Politeia : Journal of Public Administration and Political Science and International Relations
E-ISSN : 3031-3929
Volume. 3 Issue 2 April 2025
Page No: 114-127

Artificial Intelligence and Cybersecurity Governance: Comparative Insights into National Defense Strategies

Widaningsih[1], Sholahuddin Shoum Abdurrahman[2], Hasan Busairi[3]
[1]Universitas Garut, Indonesia
[12]Universitas Muhammadiyah Palangkaraya, Indonesia
Correspondent: widaningsih@uniga.ac.id[1]

Received : March 07, 2025
Accepted : April 24, 2025
Published : April 30, 2025

Citation: Widaningsih, Abdurrahman, S.S., & Busairi, H., (2025). Artificial Intelligence and Cybersecurity Governance: Comparative Insights into National Defense Strategies. Politeia : Journal of Public Administration and Political Science and International Relations, 3(2), 114-127.

ABSTRACT: Artificial intelligence (AI) is reshaping national cybersecurity strategies worldwide, offering both innovative defense mechanisms and complex new threats. This study examines how AI influences cybersecurity frameworks across the United States, United Kingdom, Singapore, Sub-Saharan Africa, and the European Union. The objective is to assess AI's dual role as a tool for cyber defense and offense, and its broader implications for global digital stability. Using a comparative analytical framework, the research integrates qualitative data from national policy documents, institutional reports, and secondary literature. Key indicators include national AI strategies, public–private collaboration models, secure-by-design principles, and resilience metrics. Cross-case comparisons reveal structural gaps and highlight effective practices. Findings indicate a growing divide between advanced and developing regions. Technologically advanced economies have incorporated AI into predictive threat modeling and automated defense systems, while emerging regions face infrastructure constraints and fragmented regulations. The study also notes the escalating economic impact of AI-driven cybercrime, expected to exceed $10 trillion globally by 2025. Promising defense technologies such as immutable backups, predictive analytics, and AI-based Managed Detection and Response (MDR) are identified as critical components of modern cybersecurity systems. In conclusion, the integration of AI into cybersecurity demands balanced policies that foster innovation while ensuring ethical governance, global interoperability, and equitable capacity building. The study advocates harmonized regulatory standards, stronger public–private partnerships, and inclusive governance to enhance global cybersecurity resilience in the AI era.

Keywords: Artificial Intelligence, Cybersecurity, National Security, AI Regulation, Digital Threats, Public Private Collaboration, Global Standards.

INTRODUCTION

Artificial intelligence (AI) has significantly reshaped the modern cybersecurity landscape. On the one hand, AI strengthens defensive capabilities. On the other hand, it provides new opportunities for offensive actions. Cybercriminals increasingly exploit machine learning, natural language

processing, and autonomous decision-making algorithms to conduct highly targeted and adaptive cyberattacks. These AI-driven attacks are not only more efficient but also more successful, with studies indicating up to 67% higher success rates than traditional methods. As their methodologies evolve, they add new layers of complexity and unpredictability. Conventional defenses are often outpaced, raising serious concerns for governments, security agencies, and enterprises worldwide.

Despite these threats, AI also provides unprecedented potential to strengthen cybersecurity resilience. When combined with big data analytics, anomaly detection, and behavior modeling, AI has dramatically improved threat intelligence and real-time monitoring. AI systems can now autonomously analyze vast volumes of structured and unstructured data to uncover hidden patterns, detect vulnerabilities, and identify zero day exploits. This allows security operations centers to shorten incident response times, enhance situational awareness, and shift toward a more proactive, intelligence led defense posture. This dual nature of AI as both a threat enabler and a protective mechanism positions it as a strategic cornerstone in modern cybersecurity policy and infrastructure development

Within this rapidly transforming digital arena, hybrid warfare has emerged as a formidable threat paradigm. Hybrid warfare blurs the traditional boundaries between war and peace, combining conventional military tactics with cyber operations, psychological manipulation, misinformation, and economic coercion. The infusion of AI into hybrid operations amplifies these tactics, enabling adversaries to execute cyberattacks with high precision, speed, and plausible deniability. AI powered disinformation campaigns can target electoral systems, disrupt democratic institutions, and fragment public consensus all without crossing physical borders. These strategies have been increasingly deployed by both state and non-state actors in pursuit of political, military, and economic objectives.

Regions undergoing geopolitical friction such as Eastern Europe, the South China Sea, and parts of the Indo Pacific are especially vulnerable to these AI driven hybrid threats. In these environments, adversarial actors exploit digital vulnerabilities to conduct surveillance, disrupt energy grids, compromise defense infrastructure, or influence public sentiment. Moreover, asymmetric warfare is now more accessible; technologically less advanced actors can harness AI to exploit sophisticated targets, leveling the playing field in international confrontations. In response, nations have started reconfiguring their security doctrines to emphasize anticipatory defense, digital sovereignty, and collective intelligence sharing mechanisms.

To address these growing challenges, national defense strategies are undergoing a fundamental transformation. Defense ministries and cybersecurity agencies are integrating AI into a wide array of systems: from perimeter defenses and endpoint security to command and control infrastructures and critical infrastructure protection. These technologies support automation of complex workflows, identification of insider threats, and orchestration of adaptive countermeasures. The paradigm shift from reactive to predictive and adaptive security models reflects a broader evolution in military doctrine, one that increasingly relies on AI to ensure decision superiority, operational resilience, and mission assurance.

However, this technological advancement comes with its own set of ethical and strategic dilemmas. The dual use nature of AI where innovations intended for societal benefit are repurposed for harm

presents a profound risk. Technologies such as autonomous drones, biometric surveillance, predictive policing, and data aggregation can easily transition from defense tools to instruments of control or disruption. In this context, the lack of robust legal frameworks, ethical oversight, and international norms becomes a critical vulnerability. If left unregulated, AI could exacerbate inequality, fuel geopolitical tensions, and destabilize already fragile regions.

Consequently, many national security policies are evolving to incorporate AI not just as a technological asset but as a governance challenge. Modern policy frameworks are adopting secure by design principles, resilience planning, and ethical AI governance as foundational pillars of their digital defense architecture. These frameworks emphasize transparency, accountability, and alignment with democratic values, while simultaneously preparing for high consequence scenarios such as AI enhanced cyber sabotage, misinformation warfare, and critical infrastructure disruption.

This chapter explores these evolving dynamics by examining the dual role of AI in cyber conflict and analyzing the strategic adaptations being implemented by states to address AI driven hybrid threats. Drawing upon case studies and empirical data from countries including the United Kingdom, United States, and Singapore, this study provides a comparative lens through which to assess the global readiness and policy maturity of nations facing the next frontier of cyber enabled warfare.

METHOD

This study employs a multi-tiered comparative methodology aimed at assessing the integration of artificial intelligence (AI) into national cybersecurity strategies. The analytical model is structured to evaluate not only the technological deployment of AI but also the institutional readiness, governance structures, and strategic coherence within the national security apparatus. Case studies include Singapore, the United Kingdom, and the United States, chosen for their policy transparency, AI maturity, and contrasting geopolitical contexts. These nations represent diverse approaches to AI in cyber defense.

The research design accommodates cross case analysis, allowing for pattern recognition in policy implementation, technological adoption, and cyber governance. Special emphasis is placed on identifying best practices and systemic gaps in national strategies, offering insights into the strengths and vulnerabilities of AI deployment in different governmental systems.

The conceptual framework is rooted in the National Cyber Security Strategies (NCSS) model, which provides a standardized foundation for analyzing national policies. This is supplemented by performance indicators derived from Teoh & Mahmood (2018), Kamariotou & Kitsios (2023), and policy specific metrics detailed in each nation's official cybersecurity strategy. The study examines the following dimensions:

- AI capabilities in threat identification, prevention, and mitigation
- Cybersecurity workforce availability, expertise, and training infrastructure
- Institutional coordination across defense, civilian, and private sectors

- Legal and ethical frameworks surrounding AI governance
- Adaptability of policy frameworks in response to evolving hybrid threats
- Strategic resource allocation and innovation investment

These dimensions form the basis for scoring and categorizing national readiness and adaptability levels, ultimately contributing to a synthesized comparative matrix.

The study utilizes a mixed methods approach, combining qualitative policy analysis with empirical indicators. Primary data sources include:

- National AI and cybersecurity strategy documents
- Reports and position papers from cyber authorities
- Scholarly articles and technical whitepapers
- Incident datasets from cybersecurity firms
- International indexes such as the Global Cybersecurity Index (GCI)
- Open source intelligence (OSINT) and threat intelligence feeds

Content analysis software is used to code AI technologies, legal clauses, and institutional roles. Quantitative indicators (e.g., average detection time, cybersecurity workforce density) complement qualitative insights.

This section dissects each country's institutional architecture and its alignment with national AI goals. Evaluation metrics include:

- Autonomy and scope of National Cyber Security Authorities (NCSAs)
- Institutional integration of AI governance into national security structures
- Multi stakeholder collaboration (government, industry, academia)
- Existence of cybersecurity simulation or training programs
- Mandates for secure by design systems and national AI audit bodies

Particular attention is given to legal coherence between AI deployment and broader constitutional values, including privacy, civil rights, and data governance.

Several methodological limitations are acknowledged. Firstly, the classified nature of many cyber defense operations restricts access to critical data. Secondly, the rapid technological evolution of AI tools often outpaces the available documentation, making longitudinal comparisons difficult. Thirdly, differing degrees of transparency across jurisdictions present inconsistencies in public data availability.

To mitigate these issues, the study employs a robust triangulation process involving cross verification with multiple data streams, including media analysis, interviews with cybersecurity

practitioners, and peer reviewed literature. Recognizing these constraints, the findings are presented with nuanced caveats where data ambiguity may affect interpretation.

The integration of AI into national defense introduces complex ethical dilemmas. This study evaluates the presence and quality of AI specific regulatory frameworks in each case study. Areas of concern include:

- Algorithmic fairness and explainability in decision making processes
- Transparency of surveillance mechanisms and scope of data usage
- Mechanisms for public accountability in AI applications
- Compatibility with international laws on warfare, privacy, and digital rights

Ethical analysis is conducted using a normative framework that cross references national legislation with global benchmarks such as the OECD AI Principles and EU GDPR standards. The study also evaluates whether ethics review boards or civilian oversight mechanisms are integrated into national cybersecurity governance.

In summary, this research applies an interdisciplinary methodology combining technical analysis, institutional mapping, and ethical scrutiny. Using a comparative framework across diverse contexts, the study aims to generate actionable insights on the opportunities and risks of AI in national defense.

RESULT AND DISCUSSION

National AI Cybersecurity Initiatives and Strategic Integration

Governments around the world are accelerating their deployment of artificial intelligence (AI) in national cybersecurity strategies, in response to a rapidly evolving digital threat environment. These initiatives reflect diverse regional priorities, technological capacities, and institutional frameworks. AI adoption spans everything from real time threat detection to regulatory policy harmonization, underpinned by growing recognition of AI's dual use potential in both defense and attack.

United Kingdom:

The UK leads in integrating AI and quantum computing within its national cyber defense posture through its Cyber and Electromagnetic (CyberEM) Command. The CyberEM initiative operates as a cross functional platform combining civilian, military, and private sector capabilities to secure critical infrastructure. AI enhanced systems are used to monitor the electromagnetic spectrum, detect intrusions, and simulate adversarial attacks. These efforts are governed by the National Cyber Strategy 2022, which calls for secure by design mandates and ethical AI standards for defense systems (Radu, 2021).

United States:

The U.S. maintains a multi-pronged strategy under the National Artificial Intelligence Initiative Act of 2020. The Department of Homeland Security (DHS) and the Department of Defense (DoD) integrate AI across threat detection, predictive modeling, vulnerability analysis, and cyber simulations. The country also emphasizes a strong research ecosystem, promoting public private partnerships to develop AI powered tools such as Managed Detection and Response (MDR), adversarial emulation platforms, and autonomous threat classification engines. Federal incentives ensure scalability and long term AI innovation in the cybersecurity space (Singh, 2023).

Singapore:

As one of Asia's digital forerunners, Singapore's National AI Strategy embeds AI within state governance, defense operations, and critical public services. AI enhanced SIEM (Security Information and Event Management) and predictive threat modeling systems are widely implemented. The Cyber Security Agency of Singapore (CSA) works closely with international and domestic partners to develop secure AI standards and coordinate rapid incident response through AI augmented war rooms and cyber labs. Singapore also supports regional capacity building and digital infrastructure resilience through ASEAN collaborations.

Sub Saharan Africa and the EU:

In Sub Saharan Africa, digital governance initiatives focus on establishing AI capabilities alongside core cybersecurity infrastructure. Countries emphasize sovereign data control and responsible AI frameworks, though challenges persist due to funding and technical capacity constraints (Ayana et al., 2024). Meanwhile, the European Union has taken a regulatory leadership role. The EU's Digital Strategy promotes cross border cooperation and GDPR aligned AI practices to foster interoperability, trust, and ethical compliance across member states (Taddeo et al., 2021).

Table 1. Selected National AI Cybersecurity Initiatives

Country/Region	Initiative/Program	Key Features	Source
United Kingdom	CyberEM Command, National Cyber Strategy	Quantum AI integration; electromagnetic defense; secure by design mandates	Radu (2021)
United States	National AI Initiative Act, DHS/DoD Programs	MDR scaling, AI modeling; federal R&D incentives; red teaming simulations	Singh (2023)
Singapore	National AI Strategy	AI enhanced SIEM; cyber war rooms; predictive intelligence; ASEAN partnerships	
Sub Saharan Africa	Regional Digital and AI Governance	Sovereign data initiatives, ethical frameworks, limited infrastructure	Ayana et al. (2024)

European Union	EU Digital Strategy, GDPR, AI Act	Regulatory harmonization; cross border AI governance; privacy centric compliance	Taddeo et al. (2021)

Economic Impacts of AI Driven Cyber Threats

AI-powered cyberattacks have generated severe economic losses. Threat actors use AI for social engineering, deepfake generation, polymorphic malware, and large-scale phishing. These developments have increased both the frequency and economic scale of cybercrime.

Global Financial Outlook:

Estimates suggest that by 2025, global damages from cybercrime will exceed $10 trillion, primarily due to AI's ability to automate attacks, bypass traditional defenses, and target multiple sectors simultaneously (Thapaliya & Bokani, 2024). AI lowers the barrier for cybercrime syndicates and rogue states, enabling precision attacks with global reach.

Regional Insights:

Southeast Asia, a region experiencing rapid digital growth, has suffered $37 billion in losses due to AI driven scams, impersonation schemes, and business email compromise (BEC) in 2023 alone. Similarly, Sub Saharan Africa's exposure is increasing due to outdated systems, regulatory underdevelopment, and reliance on legacy infrastructure (Ayana et al., 2024).

Impact of Deepfakes:

Deepfake technology has emerged as a major economic disruptor. Financial institutions, electoral bodies, and media companies have reported damages from misinformation campaigns, reputational sabotage, and fraud attempts using synthetic audio/video content (Gilbert & Gilbert, 2024). These incidents undermine public trust and strain emergency response mechanisms.

Standardization Efforts:

To improve transparency and risk forecasting, agencies like ENISA and NIST have issued loss reporting frameworks for cyber incidents. These protocols include mandatory disclosures on financial loss, breach duration, remediation costs, and reputational damage (Sarjito, 2024).

Table 2. Estimated Economic Impact of AI driven Cybercrime by Region

Region	Estimated Annual Losses (USD)	Predominant Threats	Sources
Global (projected)	$10 trillion (by 2025)	Phishing automation, ransomware, supply chain hacks	Thapaliya & Bokani (2024)

Region	Estimated Annual Losses (USD)	Predominant Threats	Sources
Southeast Asia	$37 billion (2023)	Deepfake fraud, AI impersonation, financial scams	Gilbert & Gilbert (2024)
Sub Saharan Africa	Escalating losses	Infrastructure attacks, limited mitigation capacity	Ayana et al. (2024)

AI Enhanced Threats and Defensive Capabilities

As AI capabilities evolve, so too does the threat environment. Threat actors now deploy AI to mimic human behavior, automate malware deployment, and manipulate datasets, making attacks increasingly dynamic and adaptive.

Advanced Threat Landscape:

Notable AI-driven threats include spear phishing (contextual email generation that bypasses firewalls), deepfake audio (executive impersonation), and adversarial machine learning (data manipulation to evade detection) (Kumar et al., 2024). These threats challenge static defenses and require adaptive, continuous learning systems.

Defensive Advances:

National systems have begun integrating AI for real time behavioral analytics, intelligent threat correlation, and pattern recognition. MDR services powered by AI now process terabytes of data per second, improving anomaly detection and incident prioritization. Meanwhile, next gen SIEM tools provide cross layer visibility and automation for both endpoint and network security(Camacho, 2024).

Data Resilience Measures:

Immutable backup architectures have become vital in ransomware preparedness. These systems ensure data cannot be altered post write, providing reliable restoration without ransom payments. Governments and private sectors are increasingly incorporating immutable backups into disaster recovery policies (Camacho, 2024).

Predictive Intelligence:

Predictive analytics models are now used in intrusion detection systems (IDS), endpoint detection and response (EDR), and supply chain monitoring. These tools analyze historical breach data and real time signals to forecast attack probabilities, allocate defense resources, and generate preemptive alerts (Zeadally et al., 2020).

Table 3. Comparative Overview of AI Enabled Cyber Threats and Defenses

Category	Example Technologies/Methods	Functional Impact	Source(s)
Threats	AI phishing bots, deepfake media, adversarial ML	Targeted disinformation, evasion of AI based detection	Kumar et al. (2024)
Defensive Tools	MDR, AI enhanced SIEM, behavioral analytics	Rapid threat detection, insider threat prevention	Camacho (2024); Zeadally (2020)
Recovery Strategies	Immutable backups	Guaranteed data restoration post attack	Camacho (2024)
Proactive Defense	Predictive analytics in IDS/EDR systems	Anticipation of threats, strategic preemption	Zeadally et al. (2020)

Regulatory Challenges in AI Cybersecurity Policy

As artificial intelligence (AI) becomes increasingly integrated into cybersecurity, a range of regulatory challenges has emerged that complicate effective governance. Prominent among these challenges is the existing lag in legislative frameworks, which often struggle to keep pace with the rapid advancement of AI technologies (Jaiswal & Mishra, 2024). The inherently dynamic nature of AI presents difficulties in creating legislation that can effectively address current and emerging threats without becoming obsolete (Hamon et al., 2024). In particular, the need for regulations to cover AI driven cyber defense and offense mechanisms adds complexity to existing legal frameworks, highlighting gaps in liability, accountability, and data protection. This gap highlights the urgency for adaptive legal mechanisms that can evolve alongside technological progress.

Moreover, the regulatory environment is characterized by fragmentation across jurisdictions, which can create hurdles for compliance especially for multinational companies that must navigate varying national and regional legal landscapes (Pasupuleti, 2024). This fragmentation is exacerbated by differing standards regarding data privacy, AI accountability, and the ethical use of technology, thereby complicating international cooperation in cybersecurity efforts. Additional challenges, such as algorithmic bias, transparency, and the rapid evolution of AI technologies, underscore the urgency of developing cohesive regulatory strategies that embrace these complexities while fostering innovation (Zaman & Mazinani, 2023).

Furthermore, many regulatory efforts face limitations in enforcement due to outdated compliance infrastructure or insufficient expertise within governmental agencies. This results in a regulatory lag that widens the gap between emerging technological applications and their governance. For instance, issues such as explainability in AI decision making and enforcement jurisdiction in transnational data incidents remain unresolved, leading to ambiguity in both public and private sector practices. Future regulatory innovation must embrace not only technical comprehensiveness but also legal interoperability to establish adaptive, scalable, and forward looking cybersecurity laws.

Secure by Design Frameworks and Practical Effectiveness

The effectiveness of current secure by design frameworks has been a focal point of analysis amid the growing emphasis on cybersecurity. Secure by design principles advocate for integrating security considerations into the software development lifecycle, rather than treating security as an afterthought (Sarsam, 2023). This proactive strategy aims to create resilient systems capable of withstanding cyber threats from inception.

However, practical implementation of secure by design frameworks highlights several shortcomings. Despite industry acknowledgment of the concept's importance, the actual execution often falls short due to resource constraints, misaligned priorities, and insufficient security training among developers (Oluoha et al., 2022). Evidence suggests that while some organizations have moved toward adopting secure by design methodologies, many continue to grapple with the complexity of implementing comprehensive frameworks that meet evolving cybersecurity demands. Furthermore, the lack of standardized practices exacerbates the situation, leading to variations in security levels across applications and systems (Janvrin & Wang, 2019).

Emerging challenges in secure by design include integrating AI based systems with legacy infrastructure and maintaining security integrity across decentralized environments like edge computing or cloud native architectures. These contexts require new security engineering practices that go beyond traditional frameworks, demanding better tooling, automated validation, and real time threat modeling. Without this evolution, the implementation of secure by design risks stagnation in dynamic environments.

As organizations strive to improve their secure by design practices, ongoing evaluation and iterative refinement of these frameworks are vital. Insufficient enforcement from regulatory bodies may result in inconsistent application and diligence, limiting the overall effectiveness of intended defense mechanisms (Pasupuleti, 2024). Without greater harmonization, international cooperation on cybersecurity will remain limited.

Public Private Cooperation in Cyber Defense

Effective cyber defense increasingly relies on cooperation between public and private sectors, culminating in various models that leverage respective strengths and capabilities. Public private partnerships (PPPs) have emerged as a strategic approach to enhancing national cybersecurity resilience, with governments seeking to harness private sector innovation, expertise, and resources in combating cyber threats (Familoni, 2024).

One notable model involves threat information sharing initiatives, where private entities share insights on emerging threats and vulnerabilities with government agencies (Abisoye & Akerele, 2022). This reciprocal exchange is fortified by initiatives like the Cybersecurity Framework established by the National Institute of Standards and Technology (NIST) in the United States, promoting collaborative efforts across sectors (Janvrin & Wang, 2019). Furthermore, frameworks for joint cybersecurity exercises and training programs help to synchronize efforts and strengthen response capabilities in the face of evolving attacks.

However, public private cooperation models are not without challenges. Trust issues, regulatory compliance complications, and differing objectives can hinder effective collaboration and impede the sharing of critical threat intelligence (IANCU, 2024). Additionally, disparities in resource availability or capacity can limit the engagement of smaller enterprises, affecting the overall resilience of the collective cybersecurity environment.

In some countries, legal constraints prevent meaningful information sharing due to privacy regulations, liability fears, or lack of safe harbor provisions. This stifles real time collaboration during major cyber incidents. To mitigate these issues, governments must offer standardized frameworks for information sharing, prioritize data anonymization protocols, and enforce protective regulations that shield cooperative partners from punitive legal consequences. Moreover, public private cyber fusion centers could act as coordination hubs to facilitate active situational awareness.

Thus, enhancing public private partnership models necessitates establishing clear governance, fostering transparency, and promoting mutual benefits that encourage participation from all stakeholders. With AI continuing to transform both attack surfaces and defense mechanisms, an agile PPP model becomes essential to leverage real time innovations and scale national cybersecurity capabilities.

Harmonizing Global Standards for AI in Cybersecurity

The harmonization of global standards for AI in cybersecurity represents a significant challenge, exacerbated by divergent national interests, regulatory environments, and technological capabilities. Establishing a common set of standards is essential for maximizing the benefits of AI while ensuring interoperability and safeguarding against security risks (Folorunso et al., 2024). As cybersecurity threats traverse borders, disparate regulatory frameworks can introduce significant vulnerabilities and inefficiencies, complicating the implementation of cohesive countermeasures (Owolabi et al., 2024).

International bodies such as the International Organization for Standardization (ISO) and the European Union's AI Act strive to create a standardized framework that balances innovation with security. However, meaningful harmonization requires multilateral engagement and commitment from nations to collaborate, share knowledge, and adopt aligned regulatory practices that account for regional variations and unique cybersecurity challenges (Satory et al., 2024). Additionally, fostering global dialogue between industry leaders, policymakers, and cybersecurity experts will be crucial in establishing principles and benchmarks that reflect collective interests (Biasin & Kamenjašević, 2024).

Another significant hurdle in harmonization is the competitive nature of AI technological advancement, which often discourages nations from openly collaborating or disclosing vulnerabilities. However, the benefits of shared AI threat intelligence and cross border response coordination far outweigh the risks of protectionism. Multilateral treaties, interoperability benchmarks, and mutual recognition of certification schemes could serve as foundational pillars for harmonized cybersecurity policy ecosystems.

Ultimately, achieving harmonization involves addressing the balance between regulatory flexibility and the need for stringent security measures that adapt to the fast evolving nature of AI technologies. In fostering the collaborative development of global standards, the integration of ethical considerations, transparency mechanisms, and accountability measures will be crucial in ensuring the robust regulatory landscape necessary for effective cybersecurity in the age of AI (Omokanye et al., 2024).

CONCLUSION

This study highlights the dual role of artificial intelligence (AI) in national cybersecurity—both as a catalyst for advanced threats and as a cornerstone of modern defense strategies. Comparative insights from the United States, United Kingdom, Singapore, Sub-Saharan Africa, and the European Union reveal a widening divide: advanced economies leverage AI for predictive threat modeling, secure-by-design systems, and resilience planning, while developing regions face persistent infrastructural and regulatory gaps. The global economic toll of AI-driven cybercrime, projected to surpass $10 trillion by 2025, underscores the urgency for coordinated action.

To strengthen global resilience, three priorities stand out: first, harmonizing international regulatory frameworks to reduce fragmentation and ensure ethical AI deployment; second, institutionalizing secure-by-design principles supported by incentives, compliance mechanisms, and cybersecurity education; and third, fostering inclusive public–private partnerships that enable capacity building and equitable access to advanced defense tools such as predictive analytics, immutable backups, and Managed Detection and Response (MDR). Addressing these priorities will require not only technological innovation but also governance models that emphasize transparency, accountability, and cross-border cooperation, ensuring that AI contributes to digital stability rather than deepening global divides.

REFERENCE

Abisoye, A., & Akerele, J. I. (2022). A Practical Framework for Advancing Cybersecurity, Artificial Intelligence and Technological Ecosystems to Support Regional Economic Development and Innovation. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(1), 700–713. https://doi.org/10.54660/.ijmrge.2022.3.1.700-713

Ayana, G., Dese, K., Nemomssa, H. D., Habtamu, B., Mellado, B., Badu, K., Yamba, E. I., Faye, S. L., Ondua, M., Nsagha, D. S., Nkweteyim, D., & Kong, J. D. (2024). Decolonizing Global AI Governance: Assessment of the State of Decolonized AI Governance in Sub-Saharan Africa. *Royal Society Open Science*, *11*(8). https://doi.org/10.1098/rsos.231994

Biasin, E., & Kamenjašević, E. (2024). Regulatory Approaches Towards AI-Based Medical Device Cybersecurity: A Transatlantic Perspective. *European Journal of Risk Regulation*, *15*(4), 876–886. https://doi.org/10.1017/err.2024.23

Camacho, N. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Jaigs*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

Familoni, B. T. (2024). Cybersecurity Challenges in the Age of Ai: Theoretical Approaches and Practical Solutions. *Computer Science & It Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

Gilbert, C., & Gilbert, M. A. (2024). Leveraging Artificial Intelligence (AI) by a Strategic Defense Against Deepfakes and Digital Misinformation. *International Journal of Scientific Research and Modern Technol*, *3*(11), 62–78. https://doi.org/10.38124/ijsrmt.v3i11.76

Hamon, R., Junklewitz, H., Garrido, J. S., & Sánchez, I. (2024). Three Challenges to Secure AI Systems in the Context of AI Regulations. *Ieee Access*, *12*, 61022–61035. https://doi.org/10.1109/access.2024.3391021

IANCU, N. (2024). *A National Security Perspective on Strengthening E.U. Civilian-Defence Cybersecurity Synergy: A Systemic Approach*. 22–34. https://doi.org/10.19107/cybercon.2024.03

Jaiswal, A., & Mishra, P. C. (2024). Artificial Intelligence (Ai) and Cybersecurity Law: Legal Issues in Ai-Driven Cyber Defense and Offense. *Shodhkosh Journal of Visual and Performing Arts*, *5*(6). https://doi.org/10.29121/shodhkosh.v5.i6.2024.4144

Janvrin, D. J., & Wang, T. (2019). Implications of Cybersecurity on Accounting Information. *Journal of Information Systems*, *33*(3), A1–A2. https://doi.org/10.2308/isys-10715

Kamariotou, M., & Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics*, *12*(2), 382. https://doi.org/10.3390/electronics12020382

Kumar, A., Rayne, D., Salo, J., & Yiu, C. S. (2024). Battle of Influence: Analysing the Impact of Brand-Directed and Influencer-Directed Social Media Marketing on Customer Engagement and Purchase Behaviour. *Australasian Marketing Journal (Amj)*, *33*(1), 87–95. https://doi.org/10.1177/14413582241247391

Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). Artificial Intelligence Integration in Regulatory Compliance: A Strategic Model for Cybersecurity Enhancement. *Ijfmr*, *3*(1), 35–46. https://doi.org/10.54660/.ijfmr.2022.3.1.35-46

Omokanye, A. O., Ajayi, A. A., Olowu, O., Adeleye, A. O., Chianumba, E. C., & Omole, O. M. (2024). AI-powered Financial Crime Prevention With Cybersecurity, IT, and Data Science in Modern Banking. *International Journal of Science and Research Archive*, *13*(2), 570–579. https://doi.org/10.30574/ijsra.2024.13.2.2143

Owolabi, I. O., Mbabie, C. K., & Obiri, J. C. (2024). AI-Driven Cybersecurity in FinTech &Amp; Cloud: Combating Evolving Threats With Intelligent Defense Mechanisms. *Ijmrset*, *07*(12). https://doi.org/10.15680/ijmrset.2024.0712004

Pasupuleti, M. K. (2024). *Empowering the Global Economy: Digital Currencies and Financial Inclusion for Equitable Growth*. 90–105. https://doi.org/10.62311/nesx/17991

Radu, R. (2021). Steering the Governance of Artificial Intelligence: National Strategies in Perspective. *Policy and Society*, *40*(2), 178–193. https://doi.org/10.1080/14494035.2021.1929728

Sarjito, A. (2024). Countering Hybrid Threats: Challenges and the Role of Defense Science. *Publicness Journal of Public Administration Studies*, *3*(1), 101–111. https://doi.org/10.24036/publicness.v3i1.188

Sarsam, S. M. (2023). Cybersecurity Challenges in Autonomous Vehicles: Threats, Vulnerabilities, and Mitigation Strategies. *Shifra*, *2023*, 34–42. https://doi.org/10.70470/shifra/2023/005

Satory, A., Wulandari, B. T., Bawembang, N., Wardana, S. K., & Nugroho, T. (2024). The Legal Challenges of Data Privacy Laws, Cybersecurity Regulations, and AI Accountability in the Digital Era. *Join*, *1*(4), 656–668. https://doi.org/10.59613/zgvwd520

Singh, P. (2023). Artificial Intelligence: The Backbone of National Security in 21st Century. *TJJPT*, *44*(4), 2022–2038. https://doi.org/10.52783/tjjpt.v44.i4.1174

Taddeo, M., McNeish, D., Blanchard, A., & Edgar, E. (2021). Ethical Principles for Artificial Intelligence in National Defence. *Philosophy & Technology*, *34*(4), 1707–1729. https://doi.org/10.1007/s13347-021-00482-3

Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity Workforce Development for Digital Economy. *The Educational Review Usa*, *2*(1). https://doi.org/10.26855/er.2018.01.003

Thapaliya, S., & Bokani, A. (2024). Leveraging Artificial Intelligence for Enhanced Cybersecurity: Insights and Innovations. *Sadgamaya*, *1*(1), 46–52. https://doi.org/10.3126/sadgamaya.v1i1.66888

Zaman, D., & Mazinani, M. (2023). Cybersecurity in Smart Grids: Protecting Critical Infrastructure From Cyber Attacks. *Shifra*, *2023*, 86–94. https://doi.org/10.70470/shifra/2023/010

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *Ieee Access*, *8*, 23817–23837. https://doi.org/10.1109/access.2020.2968045