International Journal of Advances in Data and Information Systems
Vol. 1, No. 2, October 2020, pp. xx~xx
ISSN: 2721-3056, DOI: 10.25008/ijadis.xxxx

Revisiting Cyber Threats in Government Sectors: A Systematic Review of Attacks, Challenges, and Policy-Level Defenses

Aisyah Nuraeni[1], Yudhistira Nugraha[2], Muhamad Erza Aminanto[3]
[1,2]Cyber Security and Digital Forensics Telkom University, Indonesia
[3]Cyber Security Monash University, Indonesia

Article Info

Article history:

Received Jan x, 20xx
Revised Feb x, 20xx
Accepted Apr x, 20xx

Keywords:

Systematic Literature Review
Cybersecurity Threats
Government Sector
Security Operations Center (SOC)
Institutional limitations

ABSTRACT

This paper presents a systematic literature review (SLR) based on the PRISMA framework, synthesizing 128 peer-reviewed studies published between 2020 and 2024, drawn from major scholarly databases. The review investigates cyber threats specifically targeting government institutions and identifies phishing, ransomware, malware, and denial-of-service (DoS) attacks as the most prevalent attack vectors affecting government sector environments. In addition to these threats, the study highlights persistent institutional limitations, such as outdated infrastructure, fragmented inter-agency coordination, limited technical capacity, and regulatory gaps, which hinder effective cybersecurity governance and response. To address these challenges, the review compiles both proactive and reactive mitigation strategies, emphasizing the need for SOC design principles such as scalability, interoperability, inter-agency coordination, and resilience in cyber operations. The paper synthesizes its findings into a taxonomy of threat profiles and contextual constraints, offering a foundational reference for building government-specific SOC models. It also outlines future research directions related to operational validation, capability maturity modeling, and institutional alignment in public-sector cybersecurity architectures.

Corresponding Author:

Aisyah Nuraeni,
Master's Program in Cyber Security and Digital Forensics,
Telkom University,
No. 1 Telekomunikasi Street, Buahbatu–Bojongsoang Extension, Sukapura, Dayeuhkolot Subdistrict,
Bandung Regency, West Java 40257, Indonesia.
Email: aisyahnuraeni@student.telkomuniversity.ac.id

1. INTRODUCTION (11 PT)

Across the globe, the public sector faces escalating cybersecurity threats. This trend is driven by rapid digital transformation and increasingly advanced adversarial capabilities[1]. Government institutions are now primary targets for phishing, ransomware, malware, and distributed denial-of-service (DDoS) attacks. These threats often lead to data loss, service disruption, and erosion of public trust. These threats jeopardize operational continuity and raise serious national security concerns. This is particularly relevant amid increasing geopolitical tensions and the growing prevalence of advanced persistent threats (APTs) [2] [3] [4].

While several studies have addressed cyber threats and security frameworks in public sector environments, the existing body of literature often focuses on isolated aspects. For example, Humayun et al. [4] presented a systematic mapping study on cyber threats and vulnerabilities,

while Al-Hawamleh examined cybersecurity practices and their impact on e-government service quality [5]. Others, such as Kure et al., Syuntyurenko, and Kulugh et al. emphasized risk frameworks or resilience assessment models without integrating broader threat typologies or institutional limitations [6], [7], [8]. Several studies have highlighted the importance of legislation, capacity building, and institutional coordination in cybersecurity governance [9], [10], [11], [12], [13] Advanced approaches, including intrusion detection frameworks and risk prediction models, have also been proposed in response to persistent threats like APTs [14]. Additionally, a recent study by Hossain et al. provides a systematic review focused specifically on cybersecurity in local governments, identifying key governance and institutional challenges that align closely with the gaps addressed in this paper [15].

To the best of our knowledge, no prior systematic literature review (SLR) has synthesized threat categories, institutional limitations, and mitigation strategies collectively across the 2020–2024 time range and within a government-specific context. This gap highlights the need for a comprehensive synthesis that maps the evolving landscape of cyber threats faced by government institutions, analyzes the capacity-related and structural limitations hindering response, and compiles strategic approaches for resilience. Addressing this gap is crucial to guide policy, investment, and research priorities.

This paper makes the following contributions:

i. Presents a structured analysis of 128 peer-reviewed studies on government cybersecurity threats from 2020–2024.
ii. Identifies institutional barriers through a thematic schema aligned with capability and governance gaps.
iii. Proposes a synthesized foundation for resilience-oriented SOC design tailored to government settings.

2. METHOD

A Systematic Literature Review (SLR) was conducted following the PRISMA 2020 guidelines [16] and the systematic review procedure proposed by Kitchenham [17]. This method was selected to ensure a transparent, replicable, and rigorous synthesis of peer-reviewed studies focusing on cyber threats in government sectors

2.1 Data Source and Search Strategy

The literature search was performed across six major academic databases: IEEE Xplore, SpringerLink, ScienceDirect, Wiley, and Emerald Insight. The primary search query used was: “cyber threats” AND “government”. This string was applied to titles, abstracts, and keywords to ensure consistency across databases. While alternative keywords such as “digital government” and “public sector” were tested, they were excluded due to low precision and high noise. This limitation is acknowledged in the limitations section.

Backward citation tracking and snowballing techniques were not applied, which constitutes a methodological constraint discussed later in this paper.

2.2 Inclusion and Exclusion Criteria

The inclusion criteria for selecting studies were as follows: (i) the study was published between January 2020 and Mei 2024; (ii) it was a peer-reviewed journal article or conference proceeding; (iii) it addressed cybersecurity in the context of government or public-sector institutions; (iv) it was published in English; and (v) the full text was accessible.

The exclusion criteria were: (i) the study focused exclusively on corporate, military, or private sector environments; (ii) it lacked full-text access; (iii) it was not peer-reviewed; or (iv) it was published in a non-English language.

2.3 Screening and Quality Assessment

The initial search yielded 1,004 articles. After removing duplicates, 945 records remained for title and abstract screening. The screening and full-text eligibility assessment were conducted by a single reviewer (the first author), following a structured protocol aligned with the predefined inclusion and exclusion criteria.

A total of 132 full-text articles were assessed for eligibility. Subsequently, 128 studies were selected based on a structured quality appraisal using seven criteria adapted from Kitchenham and Ali et al. Each criterion (C1–C7) was scored on a scale of 0 to 1. Articles that achieved a total score greater than 5.0 (i.e., exceeding 71% of the maximum score) were considered methodologically sound and marked for inclusion (EXTRACT), in line with the minimum 70% threshold for SLR quality screening[18].

Although this review was performed by a single researcher, multiple steps were taken to mitigate potential bias and enhance the credibility of the selection process. These include maintaining a documented audit trail, applying standardized screening criteria, and conducting iterative reviews to ensure consistency. The PRISMA flow diagram depicting the overall selection process is presented in Fig. 1.

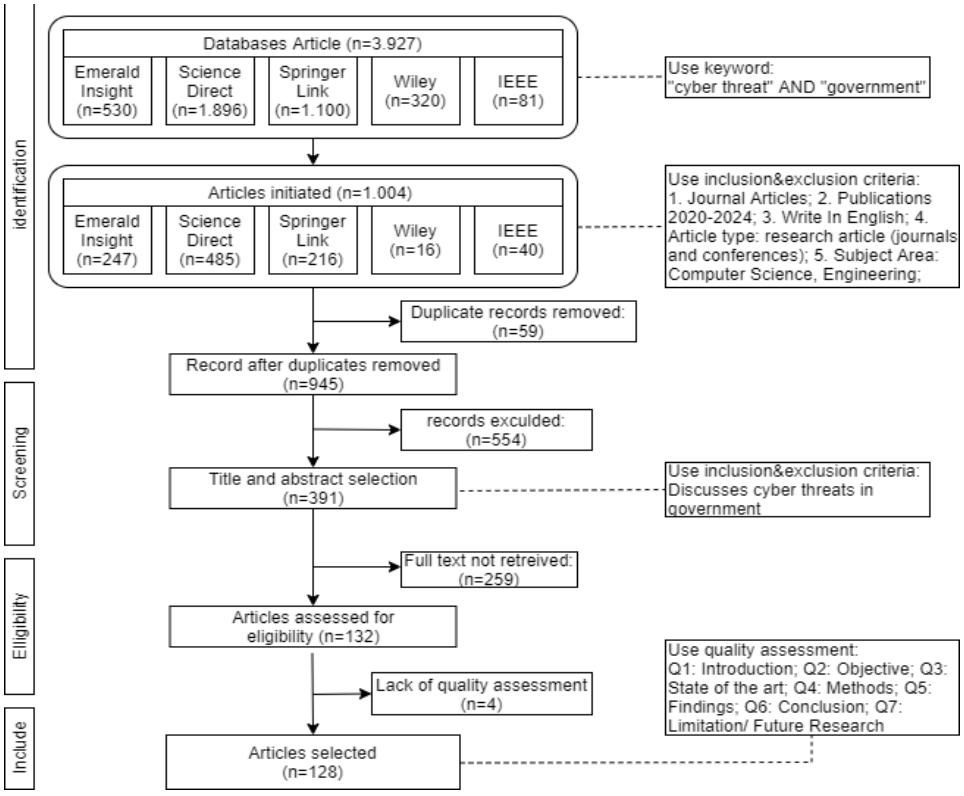

Fig. 1. PRISMA flow diagram depicting the literature selection process for the systematic review.

2.4 Data Extraction and Thematic Coding

A structured data extraction process was conducted to systematically collect and organize relevant information from the selected studies. For each article, the following fields were extracted and recorded in a Microsoft Excel spreadsheet: (i) bibliographic metadata (title, authors, year of publication); (ii) geographic focus (national, regional, or global); (iii) type of study (empirical, conceptual, or review); and (iv) thematic relevance to the research questions (RQ1–RQ3), including details of cyber threats, institutional limitations, and mitigation strategies.

Following data extraction, a thematic coding process was applied using an inductive–deductive hybrid approach. Three major coding categories were predefined, aligned with the research questions: (i) significant cyber threat profiles affecting the government sector (RQ1); (ii) institutional and structural limitations in cybersecurity governance (RQ2); and (iii) proposed

mitigation strategies and policy frameworks (RQ3). Sub-themes within each category emerged inductively during repeated readings of the full-text articles.

The coding process was conducted manually by the primary researcher, with several measures taken to ensure consistency and reduce interpretive bias. These included multiple coding iterations, consistent use of coding definitions, and documentation of all decisions within a structured matrix. Although qualitative data analysis software (e.g., NVivo, MAXQDA) was not used, the manual method allowed for rich contextual interpretation and transparent traceability of the coding logic [19]. This trade-off is acknowledged in the limitations of the study.

The coded data were then grouped and synthesized to identify patterns, frequencies, and thematic intersections across the reviewed literature. The final coding results were organized by research question and are presented visually in figures and tables. Comprehensive metadata of the selected studies and the results of thematic coding are provided in Supplementary Appendix A and Appendix B.

2.5 Bias Mitigation and Reliability

A single researcher conducted this systematic literature review. Therefore, inter-rater reliability metrics such as Cohen's Kappa or Fleiss' agreement coefficient were not applied. This limitation is acknowledged and addressed through several mitigation strategies. First, the screening process used clearly defined inclusion and exclusion criteria. Second, thematic coding was guided by a structured matrix aligned with the research questions. Third, the coding process was repeated in multiple rounds to refine categories and reduce subjectivity.

To ensure transparency, all coding decisions were documented in a master matrix. The full list of 128 included articles and their thematic alignment with RQ1–RQ3 is available. Although this review lacked independent validation from multiple coders, the use of systematic procedures and full documentation contributes to the reliability and reproducibility of the findings.

Future research is encouraged to involve multiple reviewers and compute inter-rater agreement to improve analytical rigor and reduce bias [20].

3. RESULT AND DISCUSSION

This section presents the results obtained from a systematic thematic analysis of 128 peer-reviewed articles selected through the PRISMA framework. The findings are structured to address the study's three core research questions, encompassing the identification of dominant cyber threat profiles in government sectors, institutional and structural limitations in cybersecurity response, and the range of mitigation strategies proposed in the literature. These results are elaborated in Subsection 3.1. Subsequently, Subsection 3.2 provides a thematic discussion and critical interpretation of these findings, framed through theoretical, geopolitical, and governance perspectives.

3.1. Key Findings from the Review

The key insights obtained from the thematic analysis of 128 selected articles are outlined below, structured according to the study's core research questions.

A. Taxonomy of Cyber Threats in Government

The analysis revealed that the most frequently discussed threats in government-related studies were phishing (48 articles), malware (45), ransomware (44), and Distributed Denial of Service (DDoS) attacks (34). Other threats, such as insider threats, data breaches, social engineering, and identity theft, were mentioned less frequently (see Fig. 2).

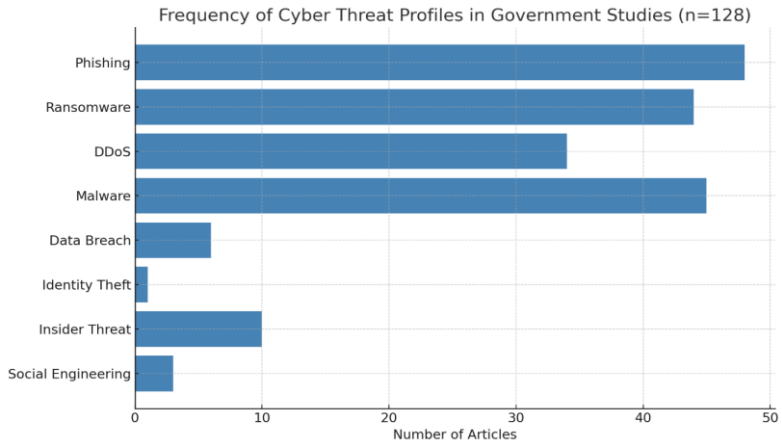

Fig. 2. Frequency of Cyber Threat Profiles in Government Studies.

To enhance operational relevance, we mapped these threats to the MITRE ATT&CK framework. This mapping contextualizes threat behaviors based on adversary TTPs (Tactics, Techniques, and Procedures), offering a standardized vocabulary for security operations (see Table I):

Table 1. Mapping Cyber Threats to MITRE ATT&CK

Threat Type	MITRE ATT&CK Tactic (ID)	Techniques Observed
Phishing	Initial Access (TA0001)	T1566.001: Spearphishing, Attachment
Malware	Execution (TA0002), Defense Evasion (TA0005)	T1059: Command & Scripting Interpreter, T1027: Obfuscated Files
Ransomware	Impact (TA0040)	T1486: Data Encrypted for Impact, T1490: Inhibit System Recovery
DDoS	Impact (TA0040)	T1499: Endpoint Denial of Service

The report emphasizes the rising sophistication of ransomware actors, who now combine multiple MITRE techniques—initial access via phishing (T1566), privilege escalation via LSASS dumping (T1003.001), and impact via encryption (T1486)—to maximize disruption and extortion leverage [21]. In parallel, these threats were also aligned with the NIST Cybersecurity Framework (CSF) to guide institutional responses across five functional areas: Identify, Protect, Detect, Respond, and Recover [22]. For instance, phishing requires strong Protect (e.g., email filtering) and Detect (e.g., anomaly detection) capabilities, whereas ransomware demands robust Respond and Recover strategies, including incident containment and backup restoration.

This dual-framework mapping, tactical from MITRE and strategic from NIST, enables government agencies to not only classify threats with precision but also prioritize defenses based on real-world attack sequences and institutional capabilities.

B. Institutional and Structural Limitations

Based on the thematic analysis of 128 studies, this review identifies a range of institutional and structural limitations that hinder the development of effective cybersecurity governance in government environments (see Fig. 3). These limitations were categorized into four major groups: technical, human capital, legal, and organizational constraints, each of which reflects distinct aspects of institutional readiness and capacity. The most frequently cited limitation was resource limitations, mentioned in 50 articles. These include inadequate infrastructure, limited budget allocations, and lack of technological modernization, thereby falling under the technical category. Closely related, lack of technical skills (3 articles) and visibility and understanding deficiencies (2 articles) were classified under human capital, emphasizing the shortage of trained cybersecurity personnel and limited awareness among public sector staff.

In the legal domain, several articles highlighted deficiencies in regulatory frameworks. These include legislative and regulatory issues (1 article), data protection issues (10 articles), and insufficiency of legal measures (1 article). These findings illustrate the challenges governments

face in updating or enforcing cybersecurity-related regulations and data governance standards. Organizational limitations were also prominent, encompassing fragmented coordination, overlapping roles, and weak institutional capacity. Notably, international cooperation (7 articles), financial sector vulnerabilities (2 articles), conflict management between regulators (1 article), and dependence on the private sector (1 article) reflect the lack of coherent governance structures and strategic partnerships across sectors.

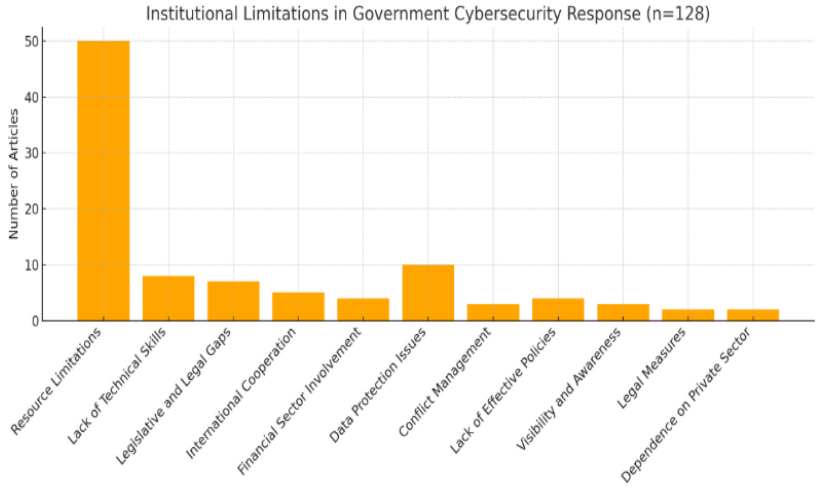

Fig. 3. Government Limitations in Cybersecurity Response Studies.

These limitations vary significantly across regions. For example, while countries such as the U.S., U.K., and South Korea demonstrate high institutional maturity and inter-agency coordination, nations in Sub-Saharan Africa, South Asia, and Latin America face multi-layered challenges, including legal voids, insufficient budgets, and weak enforcement mechanisms. This geopolitical disparity underscores the need for regionally tailored capacity-building programs and international legal harmonization

C. Strategic Responses and Mitigation Frameworks

Eight categories of mitigation strategies were identified (see Fig. 4), with Innovation and Research and Technology Infrastructure Enhancement emerging as the most frequently proposed.

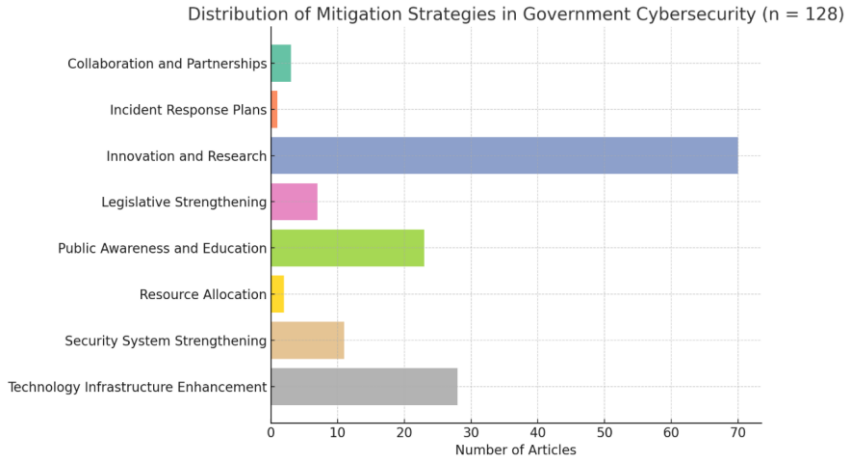

Fig. 4. Commonly proposed solutions for cyber threat mitigation in government studies.

To provide greater clarity, these strategies were grouped into two categories: proactive (anticipatory and resilience-building) and reactive (incident-driven and response-based). This classification helps governments prioritize and balance their cybersecurity investments based on their institutional maturity and resource availability. Proactive measures emphasize preventing incidents before they occur and strengthening systemic resilience. One of the most commonly

recommended strategies is the implementation of cybersecurity awareness and training programs, which aim to improve digital literacy among civil servants and reduce susceptibility to phishing and social engineering attacks. Such programs also enhance organizational readiness by increasing incident reporting and response capabilities [2], [23]. In addition, the deployment of cyber threat intelligence (CTI) platforms has been associated with faster detection and more coordinated incident response. CTI maturity is critical for situational awareness and for sharing threat indicators in real time across government entities[24].

Another strategic measure is the development of Computer Security Incident Response Teams (CSIRTs), which institutionalize structured defense protocols and provide a formal mechanism for rapid containment and recovery. This is especially vital in countries where Security Operations Centers (SOCs) are not yet fully established [23], [25]. Cross-sector collaboration also emerges as a critical enabler of cyber resilience. Partnerships between government, academia, and industry allow for the pooling of technical resources and the exchange of knowledge, bridging gaps in expertise and infrastructure [5], [25]. Finally, capacity building and workforce development remain essential, particularly in developing regions where trained cybersecurity personnel are in short supply. Long-term investments in civil service training and education are considered foundational to building a sustainable cybersecurity culture [23]

Reactive strategies, while still dominant in many government environments, focus on mitigating the damage after an incident has occurred. The most frequently cited reactive measure is technology infrastructure enhancement, which includes upgrading legacy systems and deploying monitoring tools. These interventions are often implemented after a significant compromise has occurred [26], [27]. Another essential component of a reactive strategy is incident response planning, which involves preparing escalation protocols, incident playbooks, and continuity-of-operations procedures. These frameworks form the backbone of national emergency preparedness and are vital for minimizing downtime during cyber crises [28]. Policy and regulatory reforms also play a reactive role, often triggered by high-profile breaches or operational failures. Several studies highlight how digital transformation outpaces legal readiness, leading to regulatory gaps that undermine national cyber defense [29]. Moreover, outdated or poorly enforced cybercrime laws continue to limit the deterrent effect of penalties and hinder post-incident recovery [30].

This classification reflects a global transition toward more structured cybersecurity governance. However, the review also reveals that reactive measures still dominate, especially in low- and middle-income countries, where budget constraints and institutional inertia limit proactive investments.

3.2. Discussion of the findings

The findings presented above are further examined in this subsection to interpret their implications through theoretical, institutional, and practical lenses.

A. Synthesizing Findings Through Theoretical Lenses

The observed prevalence of reactive cyber responses—largely focused on infrastructure upgrades and regulatory patching can be interpreted through institutional theory, where governments tend to conform to external legitimacy rather than adapt internal efficiency [27], [31]. Similarly, symbolic compliance explains the surface-level adoption of standards like NIST CSF, which often lack institutionalization [32], [33]. From the perspective of governance theory, particularly multi-level governance [29] Cyber fragmentation, manifested through inter-agency role confusion and decentralized incident handling, is a recurring pattern across federal and developing states [3], [5]. These frameworks help make sense of why technical solutions alone have not yielded resilient digital public services.

B. Evaluating the Effectiveness of Current Responses

Although cybersecurity strategies have expanded post-COVID, several studies report a gap between planning and execution. Awareness programs remain underfunded and uncoordinated [2] while many developing countries still lack functional CSIRTs [23]. Legal reforms tend to be event-driven, as seen in the UAE and Turkey [34][30], and are not matched with operational enforcement mechanisms [35]. Technology-centered responses, such as firewalls and intrusion prevention

systems, are widespread [24], [26], but without integration into national strategy or interagency SOPs, they function as reactive band-aids rather than systemic solutions [36], [37].

C. Geographical and Temporal Variations

The analysis reveals a growing interest in cyber threats across various geopolitical contexts (see Table II), with a notable number of studies emerging from countries such as the USA, India, Saudi Arabia, South Korea, and China. Furthermore, some research adopts a global perspective without focusing on any single nation, highlighting the transnational nature of cybersecurity concerns in the public sector.

Table 2. Distribution of Reviewed Studies by Country and Year

Year	Countries Covered in the Studies
2020	United Arab Emirates (UAE), Saudi Arabia, USA, Brazil, Uganda, Portugal, Spain, Germany, Netherlands, Japan, Pakistan, South Korea, United Kingdom, France, Canada, India, United States and France, Norway, Italy
2021	India, Russia, China, United Kingdom, France, USA and Belgium, South Korea, Italy, Norway, Bangladesh, Switzerland, Saudi Arabia, Belgium, Netherlands, Canada, Poland
2022	Caribbean, Bahrain, Poland, European Union (EU), Hungary, Spain, Republic of Kosovo, India, Saudi Arabia, Russia, UAE, Malaysia, China, Nigeria, South Africa, South Korea, Canada
2023	Nigeria, Kingdom of Bahrain, USA, Indonesia, Australia, France, South Korea, Sweden, China, Zimbabwe, South Africa, UK, Oman, India, Pakistan, Malaysia, Philippines, Botswana, Spain, Germany, Italy
2024	Saudi Arabia, India, Qatar, Austria, Estonia
Global	Several studies present global or international perspectives without focusing on specific countries

From a geopolitical lens, cybersecurity maturity aligns with state capacity and digital sovereignty orientation. Countries like South Korea and the UAE have invested in cross-sector coordination and centralized threat monitoring [5]. Conversely, Caribbean and African nations face constraints in legislation, workforce development, and funding [38], [39].

D. Implications for Government Cybersecurity Resilience

The findings underscore the urgent need for governments to transition from fragmented and reactive cybersecurity postures toward more resilient and systemically integrated approaches. Security Operations Centers (SOCs), which were once limited to enterprise or military environments, are now essential in the public sector for safeguarding national digital infrastructure. However, public-sector SOCs must be designed differently from their corporate counterparts, taking into account institutional constraints, procurement complexity, and bureaucratic workflow management [5], [32].

The taxonomy developed through this review provides a practical basis for conceptualizing a government-specific SOC model. One key requirement is the integration of cyber threat intelligence (CTI) platforms with mechanisms to filter, verify, and disseminate actionable intelligence across agencies. This step is crucial to break the silos between ministries and foster coordinated situational awareness [40], [41]. Additionally, robust interagency coordination mechanisms are vital. Studies have shown the importance of extending the roles of national Computer Emergency Response Teams (CERTs) into fully functional SOCs that operate with standardized escalation paths and real-time collaboration across departments [26], [42].

Another pillar of SOC readiness is human capital development. Upskilling civil servants, particularly those responsible for critical IT systems in areas such as cyber hygiene, forensic analysis, and threat modeling, is a long-term investment that underpins the operational sustainability of public SOCs [23], [37]. Equally important is the capacity for proactive threat detection and automated response. SOCs in government environments, which are often characterized by a mix of modern and legacy systems, must implement AI-assisted Security Information and Event Management (SIEM) solutions tailored to detect anomalies across

heterogeneous platforms [43], [44]. Rather than serving as passive monitoring hubs, government SOCs should evolve into institutional nerve centers integrating intelligence, operations, and policy to enable agile, anticipatory responses to cyber threats.

E. Contribution to Theory, Policy, and Practice

This study makes several original contributions to both theory and practice. First, it bridges established cybersecurity frameworks such as MITRE ATT&CK and the NIST Cybersecurity Framework with organizational theory, providing new analytical perspectives for understanding institutional cybersecurity governance. Second, it offers a taxonomic foundation that can inform the design of context-specific Security Operations Center (SOC) models, particularly those aligned with the unique constraints of public governance environments. Third, the findings highlight the presence of regionally differentiated pathways in the development of cyber capabilities, which may serve as strategic entry points for both international donor engagement and comparative policy benchmarking, as observed in recent studies on cross-country institutional evolution [36], [45].

F. Limitations

This review has several limitations that must be acknowledged. First, the entire review process was conducted by a single researcher. The absence of multiple independent reviewers limited the ability to perform inter-rater reliability analysis. Although mitigation steps were taken to ensure consistency, future reviews should involve multiple coders to enhance objectivity and analytical rigor.

Second, this study is subject to publication bias. Governments often do not disclose failed cybersecurity initiatives or internal weaknesses, which may lead to overrepresentation of successful or theoretical models in the literature [38], [43]. Third, the review included only English-language and accessible academic sources. This restriction may have excluded region-specific insights available in non-English publications or gray literature.

Fourth, the selected time frame (2020–2024) provided a focused and contemporary view, but may overlook longer-term developments and legacy challenges [46]. Fifth, the findings rely entirely on publicly available materials and academic analyses. Due to the lack of access to classified or internal government documents, the review could not assess operational realities such as actual SOC deployment, coordination mechanisms, or escalation paths [43], [44].

Finally, this study does not incorporate direct input from public-sector cybersecurity practitioners. The absence of practitioner validation limits contextual depth, particularly in assessing practical feasibility, inter-agency collaboration, and real-world implementation challenges [41], [47], [48], [49], [50].

These limitations highlight the need for future research to emphasize multilingual inclusion, cross-sectoral fieldwork, and institutional feedback. These approaches are essential to ensure that proposed SOC models are not only technically robust but also contextually grounded and administratively practical

4. CONCLUSION

This systematic review analyzed cyber threats, institutional challenges, and mitigation strategies in government sectors between 2020 and 2024. The results reveal that public institutions continue to face persistent threats, particularly phishing, ransomware, malware, and denial-of-service attacks, while their responses are often hampered by fragmented governance, outdated infrastructure, and limited cybersecurity expertise. One of the key contributions of this study is the development of a taxonomy that links threat profiles with institutional limitations and strategic responses. This taxonomy provides not only conceptual clarity but also a practical framework for designing Security Operations Center (SOC) models that align with the unique needs and constraints of public governance environments. By bridging technical standards with institutional analysis, the review offers new insights for both policy development and academic discourse. It emphasizes the urgent need for governments to move beyond reactive measures and adopt proactive, resilient cybersecurity governance. In doing so, this study lays the groundwork for future efforts to build scalable and context-aware SOC implementations in the government sector.

Building on the findings of this review, future research should focus on designing and validating Security Operations Center (SOC) models that are specifically tailored for government contexts. This paper provides a taxonomic foundation and strategic direction to inform such developments. Key areas for further exploration include:

1. Modular SOC Architectures that can scale across local, provincial, and national governance levels.
2. Government-specific SOC Capability Maturity Models (SOC-CMM) that reflect institutional realities, including fragmentation and budget limitations.
3. Trust and Interoperability Frameworks to enable secure and timely cyber threat intelligence exchange among ministries and agencies.
4. AI-assisted Threat Detection and Analytics that are optimized for legacy-rich public IT environments.
5. Empirical Validation in Government Settings, including real-world deployments and scenario-based evaluations within municipal and national agencies.

REFERENCES

[1] Torvald F. Ask, Ricardo G. Lugo, Benjamin J. Knox, and Stefan Sütterlin, "Human-Human Communication in Cyber Threat Situations A Systematic Review," Jul. 2021. [Online]. Available: http://www.springer.com/series/7409

[2] A. Ubowska and T. Królikowski, "Building a cybersecurity culture of public administration system in Poland," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 1242–1250. doi: 10.1016/j.procs.2022.09.180.

[3] F. R. Bechara and S. B. Schuch, "Cybersecurity and global regulatory challenges," *J Financ Crime*, vol. 28, no. 2, pp. 359–374, 2020, doi: 10.1108/JFC-07-2020-0149.

[4] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab J Sci Eng*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020, doi: 10.1007/s13369-019-04319-2.

[5] A. M. Al-Hawamleh, "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA," *Digital Policy, Regulation and Governance* , vol. 26, no. 3, pp. 317–336, Apr. 2024, doi: 10.1108/DPRG-11-2023-0168.

[6] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Comput Appl*, vol. 34, no. 18, pp. 15241–15271, Sep. 2022, doi: 10.1007/s00521-022-06959-2.

[7] O. V. Syuntyurenko, "Predicting Potential Threats and Megarisks in Information Technology Development," *Scientific and Technical Information Processing*, vol. 49, no. 1, pp. 48–59, Mar. 2022, doi: 10.3103/S0147688222010130.

[8] V. E. Kulugh, U. M. Mbanaso, and G. Chukwudebe, "Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure," *SN Comput Sci*, vol. 3, no. 3, May 2022, doi: 10.1007/s42979-022-01108-x.

[9] S. Dutta, S. K. Sahu, S. Dutta, and B. Dey, "Leveraging a micro synchrophasor for fault detection in a renewable based smart grid—A machine learned sustainable solution with cyber-attack resiliency," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 2, Jan. 2022, doi: 10.1016/j.prime.2022.100090.

[10] B. Sule, U. Sambo, and M. Yusuf, "Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria," *J Financ Crime*, vol. 30, no. 6, pp. 1557–1574, Dec. 2023, doi: 10.1108/JFC-07-2022-0157.

[11] A. S. Muhammad and T. Kaya, "Factors affecting the citizen's intention to adopt e-government in Nigeria," *Journal of Information, Communication and Ethics in Society*, vol. 21, no. 3, pp. 271–289, Jul. 2023, doi: 10.1108/JICES-05-2022-0054.

[12] D. C. Le Nguyen and D. W. Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action,'" *Computer Law and Security Review*, vol. 40, Apr. 2021, doi: 10.1016/j.clsr.2020.105521.

[13] S. Sarefo, B. Mphago, and M. Dawson, "An analysis of Botswana's cybercrime legislation," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 1023–1033. doi: 10.1016/j.procs.2023.01.380.

[14] N. E. Park *et al.*, "Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks," *Computers and Electrical Engineering*, vol. 105, Jan. 2023, doi: 10.1016/j.compeleceng.2022.108548.

[15] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," 2025, *Elsevier B.V.* doi: 10.1016/j.ugj.2024.12.010.
[16] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.
[17] B. Kitchenham and S. M. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007. [Online]. Available: https://www.researchgate.net/publication/302924724
[18] N. Bin Ali and M. Usman, "Reliability of search in systematic reviews: Towards a quality assessment framework for the automated-search strategy," *Inf Softw Technol*, vol. 99, pp. 133–147, Jul. 2018, doi: 10.1016/j.infsof.2018.02.002.
[19] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *Int J Qual Methods*, vol. 16, no. 1, Sep. 2017, doi: 10.1177/1609406917733847.
[20] D. Gough, J. Thomas, and S. Oliver, "Clarifying differences between reviews within evidence ecosystems," Jul. 15, 2019, *BioMed Central Ltd.* doi: 10.1186/s13643-019-1089-2.
[21] Cisa, "Recommendations to Mitigate Specific Attacker Capabilities Based Upon MITRE ATT&CK ® Tactics Mitigating Cyber Risks with MITRE ATT&CK | 2."
[22] Nist, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.
[23] O. Oriola, A. B. Adeyemo, M. Papadaki, and E. Kotzé, "A collaborative approach for national cybersecurity incident management," *Information and Computer Security*, vol. 29, no. 3, pp. 457–484, 2021, doi: 10.1108/ICS-02-2020-0027.
[24] K. Shaheen and A. H. Zolait, "The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain," *Information and Computer Security*, vol. 31, no. 5, pp. 529–544, Nov. 2023, doi: 10.1108/ICS-06-2022-0108.
[25] M. Dev and D. Saha, "Does e-government development moderate the impact of female labor participation on national cybersecurity maturity? An empirical investigation," *Information and Computer Security*, vol. 32, no. 1, pp. 74–92, Jan. 2024, doi: 10.1108/ICS-03-2023-0042.
[26] P. A. W. Putro, D. I. Sensuse, and W. S. S. Wibowo, "Framework for critical information infrastructure protection in smart government: a case study in Indonesia," *Information and Computer Security*, vol. 32, no. 1, pp. 112–129, Jan. 2024, doi: 10.1108/ICS-03-2023-0031.
[27] R. Goel, A. Kumar, and J. Haddow, "PRISM: a strategic decision framework for cybersecurity risk assessment," *Information and Computer Security*, vol. 28, no. 4, pp. 591–625, Oct. 2020, doi: 10.1108/ICS-11-2018-0131.
[28] J. A. Paul and M. Zhang, "Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker," *Eur J Oper Res*, vol. 291, no. 1, pp. 349–364, May 2021, doi: 10.1016/j.ejor.2020.09.013.
[29] A. Visvizi and M. D. Lytras, "Government at risk: between distributed risks and threats and effective policy-responses," *Transforming Government: People, Process and Policy*, vol. 14, no. 3, pp. 333–336, Aug. 2020, doi: 10.1108/TG-06-2020-0137.
[30] R. Saylam and A. Ozdemir, "Military acceptance of the Internet of Things: a research model," *Digital Policy, Regulation and Governance* , vol. 24, no. 1, pp. 1–16, Feb. 2022, doi: 10.1108/DPRG-03-2021-0045.
[31] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, and U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures," *Comput Secur*, vol. 128, May 2023, doi: 10.1016/j.cose.2023.103139.
[32] T. Gibbs, "Seeking economic cyber security: a Middle Eastern example," *Journal of Money Laundering Control*, vol. 23, no. 2, pp. 493–507, May 2020, doi: 10.1108/JMLC-09-2019-0076.
[33] O. Gulyas and G. Kiss, "Impact of cyber-Attacks on the financial institutions," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 84–90. doi: 10.1016/j.procs.2023.01.267.
[34] T. N. Al-Tawil, "Ethical implications for teaching students to hack to combat cybercrime and money laundering," *Journal of Money Laundering Control*, vol. 27, no. 1, pp. 21–33, Jan. 2024, doi: 10.1108/JMLC-01-2023-0014.
[35] F. Pathe Duarte, "Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18)," *Transforming Government: People, Process and Policy*, vol. 14, no. 3, pp. 433–451, Aug. 2020, doi: 10.1108/TG-01-2020-0011.
[36] B. Krishna and S. M.P, "Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis,"

Information and Computer Security, vol. 29, no. 5, pp. 737–760, Nov. 2021, doi: 10.1108/ICS-12-2020-0205.

[37] H. t. A. N. Abd Al Ghaffar, "Government Cloud Computing and National Security," *Review of Economics and Political Science*, vol. 9, no. 2, pp. 116–133, Apr. 2024, doi: 10.1108/REPS-09-2019-0125.

[38] L. Waller *et al.*, "Woe is the dark Web: the main challenges that governments of the Commonwealth Caribbean will face in combating dark Web-facilitated criminal activities," *Transforming Government: People, Process and Policy*, vol. 17, no. 1, pp. 87–100, Feb. 2023, doi: 10.1108/TG-06-2022-0082.

[39] S. Takavarasha Jr, R. Van Heerden, S. C. Thakur, and A. Jordaan, "Cyber-security in the era of the COVID-19 pandemic: a developing countries' perspective," *International Journal of Industrial Engineering and Operations Management*, vol. 5, no. 2, pp. 77–85, Jun. 2023, doi: 10.1108/ijieom-02-2023-0026.

[40] N. H. Chowdhury, M. T. P. Adam, and T. Teubner, "Rushing for security: a document analysis on the sources and effects of time pressure on organizational cybersecurity," *Information and Computer Security*, vol. 31, no. 4, pp. 504–526, Oct. 2023, doi: 10.1108/ICS-01-2021-0013.

[41] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya, and S. Khan, "Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack," *IEEE Access*, vol. 10, pp. 108760–108774, 2022, doi: 10.1109/ACCESS.2022.3213644.

[42] S. A. Lone and A. H. Mir, "A novel OTP based tripartite authentication scheme," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 4, pp. 437–459, Jul. 2022, doi: 10.1108/IJPCC-04-2021-0097.

[43] E. Heeren-Moon, "Risk, reputation and responsibility: Cybersecurity and centralized data in United States civilian federal agencies," *Telecomm Policy*, vol. 47, no. 2, Mar. 2023, doi: 10.1016/j.telpol.2023.102502.

[44] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," *Cybersecurity*, vol. 3, no. 1, Dec. 2020, doi: 10.1186/s42400-020-00048-4.

[45] M. M. Salim, S. K. Singh, and J. H. Park, "Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks," *Appl Soft Comput*, vol. 113, Dec. 2021, doi: 10.1016/j.asoc.2021.107859.

[46] R. Gafni and T. Pavel, "Cyberattacks against the health-care sectors during the COVID-19 pandemic," *Information and Computer Security*, vol. 30, no. 1, pp. 137–150, Jan. 2022, doi: 10.1108/ICS-05-2021-0059.

[47] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security," *Comput Secur*, vol. 114, Mar. 2022, doi: 10.1016/j.cose.2021.102598.

[48] K. Zhao, "Construction of Network Culture Security Indicator System Based on Deep Learning Algorithm," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 438–445. doi: 10.1016/j.procs.2023.11.050.

[49] J. Navajas-Adán, E. Badia-Gelabert, L. Jiménez-Saurina, M. J. Marijuán-Martín, and R. Mayo-García, "Perceptions and dilemmas around cyber-security in a Spanish research center after a cyber-attack," *Int J Inf Secur*, vol. 23, no. 3, pp. 2315–2331, Jun. 2024, doi: 10.1007/s10207-024-00847-7.

[50] D. Humphreys, A. Koay, D. Desmond, and E. Mealy, "AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business," *AI and Ethics*, vol. 4, no. 3, pp. 791–804, Aug. 2024, doi: 10.1007/s43681-024-00443-4.