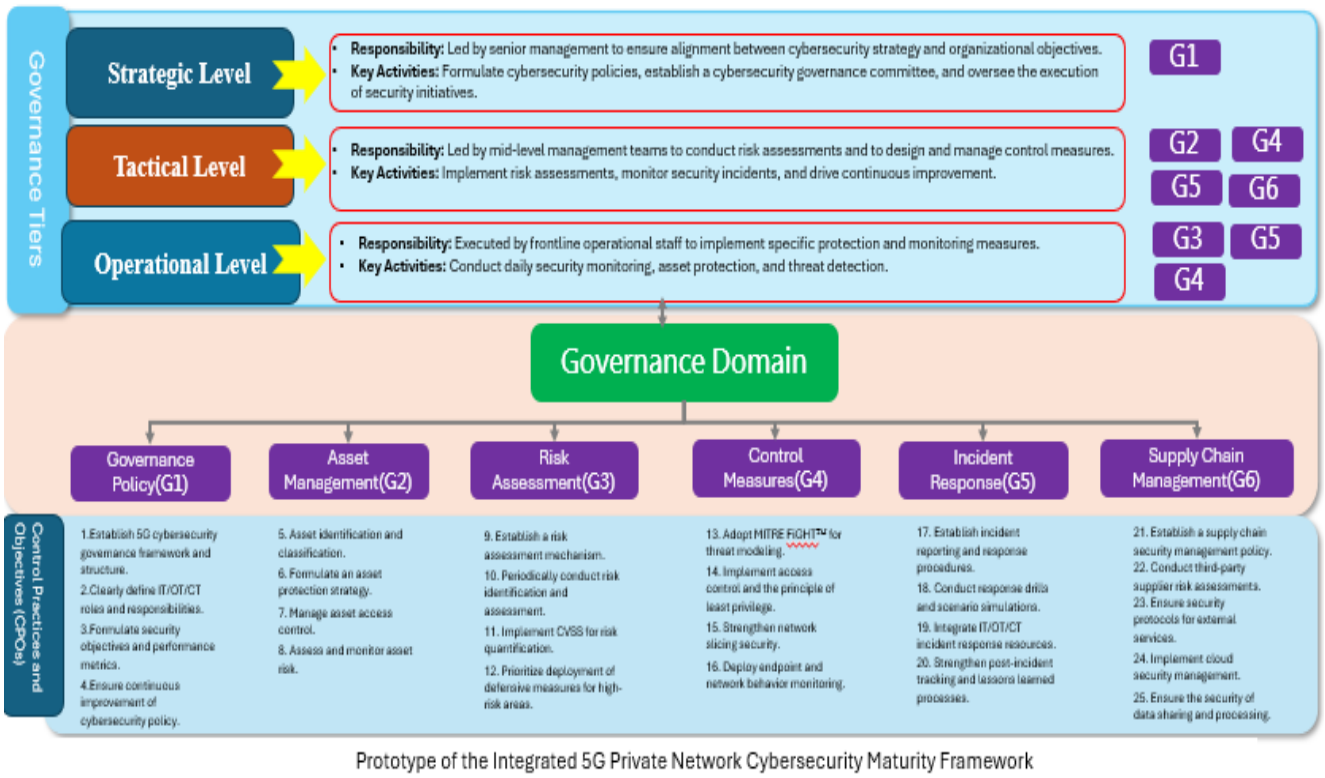

Figure 3. Proposed three-tiered Cybersecurity Governance Maturity Framework (Source: Author's own representation)

3 Research Methodology and Design

The experimental architecture in this study was modeled after a typical 5G private network deployment within Taiwan's smart manufacturing sector, adopting a *Shared Cloud Core Network* configuration. Within this simulated environment, penetration testing scenarios were designed and executed to validate the effectiveness of defensive mechanisms under the proposed Cybersecurity Governance Maturity Framework.

3.1 Attack Framework: MITRE FiGHT™

The penetration tests were constructed using the MITRE 5G *Hierarchy of Threats* (FiGHT™) framework [11], which operationalizes threat intelligence, adversary emulation, and defense gap analysis in 5G environments [5]. This framework complements the broader ATT&CK® matrix [12] by modeling attack behaviors and architectural vulnerabilities that are specific to mobile networks. FiGHT™ version 2.1.1 classifies 5G-related techniques as *theoretical*, *proof-of-concept (PoC)*, or *observed*, providing a realistic foundation for systematic threat modeling. Following the testing design proposed by Attieh et al. [25], the FiGHT™ framework was employed as a baseline for simulating lateral movement and cross-domain attack scenarios, thereby validating both the coverage and the effectiveness of existing defensive mechanisms.

3.2 Vulnerability Assessment and Quantification: CVSS v3.1

To ensure consistency in evaluating vulnerabilities identified during testing, the Common Vulnerability Scoring System (CVSS) v3.1, maintained by the Forum of Incident Response and Security Teams (FIRST) [26], was adopted. CVSS provides a standardized method for deriving a quantitative *Base Score* that reflects the severity of each vulnerability on a scale ranging from *None* to *Critical*. This score is computed from exploitability metrics (e.g., Attack Vector, Attack Complexity) and impact metrics (e.g., Confidentiality, Integrity, Availability). The resulting score offers an objective measure of the potential risk associated with each vulnerability and serves as a critical input for the governance maturity assessment, supporting risk prioritization and enhancing the precision of the proposed model.

3.3 Mitigation Strategy: MITRE FiGHT™ Defensive Recommendations

Beyond defining attack techniques, the MITRE FiGHT™ framework provides a corresponding set of mitigations aimed at preventing or limiting the impact of identified threats. These mitigations are categorized into technical, procedural, and policy-based controls, each directly mapped to specific attack techniques. This modular structure enables organizations to perform scenario-driven defense planning. In this study, the recommended mitigations for three representative attack techniques were analyzed: host discovery via IP scanning, core network scanning for isolation weaknesses, and endpoint denial-of-service (DoS) attacks. The analysis confirms that the FiGHT™ framework delivers actionable and technically grounded defensive recommendations that can be incorporated into enterprise 5G cybersecurity governance policies to enhance overall network resilience.

3.4 Governance Efficacy Assessment: Correlating Vulnerability Scores with Maturity

It is important to emphasize that a CVSS score represents a technical measure of risk rather than a direct indicator of governance capability. Consequently, this study does not map CVSS scores directly to maturity levels. Instead, the CVSS score serves as a quantitative risk indicator that is interpreted alongside the organization's observed performance during penetration testing. This combined analysis enables the inference of governance maturity within specific domains by identifying defensive weaknesses and institutional response deficiencies. For example, the existence of a high-CVSS vulnerability without effective countermeasures indicates a low maturity level in the corresponding governance domain. Conversely, when robust management processes and responsive mechanisms are in place for high-risk vulnerabilities, a higher level of governance maturity is reflected. This conceptual correlation is outlined in Table 5.

Table 5. Correlation between cvss base score and inferred governance maturity level (Source: Author's own representation)

Cvss score	Severity	Maturity indicator	Description	Key elements
9.0~10	Critical	Initial Level (L1)	The organization has limited awareness of 5G private network security and lacks formal strategies and procedures.	Risk Awareness: Low, insufficient recognition of security threats in 5G private networks.
7.0~8.9	High	Repeatable Level (L2)	The organization has begun implementing partial private network control measures, which are typically reactive and lack unified management.	Risk Assessment: Initiation of informal risk assessments.
4.0~6.9	Medium	Defined Level (L3)	The organization has established formal private network security strategies and procedures, integrating them into business processes.	Threat Defense: Implementation of standardized security control measures.
0.1~3.9	Low	Quantitatively Managed Level (L4)	The organization can quantify the effectiveness of private network security measures and continuously improve based on analytical results.	Incident Response: Establish incident response plans and conduct regular exercises.
0.0	None	Optimized Level (L5)	The organization's private network security measures have reached best-practice levels and can proactively address emerging threats.	Continuous Monitoring: Implement automated monitoring and analysis to detect and respond to security incidents in real time.

4 System Implementation and Experimental Analysis

4.1 Simulation Environment and Attack Scenario Design

To validate the proposed framework, a simulated 5G private network environment was established to conduct attack simulations and evaluate mitigation measures. The experimental setup utilized the open-source *free5GC* project (v3.3.0), based on the 3GPP Release 15 architecture [27], together with *UERANSIM* [28] to emulate both user equipment (UE) and the gNodeB radio access network module. This configuration accurately replicates a typical 5G private network deployment in smart factory environments, reproducing the complete communication sequence—from UE registration through the access network to the 5G Core (5GC). The tools, functionalities, and configurations employed in the simulation are summarized in Table 6.

The environment was deployed on an Ubuntu 20.04.4 virtual machine running on VirtualBox. The core network (*free5GC*), access network (*gNodeB*), and user equipment (*UE*) were interconnected via virtual network interfaces to form a complete 5G private network topology, as depicted in Figure 4.

Table 6. Experimental environment tools and configuration (Source: Author's own representation)

Simulation tool	Simulation target	Primary functions	Application scenarios	Deployment method
free5GC v3.3.0	5G core network modules (AMF, SMF, UPF, NRF, PCF, etc.)	Implements 5GC functions compliant with 3GPP Release 15, supporting session management and user-plane processing, simulating actual core network behavior.	Verification of core network modules, testing of control-plane and user-plane communications, cross-domain attack simulation (e.g., UPF misuse).	Deploy each core module within virtual machines, using virtual network interfaces to emulate communication topology.
UERANSIM	Access network and terminal devices (gNodeB and UE)	Simulates UE registration, PDU session establishment, data transmission, and gNB behavior, reproducing access-layer network communications.	Exercises for access-layer attacks such as DoS, abnormal signaling registration, and traffic surges; validation of security protection measures.	Deploy gNB and multiple UE instances within the same virtual machine to emulate large-scale device access scenarios.

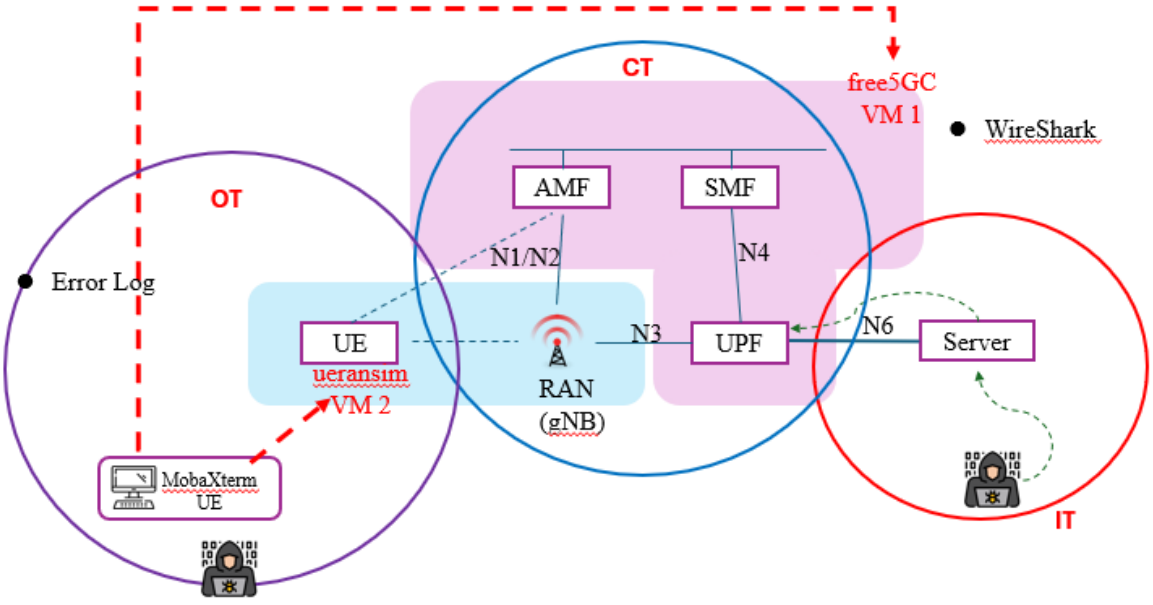

Figure 4. Topology of the 5G private network experimental environment (Source: Author's own representation)

4.2 Simulation of Cross-Domain Attacks

The attack simulation assumes that a threat actor successfully compromises a gNodeB and impersonates a legitimate UE to gain access to the private network. From this vantage point, the attacker conducts reconnaissance and exploits identified vulnerabilities. The successful interconnection between the core network (*free5GC*), the base station (*gNodeB*), and the user equipment (*UE*) was first verified, as illustrated in Figure 5.

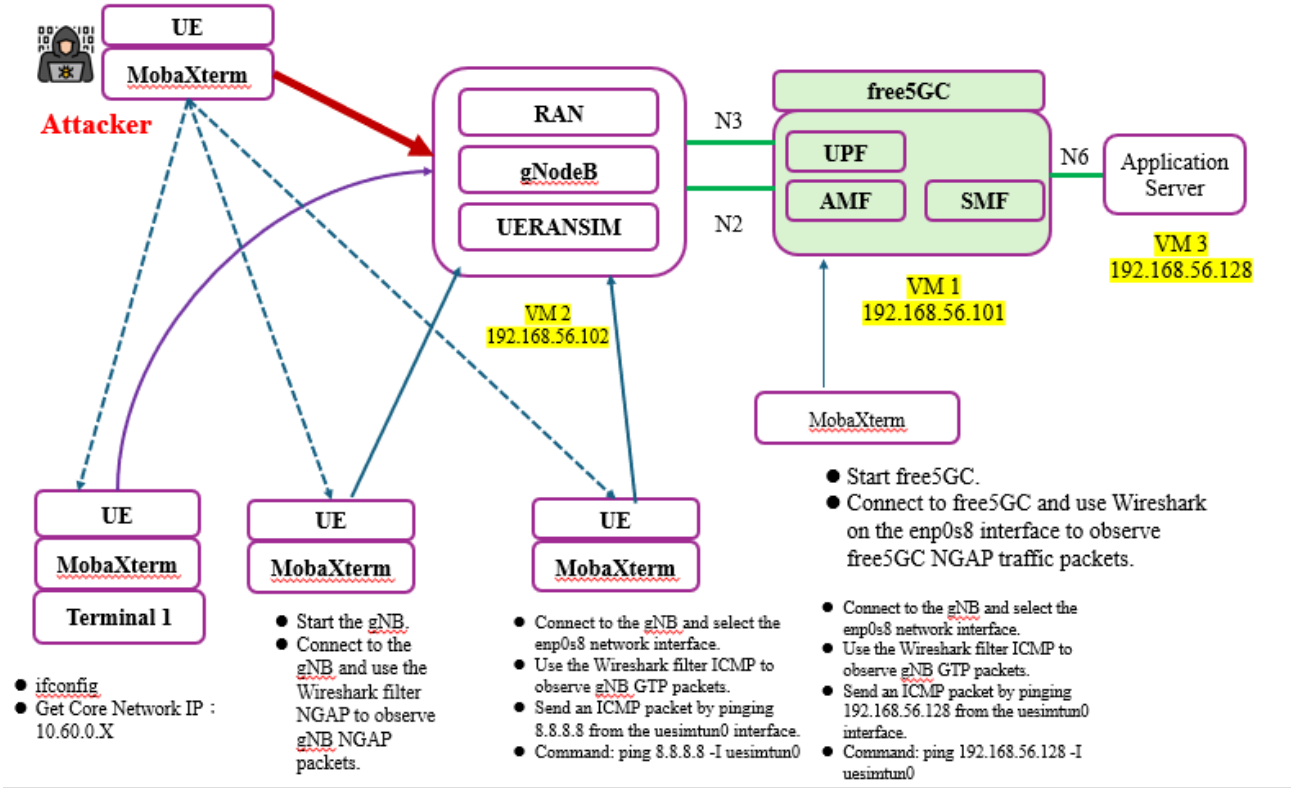

Figure 5. Simulated attack experiment setup (Source: Author's own representation)

To validate the proposed Cybersecurity Governance Maturity Framework, representative attack scenarios were designed according to tactics and techniques derived from the MITRE ATT&CK® and FiGHT™ frameworks. These scenarios encompass reconnaissance, infiltration, and denial-of-service stages, targeting potential risk vectors across the converged Information Technology (IT), Operational Technology (OT), and Communication Technology (CT) domains. The attack progression is outlined as follows:

Network Reconnaissance: After obtaining valid credentials and accessing the 5G network by impersonating a legitimate UE, the attacker conducts initial reconnaissance. Using tools such as *nmap*, the attacker scans the network to identify active hosts and open ports, gathering intelligence on the network architecture and services in preparation for subsequent attacks.

Network Isolation Testing: The attacker issues *ping* and *GET* requests to test connectivity from the compromised endpoint to external interfaces (N2, N3, N6). This phase assesses the adequacy of network segmentation and the isolation of control components across interconnected IT, OT, and CT domains.

Simulated Denial-of-Service Attack: Leveraging intelligence gathered during reconnaissance, the attacker, operating as a low-privilege user, exploits vulnerability CVE-2023-47025, which exists in the *free5gc-compose* component of *free5GC* v3.3.0. This flaw enables a local user to trigger a Denial-of-Service (DoS) condition. A successful exploit disrupts critical 5G Core functions—including AMF, SMF, and UPF—resulting in a significant degradation of system availability. This experiment demonstrates that in the absence of proper network segmentation and least-privilege controls, an attacker can pivot from IT or OT nodes to compromise the CT core, leading to a network-wide outage.

4.3 Mitigation Strategies and Maturity Assessment Indicators

The DoS attack scenarios targeted key nodes across the domains, including CT core components (AMF, UPF), the IT application layer (Application Server), and the OT device management layer, to evaluate risk exposure and defensive efficacy. Vulnerabilities were quantified using the CVSS v3.1 Base Score model, with resulting scores serving as input parameters for the governance maturity assessment.

The two primary attack cases yielded high-severity scores (7.4 and 7.5), primarily reflecting the loss of system availability. This outcome underscores how the operational flexibility inherent in converged OT/CT architectures can introduce critical security gaps. Based on the MITRE FiGHT™ framework, corresponding mitigation strategies for these attacks were identified and are summarized in Table 7.

Table 7. Endpoint denial-of-service (DoS) attack simulation and mitigation strategies (Source: Author's own representation)

Attack type	Evaluation indicators	Primary vulnerabilities	Mitigation measures
Network DoS (Traffic-Based)	CVSS 7.4 (High) AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	Unrestricted exposure of the data plane to UE nodes, leading to resource exhaustion.	Traffic monitoring and packet whitelisting to filter and validate UE traffic behavior toward N6.
Endpoint DoS (Endpoint-Oriented)	CVSS 7.5 (High) AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	UE nodes can launch unauthenticated packet attacks against the AMF core module	Vulnerability patching (e.g., CVE correspondence) and configuration of AMF isolation mechanisms

4.4 Framework Efficacy Evaluation

The feasibility and practical utility of the proposed Cybersecurity Governance Maturity Framework were validated through simulated attack exercises and the deployment of corresponding mitigations. DoS attack scenarios were conducted at both the network layer (e.g., UDP flood on the N6 interface) and the endpoint layer (e.g., AMF disruption via CVE exploit). Threat severity was quantified using CVSS, while mitigation measures were implemented according to MITRE FiGHT™ recommendations.

The experimental results demonstrate that adoption of the proposed governance framework facilitates a more systematic and consistent deployment of defensive mechanisms. At the operational level, implementing specific controls—such as packet filtering, network segmentation, access control lists, and resource limitation—significantly enhanced real-time threat detection and response capabilities. At the tactical and strategic levels, the feedback loop established by leveraging CVSS scores to inform governance decisions enabled a risk-driven approach to security policy adjustment. This approach ensures that limited resources are allocated to address the most critical vulnerabilities.

Although the initial deployment of the framework requires investment in planning, executive endorsement, and resource allocation, its long-term benefit lies in the sustained enhancement of organizational resilience and regulatory compliance. For highly dynamic and converged environments such as 5G private networks, a governance-oriented cybersecurity model provides a robust foundation for long-term architectural integrity and strategic development. The *Improved Cybersecurity Governance Maturity Framework Prototype* proposed in this study not only offers concrete support for defending against cross-domain attacks in 5G private networks but also provides extensibility and adaptability for diverse industrial applications, thereby strengthening national cybersecurity capabilities for next-generation communication infrastructures.

5 Conclusion

This study examined the cybersecurity risks associated with cross-domain attacks spanning Information Technology (IT), Operational Technology (OT), and Communication Technology (CT) systems within 5G private networks deployed in smart factory environments, and proposed a governance-oriented strategy to address these challenges. Built upon a foundation of international cybersecurity management standards, and integrated with the MITRE FiGHT threat matrix and the CVSS v3.1 scoring mechanism, this work developed a multilayered 5G cybersecurity governance maturity model that mitigates the lack of horizontal coordination and vertical integration in existing security frameworks.

On the practical side, penetration tests were conducted in a simulated 5G private network environment using Free5GC and UERANSIM under multiple attack scenarios, such as traffic-based denial-of-service and endpoint exploitation. The results indicate that applying the proposed governance-tiered framework and its corresponding defensive measures significantly reduced both the attack success rate and the associated CVSS risk scores. These findings demonstrate the model's ability to enhance the mutual reinforcement between technical controls and governance processes, thereby supporting clearer delineation of security responsibilities, optimized resource allocation, and improved interdepartmental coordination.

Furthermore, the study confirms that reliance solely on isolated technical controls or passive defenses is insufficient for addressing the complex, cross-domain threat landscape inherent to converged 5G environments. The empirical results reveal that a governance-oriented process, coupled with attack behavior modeling, can create a closed-loop mechanism linking strategic decision-making with operational control implementation. This produces concrete and quantifiable evidence for cybersecurity governance while enabling defensive mechanisms to evolve dynamically according to adversarial behaviors.

Overall, the proposed framework demonstrated its effectiveness and practical feasibility through simulation-based validation, offering substantial reference value for applications in smart manufacturing, industrial communications, and private 5G deployments. It holds strong potential to serve as a foundational basis for future policy development and industry standards, supporting both governmental and industrial sectors in strengthening cybersecurity governance and resilience across critical application domains.

Looking forward, several directions for research and practical advancement warrant further exploration:

- The development of specialized questionnaires and digital assessment tools to continuously reflect organizational governance maturity and support dynamic management.
- The expansion of validation across heterogeneous communication protocols and multi-vendor devices to enhance the model's applicability in diverse deployment scenarios.
- The incorporation of supply-chain security perspectives to extend governance across the responsibility chain and improve the completeness of third-party and external cybersecurity controls.

References

[1] A. Khan, N. U. Arfeen, K. Ali, M. Ullah, I. Ali, M. Asim, I. Uddin, *The Impact of 5G Technology on IT and Digital Communication*, ResearchGate, January, 2025.

[2] 5G Alliance for Connected Industries and Automation (5G-ACIA), *5G Non-Public Networks for Industrial Scenarios*, 5G-ACIA, July, 2019. https://5g-acia.org/media/2021/04/WP_5G_NPN_2019_01.pdf

[3] Y. Maleh, IT/OT Convergence and Cyber security, *Computer Fraud & Security*, Vol. 2021, No. 12, pp. 13-16, December, 2021. https://doi.org/10.1016/S1361-3723(21)00129-9

[4] Y. Maleh, A. Sahid, M. Belaissaoui, A Maturity Framework for Cybersecurity Governance in Organizations, *EDPACS*, Vol. 63, No. 6, pp. 1-22, 2021. https://doi.org/10.1080/07366981.2020.1815354

[5] M. Vanderveen, Threat Framework for 5G Cellular Communications, *2022 IEEE Military Communications Conference (MILCOM)*, Rockville, MD, USA, 2022, pp. 565-570. https://doi.org/10.1109/MILCOM55135.2022.10017976

[6] S. Kalhoro, F. B. Shaikh, A. Kalhoro, J. U. R. Abbasi, R. K. Ayyasamy, An Overview of Security Attacks in 5G Enabled Technologies: Applications and Use Case Scenarios, *ISeCure*, Vol. 16, No. 1, pp. 17-35, January, 2024. https://doi.org/10.22042/isecure.2023.354872.829

[7] 3rd Generation Partnership Project (3GPP), *5G System Overview*, 3GPP, August, 2022.

[8] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, 5G Security: Analysis of Threats and Solutions, *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, Finland, 2017, pp. 193-199. https://doi.org/10.1109/CSCN.2017.8088621

[9] Taiwan Association of Information and Communication Standards (TAICS), *TR-0028 v1.0:2023: Cybersecurity Assessment Guidelines for 5G Private Network Service Management Systems*, Taipei, Taiwan, November, 2023. https://ws.5ghub.org.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNDkwL3JlbGZpbGUvMTE1OTAvMzAzL2JmODViNzBjLWZmYzktNDY3Yi04MmM0LWY0NjQwMjE2NWRmYy5wZGY%3D&n=VEFJQ1MgVFItMDAyOCB2MS4w77yaMjAyMy01R%2BWwiOe2suacjeWLmeeuoeeQhuezu%2Be1seizh%2BWuieipleS8sOaMh%2BW8lS5wZGY%3D&icon=.pdf

[10] H. Djuitcheu, S. B. Mallikarjun, M. A. Habibi, N. P. Kuruvatti, H. D. Schotten, Securing Private 5G Campus Networks: Abstract Survey on Current Status, Security Threats, and Research Landscape, *2023 2nd International Conference on 6G Networking (6GNet)*, Paris, France, 2023, pp. 1-4. https://doi.org/10.1109/6GNet58894.2023.10317752

[11] The MITRE Corporation, *MITRE FIGHT™ (5G Hierarchy of Threats) Tactics & Techniques*, https://fight.mitre.org, July, 2025.

[12] National Standards of the Republic of China, *CNS 27000 X6101: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*, Taipei, Taiwan, 2023.

[13] International Organization for Standardization, *ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements*, Geneva, Switzerland, 2022.

[14] International Organization for Standardization, *ISO/IEC 27014:2020, Information Security, Cybersecurity and Privacy Protection - Governance of Information Security*, Geneva, Switzerland, 2020.

[15] Cybersecurity and Infrastructure Security Agency (CISA), *Cybersecurity Best Practices: Cybersecurity Governance: Integrating Strategy with Operational Resilience*, CISA Report, 2021.

[16] National Institute of Standards and Technology (NIST), *SP 800-100, Information Security Handbook: A Guide for Managers*, Gaithersburg, MD, USA, 2006.

[17] National Cyber Security Centre (NCSC), *Cyber Assessment Framework (CAF) v3.0*, NCSC Report, 2021.

[18] National Institute of Standards and Technology (NIST), *The NIST Cybersecurity Framework (CSF) 2.0*, Gaithersburg, MD, USA, 2024.

[19] International Organization for Standardization, *ISO/IEC 38500: 2015, Information Technology - Governance of IT for the Organization*, Geneva, Switzerland, 2015.

[20] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*, Schaumburg, IL, USA, 2019.

[21] European Union Agency for Cybersecurity (ENISA), *Cybersecurity Education Maturity Assessment*, ENISA Report, May, 2024.

[22] T. Toifur, Kusrini, A. Budi, Evaluation of Information Technology Governance Using COBIT 5 and ISO/IEC 38500, *JOIN (Jurnal Online Informatika)*, Vol. 7, No. 1, pp. 17-27, 2022. https://doi.org/10.15575/join.v7i1.814

[23] International Organization for Standardization, *ISO/IEC 27002: 2022, Information Security, Cybersecurity and Privacy Protection - Information Security Controls*, Geneva, Switzerland, 2022.

[24] F. Loeffen, *The Development of an Information Security Governance Maturity Model for Dutch Hospitals*, Ph. D. Thesis, Leiden University, Leiden, The Netherlands, 2019.

[25] A. A. H. Attieh, L. Y. X. Tong, N. J. Kai, L. T. Y. Teck, I. N. S. Mun, P. M. Mohan, Threat Hunting on 5G Future Communication Testbed Using MITRE FIGHT Framework, *2024 IEEE Region 10 Conference (TENCON)*, Singapore, 2024, pp. 1-6.

https://doi.org/10.1109/TENCON61640.2024.10903058
[26] FIRST.org, Inc., *Common Vulnerability Scoring System v3.1: Calculator*, https://www.first.org/cvss/calculator/3-1, 2023.
[27] free5GC Project, *free5GC: An Open-source 5G Core Network Platform*, https://www.free5gc.org, July, 2025.
[28] A. Güneş, *UERANSIM: An Open-source 5G UE and gNodeB Simulator*, GitHub Repository, 2024.

Biographies

Hung-Cheng Yang received a bachelor's degree in traffic management in Taiwan in 1984 and a master's degree in information management from the Central Police University in Taiwan in 2003. He has been studying computer science and Information engineering at Tatung University for a Ph.D. since 2021. Since 1984, he has worked for the police. His research interests include digital evidence and forensics, and traffic accident prevention using big data. (yangyeh5046@gmail.com).

I-Long Lin received a B.S. degree from Central Police University, Taiwan, in 1983 and M.S. and Ph.D. degrees from Tamkang University, National Taiwan University of Science and Technology, Taiwan, in 2002 and 2005. From 1983 to 2011, he worked as a professor at Central Police University, Taiwan. Since 2012 to 2021, he was a professor at Yuanpei University of Medical Technology, Taiwan. Since 2021, he has been a professor at Tatung University. His research interests include digital evidence and forensics, and cybersecurity. (cyberpaul@gm.ttu.edu.tw)

Yueh Lin received a bachelor's degree in mass communication in Taiwan in 1994. He has been working in the information services industry for over 25 years, specializing in ICT integration and infrastructure development. He has also assisted the automotive industry in data center planning and application system development project management, and obtained ISO 27001 lead auditor certification. Since 2023, he has been pursuing a master's degree in computer science and information engineering at Tatung University. His research interests include cybersecurity se governance maturity, supply chain Cyber security management, Cyber security policy. (yuehlin@gmail.com)

Chorng-Ming Chen earned a Bachelor's degree from National Chengchi University in 1995, a Master's degree from the University of Management and Technology, USA, in 2004, and another Master's degree in Computer Science and Information Engineering from Tatung University in 2023. Since 2023, he has been pursuing a Ph.D. at Tatung University. He has held roles such as R&D Manager, CTO, and CISO since 1986. His research interests include intelligent customer service, information security, digital forensics, AI, and LLM. (avenchentw@gmail.com)