iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

ENHANCING CYBER RESILIENCE IN GOVERNMENT INSTITUTIONS, A COMPARATIVE ANALYSIS OF POLICY FRAMEWORKS ACROSS DEVELOPING AND DEVELOPED NATIONS

Md Sazzad Hossain[1]
Email: mhossain@g.emporia.edu
Orchid ID: 0009-0009-4948-1179
Affiliation: School of Business and Technology, Emporia State University

Habib Md Hasan[2]
Email: hmdhasan@g.emporia.edu
Orchid ID: 0009-0002-2147-2253
Affiliation: School of Business and Technology, ESU

Fatema Akter[3]
Email: fakter@g.emporia.edu
Orchid ID: 0009-0004-1150-0243
Affiliation: School of Business and Technology, Emporia State University

ABSTRACT
Government institutions increasingly rely on digital platforms to deliver essential public services, yet this dependence has expanded the attack surface and amplified the operational, legal, and reputational consequences of cyber incidents. Cyber resilience understood as the capacity to anticipate, withstand, recover from, and adapt to cyber disruptions has therefore become a strategic public-sector requirement rather than a purely technical concern. This paper examines how cyber resilience is operationalized through governmental policy frameworks and governance arrangements, and it provides a comparative analysis of approaches adopted across developed and developing nations. Using a structured comparative policy analysis, the study synthesizes evidence from national cybersecurity strategies, e-government cybersecurity policy literature, and cyber capacity-building research to evaluate differences in regulatory completeness, institutional accountability, implementation mechanisms, and capability development. The analysis indicates that developed-country frameworks tend to demonstrate clearer governance structures, more enforceable compliance requirements, and more mature institutional coordination, while developing-country frameworks often face constraints related to capacity, fragmented accountability, and uneven implementation despite increasing strategic attention to national cyber resilience. The paper contributes a policy-comparison lens that links governance design, legal and regulatory readiness, and capacity-building measures to practical resilience outcomes in government institutions. It concludes by outlining policy directions for strengthening resilience, including more coherent governance models, targeted capacity development, and improved alignment between national strategies and operational readiness in public-sector environments.

Keywords:
Cyber resilience; government institutions; cybersecurity policy; e-governance; comparative analysis; developed and developing nations

INTRODUCTION

i. Background and Global Rise of Cyber Threats to Government Institutions

The fast digitization of the government services has altered the way the public institutions provide the governance, handle information and their communication with citizens. Online public service portals, digital identity systems, e-government platforms, and interconnected critical information infrastructures have become the key to the current operations of the state. Nevertheless, such a digital change has also made governments more vulnerable to cyber attacks, such as data breaches, ransomware, service outages, and massive cyber

ISSN: 2456-9348
Impact Factor: 5.004

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

espionage. According to the recent research, it has been shown that government institutions are one of the most commonly targeted organizations because of the sensitivity of state information, the symbolism of state institutions, and the possibility of disrupting the society as a result of cyber attack (Singh et al., 2022; Qudus, 2020).

Table 1: Key Differences in Cyber Resilience Policy Frameworks

Criteria	Developed Nations	Developing Nations
Cyber Resilience Framework	Well-established, with comprehensive national strategies	In early stages, often with fragmented frameworks
Policy Enforcement	Strong enforcement mechanisms, regulatory agencies	Weak enforcement, inconsistent implementation
Technological Adaptation	High adaptability to emerging technologies (AI, Blockchain)	Slow adaptation, reliance on outdated technologies
Institutional Capacity	Well-funded, with skilled cybersecurity personnel	Limited funding, shortage of skilled personnel
Public-Private Collaboration	Strong collaboration between sectors	Limited collaboration, reliance on external aid
Global Cooperation	Active in international cybersecurity coalitions	Limited participation in global cybersecurity efforts

Cyber threats to government institutions have taken a different form across the world and now they are systemic risks with national security, economic stability, and trust implication to the population. The sophistication of the threat actors such as state-sponsored organizations and organized cybercriminal groups has also escalated the problem of cybersecurity governance in the public sector (Calderaro and Craig, 2020; Choucri et al., 2014). Consequently, governments are increasingly being pressured to transcend conventional methods of cybersecurity management into more panoramic cyber resilience approaches that guarantee that the public functions continue even when the circumstances are hostile.

ii. Importance of Cyber Resilience in Public-Sector and E-Government Systems

The concept of cyber resilience to the public sector is not only about preventing cyberattacks but also about preparedness, response, recovery and adaptive learning as part of institutional systems. The governmental establishments should not shut down vital systems despite the attacks, especially on the availability of such services as healthcare, taxation, citizen safety, and online governance. Researchers are becoming more keen to point out that cyber resilience is not a technological defense, but rather a socio-technical construct that is influenced by policy structures, governance frameworks, institutional coordination, and human capacity (Panda and Bower, 2020; Singh et al., 2022).

Cyber resilience is particularly important in e-government situations since the access to services and integrity of data have a direct impact on citizen trust and legitimacy of the administration. The lack of resilience may also lead to a long service downtime, exposure of sensitive personal data, and the loss of trust in digital governance

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

initiatives (Krishna and MP, 2021; Younus et al., 2022). As a result, cyber resilience is now one of the key goals of national cybersecurity policies and governmental digital transformation programs.

iii. Inequality in the Cyber Resilience Capacity between Developed and Developing countries

Although cyber resilience is currently viewed as a strategic priority globally, there is still large gap between developed and developing countries, in institutional capacity, regulatory maturity, and operational preparedness. Cybersecurity policies, enforcement, and investments on cyber capacity building within governmental structures are usually more developed in developed countries (Odebade & Benkhelifa, 2023; Ali et al., 2022). Conversely, the developing countries tend to be constrained within their structures, including the lack of technical skills, divided governance systems, and a lack of financial and institutional capabilities (Peter, 2017; Sarker et al., 2019).

Such differences are further aggravated by the difference in legal structures, inter agency cooperation and access to sophisticated technologies. Although most of the developing nations have embraced national cybersecurity strategy, there are still wide gaps in implementation especially at the operational level of the public institutions (Saleem et al., 2024; Sikder and Islam, 2021). Such differences are crucial in comprehending how to develop policy frameworks that will be context-sensitive and be in a position to enhance cyber resilience in various governance frameworks.

iv. Problem Statement and Gap in Research

Despite the increasing literature on national cybersecurity policies and cyber governance, the available research tends to concentrate on particular countries or regions and comparisons between developed and developing countries are not often performed in a systematic manner. Furthermore, a significant part of the studies focuses on cybersecurity measures as opposed to the wider cyber resilience performance in the governmental institutions. An integrative comparative analysis has not been done yet to connect the policy designing, governance processes, and institutional capacity to the resilience performance in the public sector (Hossain et al., 2021; Panabergenova and Umarova, 2021).

This divide does not allow policymakers to point to any best practices that can be transmitted or used and does not allow a clear picture of how contextual elements define the success of cybers resilience policy. To eliminate this gap, it is necessary to have an organized comparative research that will evaluate policy frameworks in different national settings and pay a particular attention to government institutions.

v. Research Aim and Objectives

This research is mainly focused on exploring the function of cyber resilience as an integrated aspect of governmental policy frameworks and also evaluating the effectiveness of these frameworks relative to the developed and developing countries. In order to fulfill this purpose, the research will have the following purposes:

- To examine the fundamental elements of cyber resilience policies that are used in government institutions.
- To draw comparisons between governance structures, legal provisions and mechanisms of implementation in both developed and developing national settings.
- To determine the institutional and policy-level issues that determine the results of cyber resilience in the public sector.
- To obtain insights on policy that can guide the progress of resilience in resource limited governance space.

II. LITERATURE REVIEW

a. Cyber Resilience in Government and Public-Sector settings Definitional Cyber Resilience

The concept of cyber resilience in government institutions is increasingly developed as the capability of the systems in the public sector to recognize cyber threats, survive the disruptive incident, restore functions, and make decisions regarding the future risks. However, in contrast to classic cybersecurity that focuses on prevention and security, cyber resilience focuses on governance and service continuity amidst unfavorable cyber conditions (Singh et al., 2022; Panda and Bower, 2020). When embracing the concept of resilience in the setting of a government agency, the concept is multidimensional since it includes technical protection, agency preparedness, legal obligations, coordination of governance, and human preparedness.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Government organisations are elaborate socio-technical systems that have flow-on consequences of failure through to not only social but also essential infrastructure. Accordingly, cyber resilience is positioned as a challenge to both IT and governance and policies that necessitates forming links between national policies and institutional activities (Qudus, 2020; Choucri et al., 2014).

b. Government Institution Cybersecurity Governance and Policy Frameworks

The concept of cybersecurity governance describes the models, procedures, and the elements of accountability that governments establish, monitor, and put into practice to create and manage policies concerning cybersecurity and resilience. The system of good governance is often characterized by effective systems of roles, establishing control, prescribing of norms of standards and compliance, and coordinating between ministries and agencies (Calderaro and Craig, 2020).

Research points to the fact that poor governance, in the form of divided power, a lack of mandate, and overall ineffective enforcement actions, is a big impediment to cyber resilience in government organizations, despite the existence of formal policies (Panabergenova and Umarova, 2021; Sarker et al., 2019). On the other hand, excellent governance modalities incorporate cybersecurity in their wider public-sector risk management and national security agendas, which increases the resilience of institutions.

c. National Cybersecurity Strategies: Scope, Maturity and Mechanisms of enforcement

National cybersecurity strategies are policy tools that are foundational in shaping the cyber resilience in the government institutions. Comparative studies show that the extent and rating of these strategies is highly diverse especially among developed and developing countries (Odebade & Benkhelifa, 2023). The mature strategies normally have clear goals, objectives, stipulate resilience-oriented priorities, assign the institutional roles, and provide mechanisms to monitor and enforce.

Nevertheless, some of the researches observe that the presence of a national strategy does not necessarily amount to good performance. In most settings, enforcement activities are poor, and institutional strengths are limited in order to implement policy guidelines (Saleem et al., 2024; Ali et al., 2022). This lack of consistent correlation between the strategic intent and the operational implementation is one of the chronic issues of enhancing cyber resilience.

d. E-Government Systems Cyber Resilience

E-government systems increase the significance of cyber resilience owing to its contribution towards service delivery, citizen interactions, and handling of public data. Any interference with the digital government systems may hinder continuity in the administration and destroy the confidence of people (Krishna & MP, 2021; Younus et al., 2022).

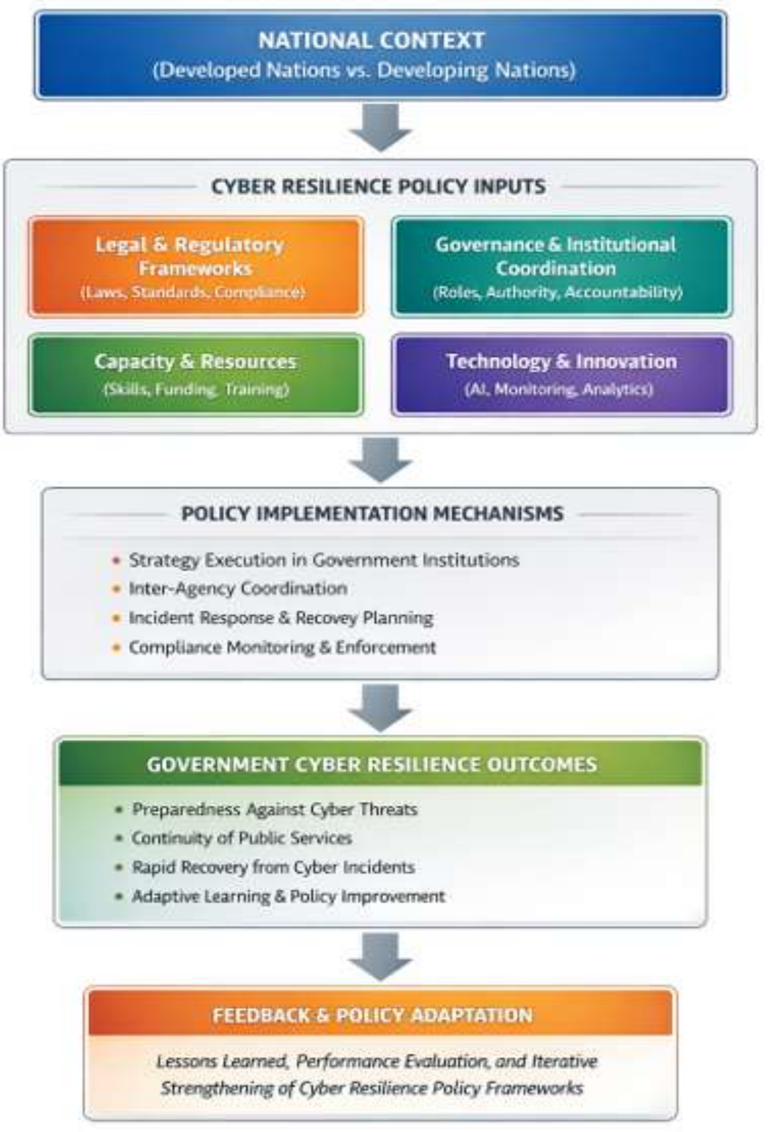
The literature underlines that effective e-government systems need to be supported with policy, institutional coordination and sustained risks assessment. Although developed countries tend to introduce the resilience need into the digital governance system, developing countries usually face difficulties in fragmented implementation and insufficient technical capabilities (Hossain et al., 2021; Singh et al., 2022).

e. Comparative Lessons of Developed Countries

Studies conducted in developed countries affirm that they have elaborate cybersecurity governance frameworks, sound regulatory regime, and sustained institutional capacity investments. The former countries prefer resilience-related practices that entail redundancy, incident response, cross-agency plans, and advanced monitoring practices (Ali et al., 2022; Odebade and Benkhelifa, 2023).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Figure 1: Conceptual Framework for Comparing Cyber Resilience Policy Frameworks in Government Institutions



III. METHODOLOGY

a). Research Design: Qualitative Comparative Policy Analysis

This paper will take a qualitative comparative policy analysis as a means of exploring the conceptualization, management and application of cyber resilience in government organisations in both developed and developing countries. The approach that best fits in this study is the qualitative comparative analysis given that cyber resilience is entrenched in multi-tiered governance frameworks that entail legal, institutional, and socio-technical aspects and not simply measurable variables. Current research is focused on qualitative methods to study the nature of policy intent, institutional structures, and dynamics of implementation in various national settings in efforts to examine national cybersecurity strategies and cyber governance concerning the public sector (Odebade and Benkhelifa, 2023; Calderaro and Craig, 2020).

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Table 2: Comparative Overview of Cyber Resilience Policy Frameworks in Government Institutions

Dimension	Developed Nations	Developing Nations
Policy Scope and Strategic Orientation	Cyber resilience policies are typically comprehensive, explicitly integrated into national cybersecurity strategies, and aligned with broader national security and digital governance agendas. Policies emphasize prevention, response, recovery, and adaptive learning.	Policies often focus primarily on cybersecurity protection and compliance, with cyber resilience concepts emerging but not always explicitly operationalized across government institutions.
Legal and Regulatory Frameworks	Strong legal foundations with enforceable cybersecurity laws, mandatory standards, and clear compliance requirements for government institutions. Regulatory oversight mechanisms are well established.	Legal frameworks exist but may be fragmented, outdated, or weakly enforced. Regulatory mandates are often present but lack consistent institutional implementation.
Governance and Institutional Coordination	Clearly defined governance structures with centralized coordination bodies, well-defined roles, and effective inter-agency collaboration mechanisms.	Governance responsibilities are frequently dispersed across multiple agencies, leading to overlaps, coordination challenges, and unclear accountability structures.
Institutional Capacity and Resources	High levels of technical expertise, sustained investment in cyber capacity building, and dedicated resources for resilience planning and incident response.	Limited technical skills, constrained funding, and reliance on external support or donor-driven initiatives hinder institutional capacity development.
Technology and Innovation Integration	Advanced use of monitoring tools, analytics, and emerging technologies, including AI-driven systems, to enhance situational awareness and adaptive response.	Adoption of advanced technologies is uneven and often constrained by financial, infrastructural, and skills limitations.
Implementation and Enforcement	Strong alignment between policy design and operational execution, supported by regular audits, performance evaluations, and enforcement mechanisms.	Significant gaps between policy intent and implementation, with limited monitoring and weak enforcement at the institutional level.
Overall Cyber Resilience Outcome	Generally higher levels of preparedness, service continuity, and recovery capability across government institutions.	Variable and often lower resilience outcomes, with progress dependent on institutional capacity and governance maturity.

b). Criteria of Case Selection

Cases were chosen to be, one representative of developed and another one of developing national settings, which is consistent with comparative cybersecurity policy research. The main selection criteria were as follows: (i) the presence of a formal national cybersecurity strategy or policy framework, which applies to government institutions, (ii) the degree of e-government development and (iii) a documented involvement in cyber resilience or cybersecurity governance programs.

c). Data Sources

The discussion is based solely on secondary qualitative data obtained by referring to authoritative sources on policies and governance. These consist of national cybersecurity strategies, e- government cybersecurity policies, legal and regulatory instruments and government policy documents that have been made public and discussed in the reviewed literature. These documents were contextualized and interpreted using peer-reviewed comparative studies and policy analysis, especially in the case when the relevant direct policy text was not available.

d). Analytical Framework and Comparison Standards

The conceptual framework, which will be used to do the comparative analysis, is illustrated in Figure 1 and presents evaluation in four main policy areas, including legal and regulatory frameworks, governance and institutional coordination, capacity and resources, and technology and innovation. Similar to these dimensions

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

are commonly mentioned determinants of cyber resilience in government institutions (Singh et al., 2022; Qudus, 2020)

IV. DISCUSSION

a. Comparative policy performance of cyber resilience developed and developing countries

This part will explain the efficacy gaps between cyber resilience measures, which will be based on the strengths and weaknesses evident in different countries. It makes comparisons of the effectiveness of these strategies in response to arising cyber threats, and the agility and adaptability of government systems are considered.

b. Institutional capacity and governance institutions

In this case, it would explore the role of the institutional arrangements of government agencies in ensuring effective or ineffective implementation of cyber resiliency policies. As an illustration, the developed countries could possess stronger systems of governance that would allow the policy to be implemented, whereas developing countries could struggle with such problems as insufficient resources and shortage of well-qualified professionals.

c. Implementation of the policies and role of international co-operation

Another element of cyber resilience that is important is the implementation of cybersecurity policies. This section will provide a comparison of the policy enforcement strategies of the various countries, both locally and internationally using international cooperation as a tool to curb the cyber threats.

d. Information Technology adaptation and e-governance systems

This section discusses the role of government in developed countries and developing countries which have now adopted technology advancement in their e-governance systems to enhance cyber resilience. It compares the willingness of countries to incorporate new technologies and their role in cybersecurity.

e. Challenges and policy gaps

A fundamental part of the discussion is the identification of the gaps in the current policies and how such issues as underreporting of cyber incidents, poor partnership between the government and business, and the obsolete legal framework impede the process.

V. CONCLUSION

This study has provided a comprehensive comparative analysis of cyber resilience policy frameworks in government institutions across both developed and developing nations. By examining the varying national contexts, institutional capacities, and governance structures, the research highlights significant disparities in the effectiveness of cyber resilience strategies. Developed nations, with their robust institutional frameworks, advanced technological capabilities, and stronger policy enforcement mechanisms, are better equipped to address the complex and evolving nature of cyber threats. In contrast, developing nations face several challenges, including limited resources, less mature policy frameworks, and institutional constraints, which hinder their ability to effectively mitigate cyber risks. The analysis underscores the need for tailored, context-specific approaches to strengthening cyber resilience in government institutions. While developed nations can focus on refining their existing policies and integrating emerging technologies, developing nations must prioritize building institutional capacity, improving public-private partnerships, and ensuring the continuous adaptation of their legal and policy frameworks. Moreover, the study identifies key policy gaps and implementation challenges, such as the lack of adequate cybersecurity training, underreporting of cyber incidents, and weak enforcement mechanisms. Based on the findings, the research advocates for a collaborative, international approach to cybersecurity governance, where countries share best practices, harmonize policies, and work together to combat the global nature of cyber threats. Future efforts should focus on enhancing policy coherence, fostering international cooperation, and investing in the capacity building of both government institutions and local communities to create a more resilient and secure digital environment. Ultimately, the advancement of cyber resilience policies will not only safeguard national security but also support the sustainable growth of e-governance systems and digital infrastructures across the globe.

REFERENCES

1) Singh, P., Sirpal, S., & Pal, O. (2022). Cyber resilience in e-governance: A review of strategies, challenges, and directions. *Internet of Things*, 101702. https://doi.org/10.1016/j.iot.2025.101702
2) Odebade, A. T., & Benkhelifa, E. (2020). A comparative study of national cyber security strategies of ten nations. *arXiv preprint arXiv:2303.13938*. https://doi.org/10.48550/arXiv.2303.13938
3) Sikder, A. S., & Islam, M. R. (2021). Enhancing Cyber-Resilience within Bangladesh's Legal Framework: Evaluating Preparedness and Mitigation Strategies against Technologically-Driven

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

Threats.: Enhancing Cyber-Resilience within Bangladesh's Legal Framework. *International Journal of Imminent Science & Technology.*, *1*(1), 40-57. https://doi.org/10.70774/ijist.v1i1.6

4) Sarker, K., Rahman, H., Rahman, K. F., Arman, M. S., Biswas, S., & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategy of Bangladesh. *arXiv preprint arXiv:1905.00299*. https://doi.org/10.48550/arXiv.1905.00299
5) Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507-518. https://doi.org/10.1108/IJDRBE-07-2019-0046
6) Saleem, B., Ahmed, M., Zahra, M. *et al.* A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: a case study of Pakistan to bridge the gap. *Int. Cybersecur. Law Rev.* **5**, 533–561. https://doi.org/10.1365/s43439-024-00128-y
7) Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2021). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501
8) Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, *3*(3), 200-231. **https://doi.org/10.3390/digital3030014**
9) Manurung, H., & Madeleine, H. C. (2021). Exploring AI techniques for improving IT system resilience and fault tolerance. ResearchGate. https://doi.org/397786244
10) Brooklyn, A., Ibrahim, A., & Madeleine, H. C. (2025). AI-driven approaches to identifying systemic problems in large-scale IT infrastructure. ResearchGate. https://doi.org/397786243
11) James, M., & Madeleine, H. C. (2020). Data-driven root cause analysis using AI in cloud-based IT infrastructures. ResearchGate. https://doi.org/397786245
12) Harper, S., & Madeleine, H. C. (2021). Microbiome dysbiosis, immune dysfunction, and behavioral manifestations in autism spectrum disorders. ResearchGate. https://doi.org/397786246
13) Evelyn, M., & Madeleine, H. C. (2022). Behavioral manifestations in autism spectrum disorders: Parents of children with developmental disabilities. ResearchGate. https://doi.org/397786247
14) Evelyn, M., & Madeleine, H. C. (2019). Behavioral manifestations in autism spectrum disorders: Parents of children with developmental disabilities. ResearchGate. https://doi.org/397786248
15) Evelyn, M., & Madeleine, H. C.. Coping mechanisms among parents of children with developmental disabilities and psychological resilience. ResearchGate. https://doi.org/397786249
16) Evelyn, M., & Madeleine, H. C. (2025). Psychological resilience and coping mechanisms among parents of children with developmental disabilities. ResearchGate. https://doi.org/397786250
17) Grace, C., & Madeleine, H. C. (2025). Early childhood infections and neurodevelopmental disorders: Focus on autism spectrum disorder. ResearchGate. https://doi.org/397786251
18) Max, T., & Madeleine, H. C. (2025). Governance, security, and ethical implications of AI in modern enterprises. ResearchGate. https://doi.org/397786252
19) Logan, J., & Madeleine, H. C. (2025). Real-time decision-making frameworks using edge-AI for autonomous industrial systems. ResearchGate. https://doi.org/397786253
20) Thomas, E., & Madeleine, H. C. (2025). AI-driven optimization in smart manufacturing: Integrating predictive maintenance, edge computing, and performance monitoring. ResearchGate. https://doi.org/397786254
21) Qudus, L. (2020). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive*, *14*(1), 1146-1163. https://doi.org/10.30574/ijsra.2025.14.1.0225
22) Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729
23) Panabergenova, J., Umarova, K. Corporate governance cybersecurity framework in CIS countries: comparative analysis of regulatory standards and digital risk management practices. *Int. Cybersecur. Law Rev.* **6**, 367–376 (2021). https://doi.org/10.1365/s43439-025-00146-4
24) Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, *17*, 49-59. https://doi.org/10.1016/j.ijcip.2017.03.002

International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

25) Ali, A.S., Zaaba, Z.F., Singh, M.M. *et al.* Advancing cybersecurity in ASEAN: current trends, emerging challenges, and opportunities for enhanced resilience. *Int. J. Inf. Secur.* **24**, 200 (2022). https://doi.org/10.1007/s10207-025-01111-2
26) Younus, M., Suardi, W., & Anggita, I. (2022). Evaluating E-Government Cybersecurity Policies: A Comparative Study of Current Challenges and Future Implications. *INTEGRAL: Jurnal Inovasi, Teknologi Terapan, dan Litbang*, *3*(2), 122-139. https://doi.org/10.57122/integral.v3i2.45
27) Krishna, B., & MP, S. (2021). Examining the relationship between e-government development, nation’s cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Information & Computer Security*, *29*(5), 737-760. https://doi.org/10.1108/ICS-12-2020-0205
28) Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, *20*(2), 96–121. https://doi.org/10.1080/02681102.2013.836699