International Journal of Cyber Threat Intelligence and Secure Networking (IJCTISN)
eISSN: 3087-4297
Volume03 Issue08 | Page No: -66-71

Received: 25 May 2026, Revised: 15 June 2026, Accepted: 20 July 2026, Published: 28 August 2026

DOI: https://doi.org/10.55640/ijctisn-v03i08-10

AI Governance and Cybersecurity Policy in the Public Sector: Balancing National Security, Data Privacy, and Ethical Risk

Muhammad Hamza Khan[1], Ayesha Noor Malik [2]
[1] Department of Cybersecurity and Information Technology
[2] Department of Cybersecurity and Information Technology

ABSTRACT: The increasing deployment of artificial intelligence (AI) in public-sector environments creates a complex governance challenge in which cybersecurity, national security, data privacy, and ethical accountability must be addressed simultaneously. Government agencies increasingly depend on data-intensive decision systems, making policy frameworks essential for controlling security exposure and maintaining public trust. This research and review paper examines AI governance and cybersecurity policy from a public-sector perspective, with particular emphasis on the balance between national-security objectives, privacy protection, organizational knowledge, stakeholder attitudes, and ethical risk. The study adopts a structured qualitative review and conceptual synthesis of the references supplied for this research. Ahmed (2024) provides the principal conceptual foundation for examining cybersecurity policy frameworks for AI in government, while the remaining studies are critically interpreted for their evidence concerning knowledge, attitudes, stakeholder support, counseling, perception, and technology acceptance. Although several supplied references originate from healthcare and contraceptive-service research rather than AI governance, their findings provide transferable insights into how knowledge, communication, stakeholder perceptions, and institutional support can influence policy implementation. The analysis indicates that effective public-sector AI governance requires more than technical security controls. It requires coordinated policy mechanisms, transparent decision processes, privacy-conscious data management, stakeholder education, accountability structures, and continuous risk assessment. The paper proposes an integrated conceptual governance model linking AI cybersecurity controls with privacy safeguards, ethical oversight, stakeholder capacity, and institutional accountability. The findings further indicate that policy effectiveness depends on the ability of public institutions to reconcile security imperatives with individual rights rather than treating them as independent objectives.

KEYWORDS: Artificial Intelligence Governance, Cybersecurity Policy, Public Sector, National Security, Data Privacy, Ethical Risk, AI Regulation, Government Systems, Risk Management.

1. Introduction

The Artificial intelligence has become increasingly relevant to public-sector decision-making, information processing, service delivery, monitoring, and administrative operations. However, the integration of AI into government environments creates a governance problem that extends beyond algorithmic performance. Government AI systems may process information associated with citizens, public services, institutional operations, and security-sensitive activities. Consequently, cybersecurity policy must address not only unauthorized access and technical vulnerabilities but also privacy, accountability, transparency, institutional responsibility, and ethical risk. Ahmed (2024) specifically positions cybersecurity policy frameworks for AI in government around the tension between national-security requirements and privacy concerns, making this issue central to the present research.

The fundamental policy challenge is that stronger security controls can sometimes increase institutional surveillance or restrict access to information, while stronger privacy protections can potentially constrain security-oriented data integration. Neither objective can therefore be treated as absolute. A public-sector governance framework must determine which data may be collected, who may access it, how AI systems may process it, how decisions can be challenged, and which institutional actors remain accountable when automated systems produce harmful outcomes.

The supplied literature also demonstrates the importance of knowledge, attitudes, perceptions,

counseling, and stakeholder support in implementing policies and interventions. Studies by Stone et al. (2021), Tounkara et al. (2022), Zulfitriani et al. (2021), Kurniawati et al. (2024), and Via and Cusmarih (2024) demonstrate, in their respective contexts, that technology- or service-related outcomes are influenced not only by the availability of an intervention but also by knowledge, communication, perceptions, professional roles, and social support. Although these studies concern healthcare and contraceptive services rather than AI, these institutional and behavioral dimensions are conceptually relevant to AI governance because cybersecurity policies also require organizational adoption and informed stakeholder participation.

The objective of this paper is therefore to develop a research-driven conceptual understanding of AI governance and cybersecurity policy in the public sector. The paper focuses on three interconnected policy objectives: protecting national-security interests, preserving data privacy, and reducing ethical risk. It additionally examines the role of organizational knowledge, stakeholder perception, institutional support, and policy communication in determining whether governance frameworks can be effectively implemented.

2. Literature Review

2.1 AI Governance and Cybersecurity Policy

AI governance can be understood as the collection of institutional rules, responsibilities, processes, controls, and oversight mechanisms through which AI systems are developed, deployed, monitored, and evaluated. In public-sector environments, governance becomes particularly significant because government institutions operate within formal accountability structures and frequently manage information with substantial social consequences. Ahmed (2024) provides the primary reference for connecting AI governance with cybersecurity policy and the competing requirements of national security and privacy.

A central theoretical proposition emerging from this perspective is that cybersecurity should be treated as a governance function rather than exclusively as an information-technology function. Technical controls such as access restrictions, authentication, encryption, monitoring, and incident management are important, but they cannot independently determine whether an AI deployment is ethically or institutionally acceptable. Governance must define the circumstances under which those controls are used and establish accountability when risks materialize.

2.2 Knowledge, Communication, and Institutional Adoption

The importance of knowledge and communication is visible across several supplied studies. Zulfitriani et al. (2021) examine counseling intended to increase knowledge concerning IUD contraceptives, while Pratiwi (2024) investigates knowledge among women of fertile age. Stone et al. (2021) examine the knowledge, attitudes, and practices of health providers concerning postpartum IUD provision. These studies collectively indicate that institutional implementation can be influenced by whether relevant stakeholders possess sufficient knowledge and understanding.

This insight can be transferred cautiously to AI cybersecurity policy. Employees responsible for operating or supervising AI systems cannot reliably implement governance rules that they do not understand. A policy document may specify data-access requirements, risk-assessment procedures, or reporting obligations, but practical compliance depends upon organizational knowledge. Thus, AI governance should incorporate continuous training, role-specific guidance, and mechanisms for communicating changes in security requirements.

2.3 Stakeholder Attitudes and Perceptions

Attitudes and perceptions represent another relevant dimension. Wemrell and Gunnarsson (2022), Okud et al. (2023), and Mvandal et al. (2020) examine attitudes or perceptions toward healthcare interventions and contraceptive technologies. Kurniawati et al. (2024) investigate relationships involving knowledge, attitudes, perceptions, and use, while Purwati et al. (2024) examine education and perception in relation to IUD selection.

Although these studies cannot be used as empirical evidence about AI governance, they provide a useful conceptual analogy: acceptance of an institutional intervention can depend on how stakeholders perceive its risks, benefits, reliability, and legitimacy. Applied to public-sector AI, this suggests that cybersecurity policy cannot rely exclusively on technical compliance. Employees, administrators, service providers, and citizens may respond differently to AI-enabled surveillance, automated decision-making, or data integration depending on their understanding and perceptions of the system.

2.4 Institutional and Social Support

Several supplied references emphasize the role of support structures. Thomas, The Greatest Showman, and Riwu (2024), Kurniawati et al. (2024), and Via and Cusmarih (2024) examine the relationship between knowledge, attitudes, and forms of support in healthcare decision-making. Again, the empirical contexts are different from AI governance, but the institutional principle is transferable: successful implementation frequently requires support from multiple actors rather

than depending on an isolated individual decision.

For public-sector AI, support may involve senior management, cybersecurity teams, legal departments, data administrators, system developers, frontline employees, and external oversight bodies. If these groups possess conflicting objectives, governance implementation can become fragmented. A cybersecurity department may prioritize confidentiality and threat prevention, whereas a public-service department may prioritize accessibility and operational efficiency. Governance must therefore create mechanisms for reconciling competing institutional priorities.

2.5 Research Gap

The supplied literature presents a significant contextual gap. Ahmed (2024) directly addresses AI cybersecurity policy in government, whereas most of the remaining references focus on healthcare, reproductive health, contraceptive knowledge, attitudes, counseling, and service acceptance. Consequently, the reference set does not provide sufficient empirical evidence for measuring specific AI cybersecurity controls, government AI architectures, algorithmic vulnerabilities, or privacy-preserving computational techniques.

Rather than treating this limitation as evidence that healthcare studies directly establish AI governance outcomes, this paper uses them only to support broader organizational concepts concerning knowledge, communication, perception, and institutional support. The resulting research gap is the need for integrated frameworks that connect technical cybersecurity with organizational capacity, privacy, ethical governance, and stakeholder legitimacy. This gap provides the theoretical basis for the conceptual methodology developed below.

3. Methodology

3.1 Research Design

This research adopts a qualitative research-and-review design based exclusively on the references supplied for the study. The methodology consists of thematic synthesis rather than statistical meta-analysis because the references represent substantially different empirical contexts. The principal analytical categories were derived from the research title and the recurring conceptual dimensions represented in the supplied literature: cybersecurity, national security, privacy, ethical risk, knowledge, attitudes, perceptions, communication, and institutional support.

The analysis proceeds in three stages. First, references were classified according to their direct relevance to AI governance or their transferable relevance to organizational implementation. Second, recurring concepts were compared across the literature. Third, these concepts were synthesized into a conceptual AI governance model suitable for public-sector policy analysis.

3.2 Conceptual Governance Framework

The proposed framework consists of five interconnected layers: security governance, privacy governance, ethical governance, organizational capability, and accountability.

Security governance represents mechanisms for identifying and reducing cybersecurity risks associated with AI systems. The policy objective is to protect systems, models, datasets, interfaces, and institutional operations from unauthorized or harmful activity. Ahmed (2024) provides the principal basis for connecting AI cybersecurity with national-security and privacy considerations.

Privacy governance concerns the controlled use of personal and sensitive information. It requires institutions to establish legitimate purposes for data processing, restrict unnecessary access, and define responsibilities for data handling. Privacy governance becomes particularly important when AI systems aggregate information from multiple administrative sources.

Ethical governance addresses risks that may not constitute conventional cybersecurity incidents. For example, an AI system could operate securely while producing decisions that are insufficiently transparent, difficult to contest, or inconsistent with institutional fairness requirements. Ethical governance therefore requires review procedures and accountability mechanisms alongside technical security.

Organizational capability concerns the knowledge and preparedness of employees. The knowledge and counseling literature supplied by Zulfitriani et al. (2021), Pratiwi (2024), and Stone et al. (2021) supports the broader proposition that implementation capacity depends upon understanding and communication. In an AI environment, this means training personnel in data governance, cybersecurity responsibilities, AI limitations, incident reporting, and appropriate system use.

Accountability provides the final layer. A governance framework should establish who is responsible for system design, procurement, deployment, monitoring, data management, incident response, and decisions influenced by AI. Without clear accountability, technical controls may exist without an effective mechanism for institutional responsibility.

3.3 National Security–Privacy Trade-Off

The framework conceptualizes national security and privacy as interconnected but potentially competing objectives. A government may have legitimate reasons to integrate information for threat detection or operational security. However, unrestricted information integration can increase privacy exposure and create opportunities for misuse.

A hypothetical public-sector AI system illustrates this tension. Suppose an agency uses an AI system to identify patterns associated with cyber threats. A broad dataset may improve detection capability, but the same dataset could contain unnecessary personal information. A governance-oriented approach would therefore evaluate whether each category of information is necessary, establish access restrictions, document the purpose of processing, and subject high-risk uses to additional oversight.

The important methodological principle is proportionality: security requirements should be evaluated against privacy and ethical consequences rather than automatically overriding them.

3.4 Ethical Risk Assessment

Ethical risk should be assessed throughout the AI lifecycle rather than only after deployment. A suitable assessment can examine five questions: what data are processed, what decisions are influenced by the system, who may be affected, what potential harms may arise, and how affected stakeholders can challenge or correct outcomes.

The supplied literature concerning knowledge, attitudes, perceptions, and support provides a useful organizational lens for this assessment. For example, if government employees misunderstand an AI system's limitations, inappropriate reliance may occur even when the system is technically secure. Similarly, if affected stakeholders do not understand how a system operates, perceived legitimacy may decline.

3.5 Implementation and Monitoring

Implementation should be continuous rather than treated as a one-time policy activity. Governance requirements should be translated into operational procedures, employee training, access controls, monitoring, risk reviews, and incident-response processes.

Monitoring should evaluate both technical and institutional indicators. Technical indicators may include security incidents, unauthorized access attempts, system anomalies, and policy violations. Institutional indicators may include training completion, reporting behavior, stakeholder understanding, and documented governance reviews. This combined approach prevents cybersecurity from becoming detached from organizational behavior.

4. Results

The synthesis produces five principal findings. First, AI cybersecurity governance in the public sector should be understood as a multidimensional policy problem rather than a purely technical security problem. Ahmed (2024) directly establishes the relevance of balancing national-security requirements with privacy considerations. The analysis extends this proposition by identifying organizational knowledge, stakeholder perceptions, ethical review, and institutional accountability as necessary supporting dimensions.

Second, the literature indicates that knowledge and communication are important implementation variables. Zulfitriani et al. (2021), Pratiwi (2024), and Stone et al. (2021) focus on knowledge and professional understanding in healthcare contexts. Although their findings cannot be generalized directly to AI systems, they support the conceptual proposition that policy implementation requires informed participants. For public-sector AI, insufficient employee knowledge may translate into inappropriate data handling, weak incident reporting, or excessive reliance on automated outputs.

Third, stakeholder attitudes and perceptions emerge as significant governance considerations. Wemrell and Gunnarsson (2022), Okud et al. (2023), and Kurniawati et al. (2024) demonstrate the relevance of attitudes and perceptions in technology- or service-related decisions. In AI governance, this suggests that technical compliance alone does not establish legitimacy. Stakeholders must also perceive institutional processes as understandable, responsible, and appropriately controlled.

Fourth, institutional support is an important component of governance implementation. The studies of Thomas, The Greatest Showman, and Riwu (2024), Kurniawati et al. (2024), and Via and Cusmarih (2024) provide a conceptual basis for considering support relationships in institutional decision-making. Applied to government AI, cybersecurity governance requires coordinated support among technical, administrative, legal, managerial, and operational stakeholders.

Fifth, the strongest conceptual model is therefore an integrated governance architecture in which cybersecurity, privacy, ethics, organizational capacity, and accountability operate together. Security controls without privacy safeguards can increase rights-related risks; privacy rules without operational cybersecurity can leave information vulnerable; and either approach without employee competence may fail during implementation. The principal limitation is the heterogeneous nature of the supplied evidence. Most references do not directly investigate AI, government cybersecurity, or public-sector data governance.

Therefore, the findings should be interpreted as a conceptual synthesis rather than empirical validation of the proposed framework.

5. Discussion

The findings indicate that public-sector AI governance requires a shift from isolated security controls toward integrated institutional risk management. This interpretation is consistent with Ahmed's (2024) emphasis on balancing national security and privacy in government AI policy. The central implication is that security and privacy should not be designed as sequential objectives in which one automatically dominates the other. Instead, they should be incorporated into the same policy decision process.

The first major trade-off concerns data availability. AI systems often benefit from extensive datasets, while privacy governance encourages limitations on unnecessary data collection and access. A government institution therefore faces a structural policy tension: greater data availability may improve analytical capability but can simultaneously increase exposure to unauthorized use or inappropriate secondary processing. A governance framework should respond by connecting data access to clearly defined institutional purposes and risk levels.

The second trade-off concerns automation and accountability. AI can support administrative decision-making, but responsibility cannot be transferred entirely to an algorithm. Ethical governance requires identifiable institutional actors who remain responsible for deployment, monitoring, and corrective action. This is especially important when AI outputs influence public services or security decisions.

The third issue is organizational readiness. The supplied studies concerning knowledge, counseling, attitudes, and professional practice provide useful evidence that institutional interventions are shaped by human understanding and support (Zulfitriani et al., 2021; Stone et al., 2021). Public-sector AI governance should consequently incorporate role-specific training rather than assuming that publication of a cybersecurity policy will automatically result in compliance.

Stakeholder perception also deserves greater attention. Studies addressing attitudes and perceptions demonstrate the relevance of how individuals interpret interventions (Wemrell & Gunnarsson, 2022; Kurniawati et al., 2024). In government AI, lack of transparency may create distrust even where a system satisfies technical security requirements. Therefore, communication and explainability should be treated as governance mechanisms rather than merely public-relations activities.

The major limitation of this research is the mismatch between the central research topic and most of the supplied references. The healthcare-focused studies cannot establish direct causal relationships between AI governance practices and cybersecurity outcomes. Their value lies in supporting transferable organizational concepts such as knowledge, perception, communication, and institutional support. Future empirical research should therefore test the proposed framework using public-sector AI deployments, cybersecurity incident data, privacy-risk assessments, employee surveys, and stakeholder evaluations. Such research could determine whether the conceptual relationships identified here produce measurable improvements in security, privacy protection, and ethical accountability.

6. Conclusion

AI adoption in government creates a governance challenge in which national security, cybersecurity, data privacy, and ethical responsibility must be balanced rather than pursued independently. The analysis demonstrates that effective governance depends not only on technical safeguards but also on institutional knowledge, stakeholder communication, organizational support, ethical review, and clearly assigned accountability.

The conceptual framework developed in this study integrates five dimensions: security governance, privacy governance, ethical governance, organizational capability, and accountability. Its principal contribution is to position cybersecurity policy as an institutional governance process rather than merely a technical protection mechanism. Ahmed (2024) provides the direct foundation for the security–privacy balance, while the broader supplied literature supports the importance of knowledge, attitudes, perceptions, communication, and institutional support.

For public-sector institutions, the practical implication is that AI policy should incorporate continuous risk assessment, controlled data access, cybersecurity procedures, privacy safeguards, employee training, ethical oversight, and mechanisms for accountability. Future research should empirically validate these relationships using government-specific AI cases and quantitative measures of cybersecurity performance, privacy risk, organizational readiness, and public trust. Such research would strengthen the evidence base required for designing resilient and ethically responsible AI governance systems.

References

1. AB Venturin et al., “Open-Access Women's Experiences with the Post-Placental Intrauterine Device: A Qualitative Study,” Brazilian Journal of Gynecology

and Obstetrics, pp. 1-9, 2024.

2. Abrian Thomas, The Greatest Showman, and Rut Riwu, "Relationship Between Knowledge, Attitude and Husband Support with the Choice of Intrauterine Device in Kupang City Public Health Center in 2023," Journal of Food, Nutrition and Health, vol. 13, no. 1, pp. 44-57, 2024.

3. Amira Okud et al., "Knowledge, Attitudes, and Practice About Emergency Contraception Among Saudi Women of Childbearing Age of Eastern Region in Saudi Arabia," Cureus, vol. 15, no. 11, pp. 1-14, 2023.

4. Asti Inka Pratiwi, "Overview of Knowledge of Women of Fertile Age About Iud Contraception in Grand Vienna Housing Complex, Kenali Asam Village, Kota Baru District," Midwifery Health Journal, vol. 9, no. 1, pp. 137-140, 2024.

5. Lilis Purwati, Wijayanti, and Tresia Umarianti "Relationship Between Education Level And Perception Of Choosing Intra Uterine Device (Iud) Contraception In Iud Kb Acceptors At Karangpandan Community Health Center," Al-Insyirah Midwifery: Journal of Midwifery Sciences, vol. 13, no. 2, pp. 105-110, 2024.

6. Lise Kurniawati, Rindu, and Ageng septa Rini, "Relationship between Knowledge, Attitude and Perception of Husbands with the Use of IUD Contraceptives in the Haurwangi Health Center Work Area, Cianjur Regency in 2023," Innovative: Journal of Social Science Research, vol. 4, no. 2, pp. 7706-7719, 2024.

7. Lucy Stone et al., "Assessing Knowledge, Attitudes, and Practice of Health Providers towards the Provision of Postpartum Intrauterine Devices in Nepal: A Two-Year Follow-Up," Reproductive Health, vol. 18, pp. 1-11, 2021.

8. Maria Wemrell, and Lena Gunnarsson, "Attitudes Toward the Copper IUD in Sweden: A Survey Study," Frontiers in Global Women's Health, vol. 3, pp. 1-15, 2022.

9. Mariama S. Tounkara et al., "A Mixed-Methods Study of Factors Influencing Postpartum Intrauterine Device Uptake After Family Planning Counseling among Women in Kigali, Rwanda," PLoS One, vol. 17, no. 11, pp. 1-15, 2022.

10. Nur Azizah, Elvi Murniasih, and Mira Agusthia, "Factors Related to the Incidence of Hyperemesis Gravidarum in Pregnant Women at Tanjungpinang City Hospital," Jurnal Inovasi KesehatanAdaptif, vol. 5, no. 4, pp. 71-85, 2023.

11. S. Gustika, D. C. Yun, and Dan A. W. Nainggolan "Factors that Influence the Low Interest of Women of Childbearing Age in Choosing an IUD Contraceptive Device in Uring Village, Pegasing District, Southeast Aceh Regency, 2022," STIKes Ibnu Sina Ajibarang, vol. 2, no. 4, 2024.

12. Samson Peter Mvandal, Joseph Nhandi, and Godfrey Lupoly, "Knowledge and Attitude concerning use of Intrauterine Contraceptive Device among Women attending Family Planning at Makambako RCH in Njombe-Tanzania," Preprints, pp. 1-9, 2020.

13. Vika Chita Via, and Cusmarih Cusmarih, "The Relationship Between the Role of Health Workers, Knowledge and Husband's Support on the Selection of IUD KB Acceptors at the Keagungan Village Health Center in 2023," Formil Journal (Scientific Forum) of Respati Public Health, vol. 9, no. 1, pp. 76-86, 2024.

14. W. Kerja, P. M. B. Dewi, dan S. Keb, "The Effect of IUD Birth Control Counseling Using Sheet Media to Become a Postpartum Birth Control Birth Control Acceptor," hal, pp. 8–14, 2023.

15. Zulfitriani Zulfitriani et al., "Counseling to Increase Knowledge of Women of Childbearing Age (WUS) about IUD Contraceptives," Community Empowerment, vol. 6, no. 3, pp. 374-379, 2021.

16. Ahmed, F. (2024). Cybersecurity policy frameworks for AI in government: Balancing national security and privacy concerns. Int. J. Multidiscip. Sci. Manag, 1(4), 43-53.

17. Ramamurthy, K. (2023). AI-Driven Test Automation Frameworks for the Modern Software Quality Engineering. International Journal of Emerging Trends in Computer Science and Information Technology, 4(4), 257-269.

18. Geo Philip, Paulson, Integrated Intelligent Building Energy Management: A Multi-LayerFramework for Renewable Energy, HVAC Optimization, and SmartElectrical Network Coordination. Available at SSRN: https://ssrn.com/abstract=6993209 or http://dx.doi.org/10.2139/ssrn.6993209