International Studies in Science and Technology
https://isstechjournal.science

Cybersecurity Capacity Building and Institutional Resilience in Developing Country Agencies: A Field Study

Paul Leung*

Felizberta Lo Padilla Tong School of Social Sciences, Saint Francis University, Hong Kong, Hong Kong SAR, China

Corresponding author: paul.leung@sfu.edu.hk

Abstract

This paper examines the critical dynamics of cybersecurity capacity building and its direct impact on institutional resilience within public sector agencies of developing countries. Utilizing a multiple-case study methodology across five core government ministries and agencies over an eighteen-month field research period, the study investigates how socio-technical interventions, resource allocations, and administrative structures interact to shape an organization's defense and recovery posture. The empirical findings reveal that while technical infrastructure investments are necessary, they are insufficient for cultivating true institutional resilience without parallel investments in administrative adaptation, localized human capital preservation, and flexible policy frameworks. Bureaucratic inertia, high technical staff turnover driven by private sector wage disparities, and a reliance on rigid, donor-driven capacity models often undermine long-term sustainability. Based on these insights, this research proposes a tailored, three-tiered strategic framework that emphasizes modular socio-technical designs, localized knowledge transfer systems, and continuous, threat-informed administrative feedback loops. This framework offers actionable pathways for international development partners and national policymakers seeking to secure critical public infrastructure against increasingly sophisticated global cyber threats.

Keywords: Capacity Building; Institutional Resilience; Developing Countries; Public Sector Cybersecurity; Developing Country Agencies

1. Introduction

1.1 Background and Context

The rapid digitization of public administration, commonly referred to as e-government, has emerged as a cornerstone of socio-economic development strategies globally. In developing countries, digital initiatives promise to enhance service delivery efficiency, increase transparency, reduce administrative overhead, and promote financial inclusion. However, this accelerated digital transformation has outpaced the development of robust cybersecurity capabilities, exposing public sector infrastructure to unprecedented systemic risks. The transition from legacy, paper-based administrative systems to interconnected digital databases and online portals has significantly expanded the attack surface of these nations. Consequently, public agencies have become attractive targets for a diverse array of threat actors, ranging from politically motivated hacktivists to highly organized transnational cybercriminals.

Within developing economies, cybersecurity capacity building is often conceptualized through a narrow technical lens, focusing primarily on the procurement of hardware and software solutions such as firewalls, intrusion detection systems, and antivirus suites [1]. This technology-centric approach frequently overlooks the complex socio-technical and institutional dimensions that govern how technology is deployed, maintained, and integrated into daily administrative routines. True institutional resilience requires not only advanced technical infrastructure but also organizational agility, robust governance models, comprehensive human capital strategies, and a culture of continuous risk management [2]. Without these non-technical pillars, capital-intensive

cybersecurity investments quickly obsolesce, leaving public agencies vulnerable to critical disruptions that can compromise national security and public trust.

1.2 Problem Statement

The central challenge facing developing country public agencies lies in the profound mismatch between standard, Western-centric cybersecurity models and the socio-economic, political, and administrative realities of these local contexts [3]. Most established cybersecurity capacity-building frameworks are designed under the assumption of abundant financial resources, highly stable administrative processes, mature domestic labor markets for technology professionals, and high levels of institutional trust. When these frameworks are imported without adaptation, they routinely fail to deliver sustainable security outcomes.

Public sector agencies in developing nations frequently operate under severe, chronic resource constraints, characterized by volatile budget cycles, rigid bureaucratic hierarchies, and significant salaries gaps compared to the private sector [4]. These conditions lead to acute talent shortages, as qualified cybersecurity professionals are rapidly poached by private enterprises or international organizations. Furthermore, the administrative culture in many developing institutions tends to emphasize formal, paper-based compliance over dynamic, operational risk management. This results in a state of superficial security, where policy documents exist on paper, but actual security practices on the ground remain weak and uncoordinated [5]. There is a critical shortage of empirical research that systematically analyzes these challenges from a socio-technical perspective, highlighting the need for detailed field studies that document the practical realities of cybersecurity capacity building within these complex administrative environments.

1.3 Research Objectives and Contributions

This study addresses this gap in the literature by presenting a comprehensive, field-based analysis of cybersecurity capacity building and institutional resilience in the public agencies of a developing country. The primary objectives of this research are threefold: first, to empirically document the systemic challenges and barriers to effective capacity building within diverse public sector organizations; second, to evaluate the relationship between different capacity-building interventions and the resulting levels of institutional resilience; and third, to develop a contextualized, actionable strategic framework that can guide future capacity-building efforts in resource-constrained environments.

To achieve these objectives, this paper analyzes five key government institutions that represent critical nodes of national infrastructure and administrative operations. By combining qualitative insights from semi-structured interviews and field observations with quantitative administrative data, this study offers several key contributions. It provides a nuanced understanding of how bureaucratic structures, procurement processes, and human resource policies directly impact technical security outcomes. It also shifts the analytical focus from passive compliance to active, adaptive resilience, offering a more pragmatic and sustainable pathway for international donor agencies, national policymakers, and agency leaders tasked with securing digital governance in the global South.

2. Literature Review and Theoretical Framework

2.1 Cybersecurity Capacity Building Models

The academic literature on cybersecurity capacity building has evolved significantly over the past two decades, transitioning from a narrow focus on technical system defense to a more holistic, socio-technical perspective. Early capacity-building initiatives in developing nations were heavily influenced by international development agencies and technology vendors who prioritized infrastructure deployment [6]. These interventions were often criticized for treating cybersecurity as a discrete, technical problem that could be resolved through the procurement of standardized commercial-off-the-shelf software and hardware. This approach frequently resulted in shelfware—expensive, sophisticated technologies that remained uninstalled or poorly configured due to a lack of local technical expertise to manage them.

To address these limitations, several multi-dimensional maturity models were developed, most notably the Cybersecurity Capacity Maturity Model for Nations, developed by the Global Cyber Security Capacity Centre [7]. This framework conceptualizes capacity across five distinct dimensions: cybersecurity policy and strategy,

cyber culture and society, cybersecurity education and training, legal and regulatory frameworks, and standards and technologies. While these comprehensive models have succeeded in raising awareness about the multi-faceted nature of cybersecurity, researchers have noted that they often remain descriptive rather than prescriptive [8]. They outline what a mature cybersecurity posture looks like based on developed-world standards, but provide little guidance on how resource-constrained agencies in developing countries can realistically navigate the transition from low to medium maturity levels given their unique structural constraints.

2.2 Institutional Resilience in Public Administration

In the context of public administration, resilience is defined as the capacity of an organization to anticipate, absorb, adapt to, and recover from disruptive events, whether they are natural disasters, economic crises, or cyberattacks [9]. Unlike traditional security approaches that aim for absolute protection and zero system compromise, the paradigm of institutional resilience accepts that some level of failure or breach is inevitable. Therefore, resilient organizations design their systems, policies, and workflows to minimize the blast radius of a disruption, maintain core mission-essential functions during an ongoing crisis, and recover to a stable state as rapidly as possible [10].

The theoretical foundations of institutional resilience are deeply rooted in organizational theory and high-reliability organization research. Scholars argue that resilience is not a static property of an agency but a dynamic capability that must be continuously practiced and updated [11]. In public sector agencies, this dynamic capability is shaped by three main factors: structural flexibility, cognitive readiness, and operational redundancy. Structural flexibility refers to the ability of administrative hierarchies to temporarily decentralize decision-making authority during a crisis, allowing frontline technical staff to act rapidly without waiting for lengthy bureaucratic approvals. Cognitive readiness involves the collective awareness and training of both technical and non-technical staff regarding threat vectors and response protocols. Operational redundancy ensures that critical data, systems, and communication channels have functional backups that can be activated immediately in the event of a primary system failure.

2.3 Developing Country Context and Challenges

Applying institutional resilience theories to public agencies in developing countries reveals several unique structural challenges. First, the political economy of IT procurement in these regions is highly complex and often influenced by external funding structures. Many cybersecurity projects are funded through bilateral aid or international development loans, which come with rigid project timelines, specific procurement guidelines, and a preference for international consulting firms [12]. This donor-driven model often leads to the implementation of highly sophisticated, proprietary solutions that create long-term vendor lock-in and high recurring licensing fees that local budgets cannot support once the initial project funding expires.

Second, the structural realities of public sector employment in developing nations pose a significant barrier to maintaining capacity. The massive salary disparity between the public sector and both local and international private markets creates a constant brain drain of skilled cybersecurity administrators [13]. Public agencies function as training grounds, where junior IT staff gain certifications and initial experience only to leave for private firms within twelve to eighteen months. This high turnover rate severely disrupts organizational continuity and prevents the accumulation of institutional memory, making it exceedingly difficult to build a sustained culture of security.

Finally, the administrative culture in many developing country agencies is characterized by a strong emphasis on compliance and hierarchical control [14]. In these environments, security is often treated as a checkbox exercise designed to satisfy external auditors or international treaty requirements rather than an operational priority. Bureaucratic silos prevent effective communication and coordination between different government agencies, making coordinated incident response extremely difficult. When a cyber incident occurs, the primary organizational response is often blame avoidance and information concealment, rather than transparent analysis and collective learning. This lack of transparency and collaboration directly undermines the foundational principles of institutional resilience.

3. Methodology and Field Study Design

3.1 Qualitative Field Study Approach

To capture the nuanced, socio-technical dynamics of cybersecurity capacity building, this research adopted a qualitative, multiple-case study research design. This approach is highly appropriate for investigating complex, real-world phenomena within their natural context, particularly where the boundaries between the phenomenon and the context are not clearly defined [15]. By focusing on multiple public agencies within a single developing country, the study was able to hold the macro-environmental variables constant (such as national laws, political stability, and general economic conditions) while systematically exploring how micro-level organizational variables influenced cybersecurity capacity and resilience.

The field research was conducted over an eighteen-month period, during which the primary researcher maintained active, direct engagement with the participating agencies. This prolonged engagement allowed for the triangulation of multiple data sources, including semi-structured interviews, direct field observations, internal administrative documents, and technical policy reviews [16]. This multi-method data collection strategy was essential for cross-referencing official administrative claims against the actual, operational practices observed on the ground.

3.2 Site Selection and Data Collection

Five distinct public sector agencies were selected for the study based on their criticality to national security, economic stability, and public service delivery. To protect the anonymity of the participating institutions and informants, the agencies are categorized and referred to by their functional mandates:

- Agency A: Ministry of Finance and Economic Planning (responsible for national financial transactions, budgeting, and revenue allocation).

- Agency B: Ministry of Health (responsible for national healthcare delivery, hospital networks, and public health databases).

- Agency C: Ministry of Information and Communications Technology (responsible for national digital infrastructure, e-government portal management, and telecommunications regulation).

- Agency D: Ministry of Interior and National Security (responsible for civil registration, border control coordination, and public safety databases).

- Agency E: National Revenue Authority (responsible for tax collection, customs clearance, and trade facilitation).

These agencies represent a diverse cross-section of technical maturity, budget availability, and threat exposure, providing a rich basis for comparative analysis [17]. Data collection involved fifty semi-structured interviews with key informants, including Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), system administrators, network engineers, compliance officers, and administrative directors [18]. Each interview lasted between sixty and ninety minutes, was conducted in English, and was recorded and transcribed with the explicit consent of the participants. The interview protocols were designed to explore the history of cybersecurity initiatives, procurement processes, staff recruitment and retention, incident response experiences, and inter-agency collaboration.

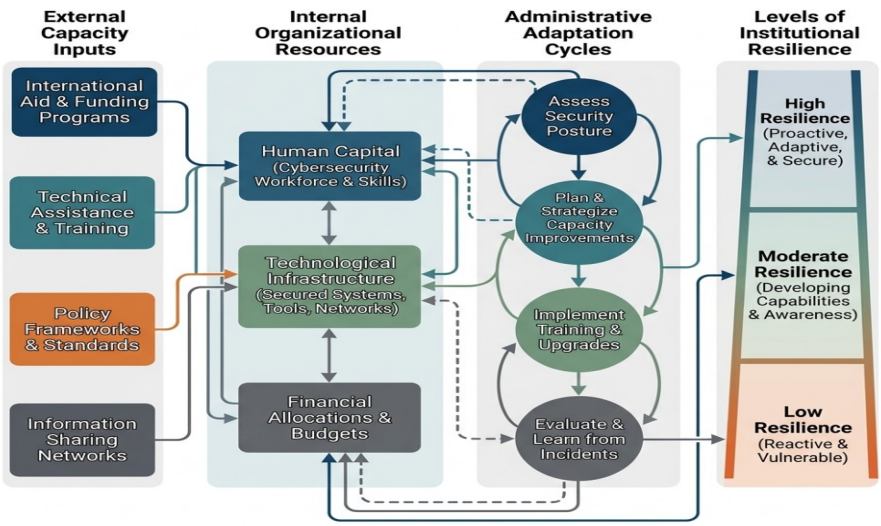

Figure 1: Conceptual Framework of Cybersecurity Capacity Building and Institutional Resilience

3.3 Analytical Framework

The collected qualitative data was analyzed using thematic analysis, utilizing a hybrid inductive-deductive approach [19]. The deductive coding structure was informed by the existing literature on capacity maturity models and institutional resilience, while inductive codes were allowed to emerge directly from the raw interview transcripts and field notes to capture contextual nuances specific to the developing country environment.

The analysis was structured around four primary thematic domains: resource configuration, human capital dynamics, administrative governance, and technical operationalization. Within these domains, researchers analyzed how specific capacity inputs (such as funding, training, and software) were transformed into organizational capabilities (such as threat detection, vulnerability management, and incident response). The triangulation of interviews with internal policy documents—such as national cybersecurity strategies, agency-level incident response plans, and IT audit reports—allowed for the identification of systemic disconnects between formal organizational policy and everyday security practices.

4. Field Study Observations and Analytical Results

4.1 Institutional Impediments and Resource Constraints

The field observations revealed that resource constraints in developing country public agencies are not merely a function of absolute financial scarcity, but are deeply linked to rigid, highly centralized budgetary and procurement processes. In all five analyzed agencies, budgeting for cybersecurity was characterized by extreme volatility and unpredictability. Unlike standard administrative operational costs, cybersecurity is rarely integrated as a recurring, dedicated line item in annual agency budgets. Instead, security expenditures are typically classified under general IT maintenance or treated as ad-hoc capital investments that require special, high-level administrative approvals.

This budgetary structure has direct operational consequences. For instance, in Agency A, despite its critical role in managing national financial transactions, the procurement of security patches and license renewals for critical database firewalls was frequently delayed by several months due to bureaucratic procurement bottlenecks. During these delay periods, systems were left running on expired subscription models without access to real-time threat intelligence updates, exposing critical transaction networks to known, exploitable vulnerabilities [20].

Table 1 provides a comparative overview of the baseline capacity metrics observed across the five participating agencies at the beginning of the study.

Table 1: Baseline Capacity Metrics Across Selected Public Sector Agencies

Agency Identifier	Annual Dedicated Cyber Budget	Ratio of Security Staff to Total Users	Incident Response Plan Status	Patch Management Frequency
Agency A	Under 2 percent	1 to 450	Outdated draft format	Semi-annual manual execution
Agency B	Under 1 percent	1 to 1200	Non-existent	Ad-hoc after major failure
Agency C	Approximately 5 percent	1 to 150	Formally approved	Monthly automated cycle
Agency D	Approximately 3 percent	1 to 350	Restrictive classified draft	Quarterly manual execution
Agency E	Approximately 4 percent	1 to 200	Formally approved	Bi-monthly semi-automated

As shown in Table 1, only Agency C and Agency E maintained formally approved incident response plans and automated patch management processes, reflecting their stronger alignment with international standards. In contrast, Agency B, which manages critical national health registries and hospital infrastructure, operated with less than one percent of its IT budget dedicated to security, a highly deficient staff-to-user ratio, and no formal incident response plan.

4.2 Technical Capacity and Human Capital Gaps

The most acute challenge identified across all five field sites was the systemic difficulty of retaining qualified cybersecurity personnel. System administrators and security engineers reported that while they frequently received valuable, highly specialized training through donor-funded capacity-building programs, this newly acquired expertise immediately made them highly competitive in the private market [21]. Within months of completing advanced certifications (such as CISSP, CEH, or OSCP) funded by public money, a significant percentage of staff resigned to accept positions in private banks, telecommunications companies, or multinational consulting firms where salaries were three to five times higher than civil service pay scales.

This phenomenon was particularly pronounced in Agency C and Agency E. In Agency C, which acts as the central technical support hub for other government ministries, the average tenure of a certified security analyst was only fourteen months. The CISO of Agency C noted that the agency was effectively functioning as a free training academy for the private sector, resulting in a continuous state of talent drain that severely disrupted operational continuity.

Furthermore, this high turnover rates led to a heavy reliance on external, third-party contractors and vendors to manage core security infrastructure [22]. In several agencies, critical firewall configurations, security information and event management (SIEM) systems, and vulnerability assessment tools were fully managed by external system integrators. This created a dangerous state of dependency. Internal IT staff lacked the technical capabilities to monitor or audit the work of these contractors, leading to vendor lock-in, inflated service costs, and a complete lack of internal visibility into the actual security posture of their networks.

4.3 Administrative Practices and Policy Alignment

The administrative culture within the studied agencies frequently prioritized formal compliance and hierarchy over operational agility. This dynamic was particularly visible in how cyber security policies were developed and enforced. In many cases, national cybersecurity policies and agency-level guidelines were drafted by international consultants who copied and pasted standard templates from developed-world frameworks [23]. These policies were often highly unrealistic for local administrative contexts.

For example, in Agency D, the formal security policy mandated that all software patches must be thoroughly tested in an isolated staging environment that mirrored the production network before deployment. However, the agency did not have the financial or physical resources to maintain a duplicate staging environment. Consequently, system administrators were forced to choose between violating formal policy by patching production systems directly, or remaining compliant with the policy by not applying patches at all. In practice,

administrators routinely chose the latter, leaving critical civil registration systems unpatched for years to avoid bureaucratic audits and potential administrative penalties.

Table 2 highlights the measured impact of targeted capacity interventions—such as customized staff training, the introduction of simplified local standard operating procedures, and the establishment of basic monitoring tools—conducted during the field study.

Table 2: Impact of Targeted Capacity Interventions on Resilience Indicators

Agency Identifier	Mean Time to Detect Incidents (Pre-Intervention)	Mean Time to Detect Incidents (Post-Intervention)	Patch Compliance Rate (Pre-Intervention)	Patch Compliance Rate (Post-Intervention)
Agency A	42 days	8 days	35 percent	78 percent
Agency B	115 days	34 days	12 percent	45 percent
Agency C	4 days	1 day	88 percent	96 percent
Agency D	68 days	14 days	22 percent	60 percent
Agency E	12 days	3 days	71 percent	89 percent

The data in Table 2 demonstrates that even basic, contextualized capacity interventions can yield substantial improvements in key security metrics. By introducing simplified, locally feasible standard operating procedures and providing tailored operational training to existing staff, the mean time to detect cyber security incidents was significantly reduced across all agencies, and patch compliance rates improved substantially, even in highly resource-constrained environments like Agency B.

5. Strategic Discussion and Recommendations

5.1 Synthesis of Findings

The empirical findings from this eighteen-month field study challenge several mainstream assumptions embedded in standard cybersecurity capacity-building methodologies. First, the study demonstrates that the primary bottleneck to effective cybersecurity in developing country agencies is rarely a lack of advanced technical tools, but rather a lack of administrative and institutional structures capable of supporting those tools over time [24]. The common donor practice of donating sophisticated security software without addressing underlying procurement inefficiencies, severe civil service wage disparities, and rigid bureaucratic cultures represents an unsustainable model that leads to widespread waste and persistent vulnerability.

Second, the study highlights the critical distinction between passive compliance and active, adaptive institutional resilience. Many public agencies have invested substantial effort in drafting comprehensive policy documents to satisfy external compliance requirements. However, these documents often remain disconnected from the actual day-to-day operational realities of the IT staff, leading to a false sense of security among executive leadership. True resilience requires shifting the organizational culture from paper-based compliance to continuous, active risk management, where security policies are iteratively adapted to match the technical, financial, and human resources actually available to the agency.

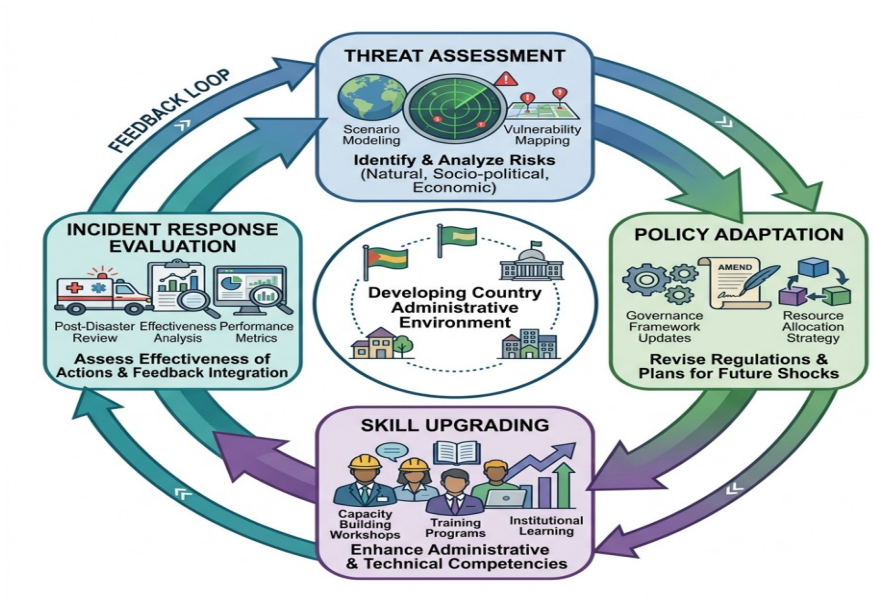

Figure 2: Operational Cycle for Iterative Institutional Resilience

5.2 A Framework for Tailored Cybersecurity Capacity Building

To address these deep-seated structural challenges, this paper proposes a tailored, three-tiered framework for cybersecurity capacity building specifically optimized for resource-constrained public sector environments in developing nations. This framework is designed to move agencies away from standard, high-cost models and toward sustainable, resilient security postures.

The first tier of the framework, Foundation, focuses on establishing basic operational hygiene and reducing external dependencies. Rather than procuring expensive, proprietary security platforms that require high recurring licensing fees, agencies should prioritize open-source security tools and focus on building strong baseline capabilities in identity and access management, asset inventory, and simplified patch management.

The second tier, Integration, addresses the human capital challenge by restructuring how cybersecurity roles are positioned within the civil service. To combat the constant drain of talent to the private sector, government agencies must establish specialized technical career paths that offer non-monetary incentives, such as funded training opportunities linked to mandatory public service periods, flexible working arrangements, and clear opportunities for rapid internal promotion [25]. Furthermore, knowledge transfer must be institutionalized through structured peer-to-peer mentoring programs, ensuring that the departure of a single trained staff member does not result in the complete loss of a specific security capability.

The third tier, Adaptation, focuses on building continuous, threat-informed administrative feedback loops. This involves establishing local, agency-level security working groups that meet regularly to review incident logs, share intelligence, and update standard operating procedures. These working groups must operate with a mandate of transparent communication and blame-free post-incident reviews, transforming security failures into valuable organizational learning opportunities.

5.3 Enhancing Institutional Resilience

Cultivating long-term institutional resilience also requires fundamental reforms at the macro-policy level. National governments must recognize that cybersecurity is a critical component of national security and public service delivery, requiring stable, recurring funding streams that are legally protected from annual budgetary volatility [26]. Procurement laws must be modernized to allow for the rapid acquisition of emergency security patches, hardware replacements, and external specialized support during active security incidents, bypassing the slow, bureaucratic bidding processes that currently paralyze emergency responses.

Furthermore, international development partners and donor agencies must shift their funding paradigms. Rather than measuring the success of capacity-building projects by the volume of hardware deployed or the number of policies drafted, project evaluations must focus on long-term sustainability metrics. These should

include the percentage of systems maintained by internal staff after three years, the continuous operation of monitoring tools without active external funding, and the demonstrable improvement of key operational metrics such as mean time to detect and mean time to respond to incidents. By aligning external support with the practical, long-term operational needs of local agencies, the international community can help build genuine, self-sustaining institutional resilience across the developing world.

6. Conclusion

6.1 Summary of Contributions

This paper has presented a comprehensive, empirically rich field study of cybersecurity capacity building and institutional resilience within the public sector agencies of a developing country. By conducting a detailed, multi-site analysis of five critical government ministries and agencies over an eighteen-month period, this research has exposed the systemic socio-technical and structural challenges that frequently undermine standardized, Western-centric capacity-building initiatives [27]. The study has documented how rigid procurement cycles, acute human capital flight, vendor dependencies, and paper-based compliance cultures interact to create persistent states of cyber vulnerability.

By shifting the analytical focus from technical infrastructure procurement to administrative adaptability and sustainable human resource development, this study has made a significant contribution to the fields of public administration and cybersecurity governance. The empirical findings demonstrate that targeted, low-cost interventions—such as customized training, simplified standard operating procedures, and the utilization of open-source tools—can yield dramatic improvements in critical operational security metrics, even in severely resource-constrained environments.

6.2 Policy Implications and Future Directions

The policy implications of this research are highly relevant for national governments, international development partners, and public sector administrators throughout the developing world. For national governments, the study underscores the urgent need to reform civil service hiring guidelines to create specialized, sustainable career paths for cybersecurity professionals, and to modernize procurement laws to support dynamic, continuous vulnerability management. For international donor agencies, the findings demand a fundamental shift away from short-term, donor-driven technology acquisitions and toward long-term, context-aware partnerships that prioritize local ownership and administrative adaptation.

Future research in this domain should focus on expanding the geographic scope of this field study to conduct comparative, cross-national analyses of cybersecurity capacity building across different developing regions. Additionally, longitudinal quantitative modeling of human capital retention strategies within public sector IT departments would provide valuable, data-driven insights into the most effective mechanisms for preserving native technical capabilities in the face of intense private sector competition. Ultimately, securing the digital future of developing nations requires moving beyond generic, borrowed frameworks and embracing localized, resilient, and adaptive socio-technical strategies that reflect the practical realities of the public administrators tasked with protecting them.

References

1. Viana, J.; Farkhari, H.; Gil Jiménez, V.P. Securing 5G and Beyond-Enabled UAV Links: Resilience Through Multiagent Learning and Transformers Detection. IEEE Access 2025, 13, 153993–154007.

2. Liu, C.; Zhao, J.; Li, J.; Wang, D.; Yu, F.R. UAV Aided Integrated Sensing, Communication and Computing: Optimization via Federated Learning. IEEE Trans. Veh. Technol. 2025, 75, 6045–6058.

3. Yang, J. On the “Five W’s Service” in socialized child care service for infants and toddlers under 3 years of age. Fujian Forum (Humanit. Soc. Sci. Ed.) 2020, 167–177.

4. Dubey, M.; Singh, A.K.; Mishra, R. AI Based Resource Management for 5G Network Slicing: History, Use Cases, and Research Directions. Concurr. Comput. Pract. Exp. 2025, 37, e8327.

5. Di, Z.; Zhong, Z.; Pengfei, Q.; Hao, Q.; Bin, S. Resource Allocation in Multi-User Cellular Networks: A Transformer-Based Deep Reinforcement Learning Approach. China Commun. 2024, 21, 77–96.

6. Yue, J.; Fan, X. China’s child care policy system: Review, reflection and reconstruction. China Soc. Sci. 2018, 92–111+206.

7. Qi, J.; Zhang, H.; Qi, X.; Peng, M. Deep Reinforcement Learning Based Hopping Strategy for Wideband Anti-Jamming Wireless Communications. IEEE Trans. Veh. Technol. 2023, 73, 2131–2144.

8. Ma, W.; Lin, B.; Pan, H.; Sun, G.; Shi, E.; An, J.; Yuen, C. SIM-Assisted Secure Mobile Communications via Enhanced Proximal Policy Optimization Algorithm. IEEE Trans. Wirel. Commun. 2026, 25, 11964–11979.

9. Wara, N.; Paul, A.; Singh, K.; Kaushik, A.; Shin, W. Multi-Agent PPO-Based Resource Optimization for Full-Duplex RIS-Aided NOMA-ISAC Systems. IEEE Open J. Commun. Soc. 2025, 6, 9802–9820.

10. Xie, W.; Yang, H.; Xiong, Z. Resource Allocation for UAV-Assisted Anti-Jamming Semantic D2D Networks: A Graph Reinforcement Learning Approach. Comput. Netw. 2025, 269, 111463.

11. Sha, S.; Liu, Y.; Huo, B. Dynamic Proximal Policy Optimization: Enhancing PPO with Adaptive Entropy and Smooth Clipping. Neurocomputing 2026, 674, 132861.

12. Ahmed, S. (2004). The cultural politics of emotion. Routledge.

13. Lin, M.; Wang, Q. Center-based childcare expansion and grandparents' employment and well-being. Soc. Sci. Med. 2019, 240, 112547.

14. Asemian, G.; Amini, M.; Kantarci, B. Anti-Jamming Task Scheduling in MEC-O-RAN With Hierarchical DRL and Transformer-Based Control. IEEE Internet Things J. 2026, 13, 7714–7729.

15. Svara, J.H.; Watt, T.C.; Jang, H.S. How are US cities doing sustainability? Who is getting on the sustainability train, and why? Cityscape 2013, 15, 9–44.

16. Raja, G.; Sanjeev, A.; Ravishankar, K.; Arunachalam, K. TRIP-B5G: Traffic Classification and Resource Allocation Using Intelligent PPO in B5G O-RAN. In Proceedings of the 2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2026; pp. 1–4.

17. Foerster, J.N.; Assael, Y.M.; de Freitas, N.; Whiteson, S. Learning to Communicate with Deep Multi-Agent Reinforcement Learning. In Advances in Neural Information Processing Systems 29 (NeurIPS 2016), Barcelona, Spain, 5–10 December 2016; Curran Associates, Inc.: Red Hook, NY, USA, 2016; pp. 2137–2145.

18. Yu, C.; Velu, A.; Vinitsky, E.; Gao, J.; Wang, Y.; Bayen, A.M.; Wu, Y. The Surprising Effectiveness of PPO in Cooperative, Multi-Agent Games. In Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks (NeurIPS 2022), New Orleans, LA, USA, 28 November–9 December 2022; Neural Information Processing Systems Foundation, Inc.: La Jolla, CA, USA, 2022.

19. Song, J.; Gao, Y.; Wu, D.; Zhou, L. Adaptive Live Tactile Streaming with Scalable Coding for Immersive Communications. IEEE Trans. Mob. Comput. 2026, 25, 5133–5145.

20. Shang, C.; Yu, J.; Thai Hoang, D. Energy-Efficient and Intelligent ISAC in V2X Networks with Spiking Neural Networks-Driven DRL. IEEE Trans. Wirel. Commun. 2026, 25, 1182–1195.

21. Markets and Markets 6G Market Size & Outlook, 2030–2036. 2025. Available online: https://www.marketsandmarkets.com/Market-Reports/6g-market-213693378.html (accessed on 24 June 2026).

22. Kahraman, İ.; Köse, A.; Koca, M.; Anarim, E. Age of Information in Internet of Things: A Survey. IEEE Internet Things J. 2024, 11, 9896–9914.

23. Xu, J.; Zhao, Z.; Wang, L.; Zhang, Y. A Novel Deep Reinforcement Learning Architecture for Dynamic Power and Bandwidth Allocation in Multibeam Satellites. Acta Astronaut. 2023, 204, 73–82.

24. Sellnow, T. L., Ulmer, R. R., Seeger, M. W., & Littlefield, R. S. (2018). Effective risk communication (3rd ed.). Springer.

25. Wang, X.; Wang, J.; Xu, Y.; Chen, J.; Jia, L.; Liu, X. Dynamic Spectrum Anti-Jamming Communications: Challenges and Opportunities. IEEE Commun. Mag. 2020, 58, 79–85.

26. Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. Annual Review of Psychology, 66, 799–823.

27. Yanow, D. (2000). Conducting interpretive policy analysis. SAGE.