Golden Sun-Rise
International Journal of Multidisciplinary on Science and Management
ISSN: 3048-5037/ Volume 1 Issue 4 December 2024 / Page No: 43-53
Paper Id: IJMSM-V1I4P107 / Doi:10.71141/30485037/V1I4P107

Original Article

Cybersecurity Policy Frameworks for AI in Government: Balancing National Security and Privacy Concerns

Faraz Ahmed
Crisp Technologies LLC, Cybersecurity researcher.

Received: 14 October 2024 Revised: 25 October 2024 Accepted: 04 November 2024 Published: 20 November 2024

Abstract: *The Integration of artificial intelligence (AI) in government cybersecurity frameworks present both transformative opportunities and unprecedented challenges. AI makes it easier to detect threats, respond to it automatically and protect critical infrastructure, but at the same time, it presents complex risks including AI enabling cyberattacks, privacy violation from mass surveillance and ethical issues of algorithmic bias. This research examines the delicate balance policymakers strike between using AI for national security and protecting fundamental civil liberties. Through the analysis of cybersecurity frameworks, such as NIST, ISO and COBIT the research identifies main gaps for addressing AI specific vulnerabilities like adversarial machine learning and data poisoning attacks. Contemporary case studies from today show the duality of AI in cybersecurity, where it can protect digital ecosystems and sophisticated threats like deepfake enabled disinformation campaigns and autonomous hacking tools. The research provides actionable policy solutions such as the adoption of privacy preserving AI techniques, e.g., federated learning, implementation of zero trust architectures and development of international governance standards to govern the distribution of ethical AI. However, the findings were also crucially pointing that for any AI cybersecurity policy to be effective it has to be dynamic, with the ability to constantly adapt to technological advancements while maintaining robust safeguards of individual rights. Taken together, the research provides a way for governments to tap into AI's defensive side without compromising on democratic values and outlines actionable steps to find the right balance between the need for security and the protection of privacy around an ever more AI driven world.*

Keywords: *Artificial Intelligence; Cyber Security; Policy Framework; NIST; ISO*

I. INTRODUCTION

In a era when everything has gone digital and there is a rapid development of artificial intelligence, security has become a key in national security and economic stability. As AI-driven technologies has become integral to government operations, it contains both great opportunities and complex security challenges. However, governments worldwide are prioritizing AI driven cybersecurity policy frameworks to protect critical infrastructure and public trust as well as sensitive data. The advanced persistent threats, AI powered cyberattacks, and state sponsored cyber warfare are the conformation of urgent need for covering security and adaptive security strategies.

Governments need AI-based cybersecurity policy frameworks to preserve their defense nationwide against ever changing digital threats by being navigating the tension between national security exigencies and citizen privacy. During the digital transformation era, governments' role has evolved considerably in terms of the adoption of AI in Automation in public services, Automated decision making and data driven governance [1–3]. However this transformation brings its own challenges especially in the area of cybersecurity where governments are storing a huge amount of confidential data, making them ideal targets to cybercriminals and hostile entities [4–6].

Fig. 1 clearly shows the frequency and sophistication of cyber attacks on government institutions, especially local government (OECD data, 142 Ransomware, 53 AI powered attack in 2023 to 2024 according to Under Fire 2024), which results from the shortage of funding, inadequate security infrastructure, and lack of AI security

expertise [7,8]. The figure 1 depicts the comparative sector data and shows that although local governments receive less attention in cybersecurity discussions, they suffer nearly 2.5 times more incidents than federal agencies due to their inability to achieve regulatory compliance and the lack of allocation of resources.

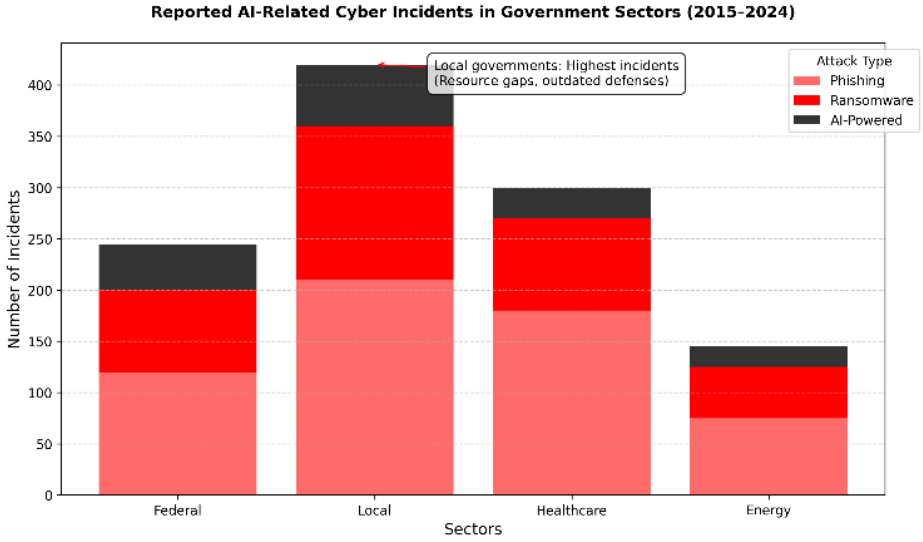

Figure 1. AI-Related Cyber Incidents in the Government Sector (2015–2024)

The challenge extended beyond cybersecurity in the area of AI governance to broader issues of ethical AI Deployment, transparency, and compliance with privacy regulations are distributed. As tools to manage this delicate balance between protecting national interests and the freedoms for individuals, cybersecurity policy frameworks provide structured approaches. Security standards and guidelines that effectively integrate and extend such frameworks into AI driven threat detection, risk management and response technologies are embodied in these frameworks. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework [9] is a risk-based approach to managing AI-controlled cybersecurity threats. It uses industry standards and good practices to help organizations understand, express, and manage AI security risks. Analysing the framework's core functions or what it is called Identify, Protect, Detect, Respond, and Recover provides a strategic visioning for securing AI-powered government systems. Like COBIT, the Control Objectives for Information and Related Technologies (COBIT) framework also ensures that the IT and AI security goals align to the business goals and are governed and managed by the enterprise AI technologies throughout its lifecycle. The Controls Oriented Business Integration and Technology (COBIT) is set of controls and metrics that contribute to good risk management and resource optimisation, developed by ISACA.

In the international arena, BSA | The Software Alliance amongst other organizations have developed such an international cybersecurity policy framework [10], which advocates for the policies geared toward AI to be i) technology neutral, ii) outcome focused, iii) risk based, iv) to be in line with internationally acknowledged standards. The framework emphasizes the necessity of public-private collaboration in the AI security and the need of balancing technology and privacy. Governments must adopt agile and adaptive policies to govern AI driven cybersecurity framework that effectively govern the security threats and at the same time are ethically and legally sound. Encryption backdoors have become a critical topic of debate within the domain of AI cybersecurity governance: as their use constitutes the enforcement of national security imperatives at the expense of the protection of individual's privacy rights. The policy must guarantee security but not infringe upon civil liberties disproportionately.

The next step for governments is having to tread carefully between the conflicting interests of security and privacy in light of the increasing impact that AI is having on cybersecurity policies. Policies, industry leaders, and civil society together coordinate development of AI driven cybersecurity frameworks that advance security, yet maintain basic rights. This research will review the developments of AI driven cybersecurity policy frameworks towards national security and privacy matters. Furthermore, it examines the major trade-off between AI cybersecurity strategies and legal, ethical and civil liberties priorities. It then presents policy recommendation and AI driven cybersecurity solutions that would promote a more balanced security and privacy in today's networked world.

II. BACKGROUND

Artificial intelligence is integrated into cybersecurity has significantly transform the use of digital defense mechanisms. This section discusses the evolution of cybersecurity policies in the backdrop of the AI advances and limitations of existing approaches in tackling risks around AI.

A. Evolution of Cybersecurity Policies with AI

Traditionally, cybersecurity policy applied a reactive perspective, treating them by defining policy before responding to known threats, usually through rules and manual interventions. The emergence of AI brought some sort of a paradigm shift to proactive, adaptive security strategies. Machine learning algorithms have been used to detect anomalies, predict potential breaches and automate responses to cyber threats using the powers of Machine Learning. Thanks to this transition, the organizations are able to cope with increasing the volume and complexity of cyber threats more efficiently.

The evolution of cybersecurity policies alongside AI advancements can be summarized as follow:

Table 1: Evolution of Cybersecurity Policies with AI.

Phase	Key Characteristics	Impact on Cybersecurity
Pre-AI Era (Reactive Policies)	Focused on predefined rules and manual interventions to mitigate known threats.	Limited adaptability; struggled with emerging cyber threats.
AI-Driven Cybersecurity (Proactive Approach)	AI and machine learning introduced anomaly detection, breach prediction, and automated responses.	Enhanced threat detection and faster response to cyber incidents.
Data-Driven Policymaking (2010-Present)	AI-driven decision-making optimizes policies based on large datasets and real-time insights.	Improves accuracy, efficiency, and cost-effectiveness of cybersecurity policies.
AI in Governance & Public Policy	AI supports decision-making in climate policies, cybersecurity, and digital identity security.	Strengthens cyber defenses while enabling more transparent and adaptive policymaking.

The fourth industrial revolution and its progression i.e. digital transformation are provoking governments to infuse AI in policymaking for better decision making. Since complete, biased or politician directed policy doesn't exist, data driven policymaking has emerged since 2010 which overcomes the problem of data[11]. By analysing large amounts of data, AI lets a government do accurate, efficient, cost effective, services. Other models such as Solo's computational public policy framework (technocratic and e-governance) [12] take advantage of mathematical models of policy followed by AI simulations. AI is already helping shape the policies in the European Union that relate to climate [13], and governments across the world use AI to help run operations and public services. AI driven policymaking is strengthened by predictive analytics and pattern detection but is still in early stages, for the full scale adoption [14]. Policymakers can instead rely on AI to offer an undistorted, evidence based, structured framework, rather than becoming an end of the human decision making process. Zhijing Jin [15] introduces NLP tools and ML algorithms that leverage public concerns from news, social media, reports to fill in the gap of communication between citizens and policymakers.

At the same time that AI is transforming governance, it is also reshaping national cybersecurity strategies. Emerging policy directions reflect this shift. For instance, President Joe Biden signed an ambitious executive order focused on artificial intelligence, aiming to balance innovation with national security and consumer protection[37]. The order urges federal agencies to harness AI to bolster their cybersecurity postures, including initiatives for AI-driven cyber defense, mandatory cybersecurity standards for federal software vendors, and expanded use of digital identity credentials. It also introduces the Cyber Trust Mark for internet-connected devices. Biden emphasized that AI is advancing at "warp speed," and the order represents an early attempt to establish guardrails ensuring that AI remains trustworthy and beneficial, rather than deceptive or dangerous. While the executive order lays a foundational framework, it is expected to be reinforced by future legislation and international cooperation to comprehensively govern AI in the context of national security.

Pakistan's 2021 climate change policy is an example of AI policymaking. Climate risks can be predicted, public concerns assessed, and adaptive policy recommendations made in real time, with real results, in response,

and with transparency[19]. Indeed, these are promising developments that indicate how AI is disrupting not only governance and public policy, but also cybersecurity by improving defences while enhancing efficiency.

B. Limitations of Existing Approaches in Addressing AI-Related Risks

Although AI provides some breakthroughs in cybersecurity, the existing policies and frameworks struggle in creating effective ways to deal with AI related risks:

- *Malicious Actors and Evolving Threat Landscape:* Malicious actors have also harnessed AI technologies for developing advanced cyber threats like deepfakes and AI driven phishing attacks. Although these novel threats may not be sufficiently detected or mitigated by traditional cybersecurity policies [16].
- *Regulatory Gaps and compliance*: In the field of AI technologies, the lack of comprehensive regulatory frameworks, which developed slowly, lags behind the rapid development of AI technologies. The ensuing lag is exploited to fill holes that result in inconsistent compliance and enforcement in different jurisdictions. The New York State Department of Financial Services[17] released guidance for financial institutions to mitigate AI related cybersecurity risks in October 2024 such as refreshing the risk assessments and policies.
- *Ethical and Privacy Concern:* There are also problems of ethical and privacy involved in the way AI is used in the cybersecurity field. Although AI systems can have unintended negative impacts on individual privacy rights as well as fairness. This poses a major challenge of ensuring transparency, and accountability, and fairness, in AI driven steps of cybersecurity [18].
- *Resource Constraints and Skill Gaps:* Implementing an AI based cybersecurity solution. Small organizations and local governments in particular, for example, may not possess the expertise and financial substance to purchase, implement, and maintain such staying in front of frameworks, making them open to AI empowered web security dangers.

These limitations have to be resolved with the development of adaptive, comprehensive cybersecurity policies that include AI specific considerations. To effectively mitigate AI risks while fostering innovation and safeguarding individual rights, there are collaboration efforts between policymakers, industry leaders and academic researchers in such framework.

III. AI-CENTRIC CYBERSECURITY POLICY FRAMEWORKS IN GOVERNMENT

The rapid integration of Artificial Intelligence (AI) into government operations now present risks and opportunities therefore artificial intelligence centric cybersecurity policy framework is needed with a view of national security and protecting the privacy principles. Governments around the world are adopting the security standards and frameworks to circumvent the AI related threats and also to meet the legal and ethical standards. Following this, this section offers up cybersecurity frameworks that are useful for the governance of AI, and then looks at the solutions that resolve these security and privacy challenges in the AI enabled government deployments.

A. The Role of Cybersecurity Standards and Frameworks in AI Governance

Cybersecurity standards and frameworks specify structured mechanism and methods for performing security controls, risk management, and compliance in an AI system. It may be said that these frameworks can be classified under a broader scope into information security standards (e.g. ISO 27000 series or NIST SP 800) and governance standards (e.g. COBIT or NIST CSF) [20]. The combination of multiple standards is necessary because of the complexity of the AI systems, and governments on ground usually only have reasonable security coverage for such systems [21].

ISO/IEC 27000 Series for AI Security: The ISO/IEC 27000 series is used for the best practice specification for the governance of the AI driven government systems. Key standards include:

- ISO/IEC 27001: There are requirements in terms of developing, implementing and maintaining an ISMS, which is a precondition for AI systems, that process sensitive data [10].
- ISO/IEC 27002: Covers AI specific risks such as adversarial attacks, data poisoning [23][32].
- ISO/IEC 27005: Covers the management of risk in relation to threat of AI like theft of model, data privacy, and bias [24].

While the ISO 27000 series includes no provision for all challenges of AI, the Challenges of AI are not codified and need further supplemental frameworks [25].

NIST Cybersecurity Framework (CSF) for AI Risk Management: As a government system risk, the implementation of the NIST CSF, which was developed using the Cybersecurity Enhancement Act of 2014[9], allows a flexible means of managing the AI cybersecurity risk within government systems. Here are the five core functions that have to follow in AI governance: identify, protect, detect, respond, recover.

- Identify: Assess AI system vulnerabilities, data sources, and threat landscapes.
- Protect: Encrypt and control access on AI models.
- Detect: Deploy AI-driven anomaly detection for cyber threats.
- Respond and Recover: Create AI incident response plans for breaches[44].

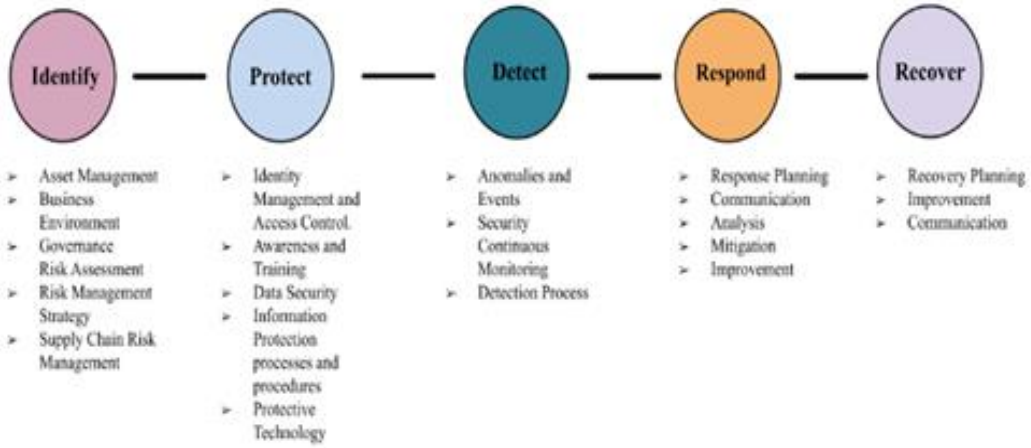

Figure 2. NIST Cybersecurity Framework (CSF) Core Functions for AI Risk Management

The NIST Privacy Framework further complements AI governance by addressing data privacy risks, ensuring compliance with regulations like GDPR and CCPA[26].

B. AI-Specific Cybersecurity Challenges and Framework Adaptations

Adversarial Attacks and Model Security: AI systems are vulnerable to adversarial attacks, where malicious inputs deceive models(e.g., deepfake manipulation in government surveillance) The descriptions of a few of the controls available in the NIST SP 800 – 53 standard used to secure the AI model against these kinds of threats are outlined briefly.

- Input validation to detect Adversarial samples
- Model hardening techniques like adversarial training [27].

Data Privacy and Ethical AI: AI system in government must comply with privacy laws while ensuring privacy. The ISO/IEC 27018 (cloud privacy), ETSI EN 303 645 (iot security) [24,28] standards are relevant for AI deployments involving personal data processing. These ethical AI principles are useful for them to follow as per the NIST's Privacy Framework.

- Data minimization (collecting only necessary data).
- Explainability (ensuring AI decision are auditable)[45]

The risk of supply chain in AI systems: Besides, these machine learning models are as dependent as on the 3rd party dataset and the libraries as well, which means they are at same risk of supply chain. NIST SP 800-161 (supply chain risk management) and IEC 62443 (industrial cybersecurity) have guidelines to security in the AI supply chain. [29].

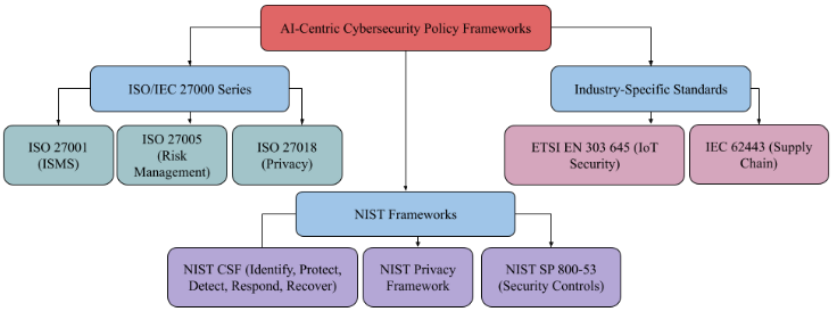

Figure 3. Taxonomy of AI cybersecurity governance frameworks

IV. POLICY RECOMMENDATIONS FOR AI-CENTRIC CYBERSECURITY IN GOVERNMENT

Some of the sensitive national security concerns will require a hybrid regulation in governments, that integrate existing cybersecurity framework with AI-specific . Below are key recommendations:

A. Mandatory AI Security Certification

These should be the mandatory compliance certification that should be implemented for the public sector application of any AI systems ISO 27001 (ISMS) and NIST CSF (this, a model for the management of the risk) [22]. It helps putting the baseline level of the security controls such as data encryption, access management and incident response protocol.

B. AI-Specific Risk Assessments

NIST SP 800-30 should identify what are the latest advances in adversarial attacks, model bias and data leakage to be mandated to use through continuous risk evaluations. Furthermore, NIST SP 800-37 (Risk Management Framework) guide the detection, in real time, of these new AI threats like the deep fake manipulation, and the modelling poisoning [27].

C. Zero Trust Architecture (ZTA) for AI Systems

To end up the insider threats and lateral movement in government's AI cybersecurity frameworks, we must integrate Zero Trust Architecture. Perhaps AI powered, real time threat monitoring is best suited to Continuous Authentication and Least Privilege which were definitely consciously intended for use with ZTA that was specified in NIST SP 800-207 [36]. An attempt to reduce the incidence of breach of sensitive data can be made in the threat of breach that can occur on AI systems processing such data.

D. Public-Private Collaboration

Governments should base their AI and cyber policies on the emerging COBIT governance principles and align them with the private sector's best practice guidelines [30]. Further that would be other cooperative types of activities that would be threat intelligence sharing and other AI red teaming type exercises to stress test the defense.

E. Ethical AI & Privacy-by-Design

ISO/IEC 27018 is integrated with the study of AI systems for data minimization, explainability and user consent which are conformant to an additional values from the Privacy Framework [24]. It is highly critical for such applications of high risk, as surveillance AI or automated decision making. To effectively safeguard AI-driven government systems, policymakers must establish a dynamic cybersecurity framework that evolves alongside emerging AI threats. By integrating standardized security controls, AI-specific risk assessments, and ethical governance principles, governments can create resilient AI ecosystems that uphold both national security and individual privacy. As AI-powered cyber threats continue to evolve, the next section delves into their implications for national security, examining real-world cases of AI-driven vulnerabilities and the defense strategies necessary to counteract them.

V. NATIONAL SECURITY IMPERATIVES IN AI CYBERSECURITY

AI has wakened the window of new opportunities but in the area of Defense and Intelligence the development is overwhelming. It improves capability to automated threat detection, predictive analytics, real time response and national security enhancement. These advances indeed involve a number of troublesome issues when it comes to encryption and, in doing so, they introduce new complexity into the realization of such backdoors. These measures are aim to provide government an access to encrypted communication but raise critical concern about balancing national security interest with preservation of individual AI.

AI's dual nature presents a unique dilemma: while it strengthens security measures, it also equips malicious actor with sophisticated tools for cyberattacks. Criminal networks acting on behalf of someone's interest, even the state's are leveraging AI to enhance their operation. AI driven attacks are seen as having authority in the ability to generate believable messages for a select audience; making an opportunity to fool and harvest data. In addition, it gives rise to development of state of the art malware and deep fakes, and the highly sophisticated targeted cyberattack on critical infrastructure, which have no precedent [31].

A. Explainability and Accountability in AI-Driven Incident Response

AI-driven cybersecurity decisions must be explainable to ensure accountability, particularly in national security contexts. For instance, if an AI system flags a false positive in surveillance, agencies must provide

auditable reasoning to prevent wrongful actions. Frameworks like NIST's Explainable AI (XAI) and the EU's AI Act's transparency requirements should be incorporated into incident response protocols. This is critical to:

- Justify automated decisions (e.g., blocking access, throttling traffic) to avoid legal challenges.
- Detect and mitigate bias in AI models used for threat detection.
- Align with due process in law enforcement and intelligence operations.

Governments should mandate interpretable AI models (e.g., decision trees, rule-based systems) for high-stakes security applications, supplemented by human-in-the-loop (HITL) oversight to review AI-generated alerts.

B. Case Studies Illustrating AI in Cyber Defense

Real-world applications demonstrate AI's impact on cybersecurity:

- Collaborative AI Cybersecurity Initiatives: The Joint Cyber Defense Collaborative (JCDC) [35] has released an AI Cybersecurity Collaboration Playbook to guide organizations in protecting AI systems from cyber threats. This initiative underscores the importance of collaboration between government agencies and industry partners to develop robust AI-driven defense strategies.
- Enhancing Cyber Defense with Multi-Dimensional Decision-Making: An intelligent logistics company implemented a discrete multidimensional decision-making approach to assess network security. This AI-driven method significantly improved the accuracy and efficiency of decision-making in cyber defense, demonstrating the practical benefits of AI applications [34].

VI. POLICY FRAMEWORKS AND LEGAL CONSIDERATIONS IN AI SURVEILLANCE

The integration of Artificial Intelligence (AI) into surveillance systems has significantly enhanced national security capabilities, yet it has also sparked concerns regarding privacy and civil liberties. Establishing comprehensive policy frameworks and legal regulations is essential to balance these interests. To balance these interests, comprehensive policy frameworks must mandate human-in-the-loop (HITL) controls for high-stakes AI decisions (e.g., cyber threat escalation, biometric identification) to ensure accountability and mitigate bias. Additionally, governments should institutionalize regular red-teaming exercises, where ethical hackers probe AI systems for vulnerabilities, to identify blind spots in automated defenses and align with transparency principles. Such measures, combined with legal safeguards, can optimize AI's security benefits while upholding fundamental rights.

A. Guiding Principles for AI Surveillance

To ensure responsible AI usage, several guiding principles have been proposed:

- Lawful and Mission-Appropriate Use: AI applications must comply with constitutional and legal standards, protecting privacy and civil liberties [33].
- Transparency and Accountability: Governments should operate AI surveillance systems transparently, providing clear information about their purpose and functioning to foster public trust.
- Risk Assessment and Mitigation: Prior to deployment, AI systems should undergo evaluations to identify potential risks to privacy and civil liberties, with strategies implemented to mitigate identified risks.

B. Legal Challenges and Regulatory Responses

The use of AI in surveillance has led to legal disputes concerning privacy violations:

- *Clearview AI Case:* Clearview AI faced multiple lawsuits alleging unauthorized collection of biometric data, raising concerns about consent and potential systemic injustice.
- *GDPR Enforcement:* In September 2024, the Dutch Data Protection Authority fined Clearview AI €30.5 million for violations of the EU's General Data Protection Regulation (GDPR), highlighting the extraterritorial reach of data protection laws.

C. Evolving Policy Initiatives

To address these challenges, various policy initiatives have been introduced:

- *AI Bill of Rights:* The White House's Office of Science and Technology Policy released a Blueprint for an AI Bill of Rights, outlining principles to protect individuals from the risks associated with AI, including those used in surveillance.
- *National Security Guidelines:* New rules guiding the use of AI by U.S. national security agencies aim to leverage AI capabilities while safeguarding against risks like mass surveillance and cyberattacks.

These developments underscore the need for robust policy frameworks and legal considerations to ensure that AI-driven surveillance systems respect privacy and civil liberties while serving legitimate security interests.

VII. POLICY RECOMMENDATIONS FOR AI SECURITY-PRIVACY BALANCE

As more Governments around the world adopt these technologies, they are thus supposed to help to further their capability to bolster their core cybersecurity posture of increased detection time, speed to response and resiliency. With its capability of utilizing vast amounts of data in real time and predict potential cyber threats that can cast a shadow on the national infrastructure and compromised data, it is because of this that AI is getting popular for use in such fields. Meanwhile the proliferation of use of AI has its own impact on privacy and civil liberties and the policymakers need to form policies between benefits of AI and personal freedom.

As models are trained more often than cross border data flows, they should be able to equally be able to address cross border data flows. The data in these datasets may even be in violation of the data sovereignty rules of the EU (such as the GDPR) or China's data localization rules. Governments should try to find the way of bilateral agreements in the monitoring of security of data, and find a way of solving the conflict of jurisdiction, as in figure 5, that is, using the solution like federated learning in management of the effect of the trade-off of jurisdiction over the efficiency of AI.

Furthermore, AI systems for integration into existing cybersecurity infrastructure must not contravene national security objectives and systems of integration must respect legal and ethical standard of data privacy. Governmental use of AI for cybersecurity is enabled while the individual liberty and trust are not compromised as well as the trust and security that people have with the use of AI technologies for the protection of the government's cybersecurity.

VIII. KEY POLICY CONSIDERATIONS

A. Privacy-Preserving AI Technologies

These kinds of Privacy Preserving AI technologies will work in the governments and will develop trust of the public power. One such technique includes federated learning where we train an AI model that couldn't have been possible without sharing the sensitive data, but instead, are able to do so by training with data from a remote source. Homomorphic encryption is another way to guarantee privacy, and being able to analyse a data after processing it. And therefore, governments should also take develop and deploy of transparent and accountable AI systems very seriously. It is in this case's meaning that ideally, mandates should exist for AI systems to generate explainable result when necessitated, for example when the on the result from AI systems influence national security or privacy of real people.

B. Ethical and Legal Standards

Ethical standards are often the cornerstone for deployment of AI for national security purposes. A good example of this is that governments should have a framework from which they have to adhere to the ethical use of AI ,Facial recognition or predictive analytics should not be done without an ethical use. These ethical considerations must address concerns related to algorithmic bias, fairness, and the potential for misuse in law enforcement or surveillance. Furthermore, international human rights frameworks should be a key part of such policies to prevent any infringement of privacy rights or the international effort of mass surveillance by AI based cybersecurity. The same is true of legal reforms which should be adopted to avoid the use of AI technologies in such a way that would violate civil liberties.

C. Stakeholder Engagement

There are therefore multiple stakeholders to be involved in the implementation of AI in cybersecurity, i.e, government agencies, private industry, academia and civil society. Therefore, there is potential to encourage collaboration between these sectors when it comes to developing government cybersecurity policies related to AI.

- Government Agencies must lead the regulatory efforts, ensuring that AI technologies comply with legal frameworks and align with national security goals.
- Private Sector involvement is crucial in ensuring that AI technologies are developed responsibly, with built-in privacy protections.
- Academic Institutions play a significant role in advancing research on AI's applications in cybersecurity and developing new privacy-presrving techniques.
- Civil Society can offer valuable insights on the societal impact of AI systems, advocating for privacy rights and transparency.

IX. INTERNATIONAL PERSPECTIVES ON AI GOVERNANCE

As AI technologies are transnational, they require global protection to privacy, and so, this technology needs to have global cybersecurity standards as well. On the subject of data protection and people's rights, which we would say is ahead on the curve on AI governance, the European Union has started in the General Data Protection Regulation (GDPR). For example, the policy of China and United States and other countries with regard to their AI policy also consider privacy and surveillance respectively, but make their own qualifiers that have something to do with national security. Consequently, this issue is of great importance in that regard of international human rights standard, in terms of evolving in a form that is based globally and from a multi stakeholders point of view to ensure that the framework of the AI governance will not give place to misuse legality of the AI technology that tends to violate privacy or individual freedom. As a response to the incremental threat of national security interests versus privacy issues, ongoing dialogue will create a constitutional governance framework of technology for AI, which is balanced and ethical.

Variety of governments around the world are channeling AI technologies to help secure their national security and individual rights. The combination of this, support for clear ethical guidelines, and cooperation between the countries will result in an environment of cybersecurity where the national infrastructure cybersecurity will rely on the solutions that protect it using AI for the protection but without harming the privacy of citizens. This path forward it is about balancing protecting the fundamentals and letting it innovate, but policies. Collaborative development and deployment for the advance cybersecurity with transparency, ethic, privacy conscious, and responsible on the part of all the stakeholders.

X. CONCLUSION

The transformative power of AI in government cybersecurity presents both extraordinary promise and profound responsibility. As nations race to adopt AI-driven security solutions, they must confront fundamental questions about the kind of digital society they wish to build. The tension between security imperatives and privacy rights has never been more acute. AI-powered surveillance systems, predictive policing algorithms, and automated threat detection tools are rewriting the boundaries of state power and individual freedom. However, this technological revolution need not come at the cost of civil liberties. The solution lies in developing intelligent governance frameworks that are as sophisticated as the AI systems they regulate. Three critical pillars must guide this effort: First, robust technical safeguards including mandatory AI security certifications, explainability requirements, and privacy-preserving technologies like homomorphic encryption. Second, institutional reforms that ensure proper oversight through independent AI ethics boards, algorithmic impact assessments, and clear accountability mechanisms. Third, international cooperation to establish baseline standards for responsible AI use in cybersecurity, preventing a dangerous race to the bottom in surveillance capabilities.

The path forward demands more than just better technology it requires a fundamental rethinking of how democratic societies balance security and liberty in the digital age. Governments that succeed in this balancing act will not only be more secure, but will preserve the trust and confidence of their citizens. As AI continues to evolve at breakneck speed, policymakers must demonstrate equal agility in crafting regulations that keep pace with technological change while protecting foundational rights. The ultimate test of AI-enhanced cybersecurity won't be whether it stops every attack, but whether it does so in ways that strengthen rather than undermine democratic values. The choices made today will determine whether AI becomes a tool for protecting freedom or a weapon for its erosion making this one of the defining governance challenges of our time.

XI. REFERENCES

1. Rotta, M.J.R.; Sell, D.; dos Santos Pacheco, R.C.; Yigitcanlar, T. Digital commons and citizen coproduction in smart cities: Assessment of Brazilian municipal e-government platforms. Energies 2019, 12, 2813.
2. Micozzi, N.; Yigitcanlar, T. Understanding smart city policy: Insights from the strategy documents of 52 local governments. Sustainability 2022, 14, 10164.
3. Yigitcanlar, T.; Agdas, D.; Degirmenci, K. Artificial intelligence in local governments: Perceptions of city managers on prospects, constraints and choices. AI Soc. 2023, 38, 1135–1150
4. Norris, D.F.; Mateczun, L.; Forno, R. Cybersecurity and Local Government; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2022.
5. Norris, D.F.; Mateczun, L.; Joshi, A.; Finin, T. Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. Public Adm. Rev. 2019, 79, 895–904.
6. Norris, D.F.; Mateczun, L.K. Cyberattacks on local governments 2020: Findings from a key informant survey. J. Cyber Policy 2022, 7, 294–317.
7. Wolff, J.; Lehr, W. When cyber threats loom, what can state and local governments do? Georget. J. Int. Aff. 2018, 19, 67–75.

8. Hatcher, W.; Meares, W.L.; Heslen, J. The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. J. Cyber Policy 2020, 5, 302–325.
9. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce, 2018. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
10. BSA | The Software Alliance. Cybersecurity Frameworks and Best Practices: Recommendations for a Secure and Resilient Digital Economy. 2021. Available at: https://www.bsa.org/files/reports/bsa_cybersecurity_frameworks.pdf.
11. Newman, J.; Mintrom, M. Mapping the discourse on evidence-based policy, artificial intelligence, and the ethical practice of policy analysis. J. Eur. Public Policy 2023, 30, 1839–1859.
12. Solo, A.M. The new fields of public policy engineering, political engineering, computational public policy, and computational politics. In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and eGovernment (EEE), Las Vegas, NV, USA, 18–21 July 2011.
13. Cowls, J.; Tsamados, A.; Taddeo, M.; Floridi, L. The AI gambit: Leveraging artificial intelligence to combat climate change Opportunities, challenges, and recommendations. AI Soc. 2023, 38, 283–307.
14. Kolkman, D. The usefulness of algorithmic models in policy making. Gov. Inf. Q. 2020, 37, 101488.
15. Jin, Z.; Mihalcea, R. Natural language processing for policymaking, in Handbook of Computational Social Science for Policy; Springer International Publishing: Cham, Switzerland, 2022; pp. 141–162.
16. Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. Journal of Computers, Mechanical and Management, 2(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064.
17. Reuters, "New York Department of Financial Services provides AI cybersecurity guidance: What to know," Reuters, Nov. 15, 2024. [Online]. Available: https://www.reuters.com/legal/legalindustry/new-york-department-financial-services-provides-ai-cybersecurity-guidance-what-2024-11-15/.intelligence
18. Hashmi, E., Yamin, M.M. & Yayilgan, S.Y. Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. AI Ethics (2024). https://doi.org/10.1007/s43681-024-00529-z.
19. M. A. Yar, M. Hamdan, M. Anshari, N. L. Fitriyani, and M. Syafrudin, “Governing with intelligence: The impact of artificial intelligence on policy development,” Information, vol. 15, no. 9, p. 556, 2024.
20. Arora, V. Comparing Different Information Security Standards: COBIT vs. ISO 27001; Carnegie Mellon University: Doha, Qatar, 2010.
21. Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. Analysis of cybersecurity standard and framework components. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 417–432
22. Tofan, D. Information Security Standards. J. Mob. Embed. Distrib. Syst. 2011, 3, 128–135.
23. Rumiche Huamani, R.E. Implementación de un Plan de Seguridad Informática Basado en la Norma ISO IEC/27002, Para Optimizar la Gestión en la Corte Superior de Justicia de Lima; Universidad Privada del Norte: Trujillo, Peru, 2022.
24. Azmi, R.; Tibben, W.; Win, K. Review of cybersecurity frameworks: Context and shared concepts. J. Cyber Policy 2018, 3, 258–283.
25. Cordero, J.A.V. Les normes ISO/IEC com a mecanismes de responsabilitat proactiva en el Reglament General de Protecció de Dades. IDP Rev. Internet Derecho Y Política Rev. D’internet Dret I Política 2021, 33, 7.
26. NIST. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management; U.S. Departement of Commere National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; p. 43.
27. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. IEEE Access 2021, 9, 121975–121995.
28. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. Comput. Secur. 2021, 102, 102136.
29. Leander, B.; Cauševi´c, A.; Hansson, H. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In ˇ ARES ’19, Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26 August 2019; Association for Computing Machinery: New York, NY, USA; Canterbury, UK, 2019; pp. 1–8.
30. Institute, I.G. Aligning COBIT, ITIL and ISO for Business Benefit: Management Summary. A Management Briefing from ITGI and OGC. IT Gov. Inst. 2005, 1, 5–62.
31. Montasari, R. (2022). Cyber Threats and National Security: The Use and Abuse of Artificial Intelligence. In: Masys, A.J. (eds) Handbook of Security Science. Springer, Cham. https://doi.org/10.1007/978-3-319-91875-4_84
32. Salem, Aya & Azzam, Safaa & Emam, O. & Abohany, Amr. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data. 11. 10.1186/s40537-024-00957-y.
33. G. Buchholtz, “Artificial intelligence and legal tech: Challenges to the rule of law,” in Regulating Artificial Intelligence, Cham: Springer International Publishing, 2019, pp. 175–198..
34. M. Malatji and A. Tolah, “Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI,” AI and Ethics, pp. 1–28, 2024.
35. Cybersecurity and Infrastructure Security Agency, “2024 JCDC Priorities,” CISA, Feb. 12, 2024. [Online]. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities
36. NIST SP 800-207 (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207.
37. J. O'Brien and M. McDermott, "Biden signs ambitious executive order addressing AI," AP News, Oct. 30, 2023. [Online]. Available: https://apnews.com/article/biden-ai-artificial-intelligence-executive-order-cb86162000d894f238f28ac029005059
38. **Dixit, S., & Jangid, J.** (2024). Asynchronous SCIM profile for security event tokens. Journal of Computational Analysis and Applications, 33(6), 1357–1371. https://eudoxuspress.com/index.php/pub/article/view/1935

39. **Dixit, S., & Jangid, J.** (2022). Optimizing software upgrades in optical transport networks: Challenges and best practices. Nanotechnology Perceptions, 18(2), 194–206. https://nano-ntp.com/index.php/nano/article/view/5169