Integrating-Credibility-and-Innovation-Formulating-Cybersecurity-Policies-for-Effective-AI-Adoption

Akinyemi Anuoluwapo, Will Smith

October 2025

{Introduction] 1.Introduction

Over the last past 2 years, there has been one emerging technology that is dominating headlines across various industries. This is a disruptive technology that is literally changing the world. That technology is Artificial Intelligence (AI). AI has also affected the cybersecurity postures of organizations as well. In our paper we are going to talk about the barriers of implementing AI to Cybersecurity process for different organizations. We will present different ways to deal with this. Artificial Intelligence has been main stream for a few years now. Despite that current cybersecurity frameworks aren't up to par with the growth of Artificial Intelligence. There is a lot that isn't understood as well. There are barriers to implementation of Artificial Intelligence in cybersecurity polices that need to be addressed. We will do so in the paper through the following matter. We have the following contributions for the paper: • Technical Difficulty. There is a lack of transparency with some of the AI models. This the black box problem that we discuss in our summary. This would be fixed by updating some of the policies. Companies with have to document logic and decision making of AI that deals with cybersecurity task. • Encourage the development of AI/Cybersecurity worker policy: What we would do with this is provide tax credits or grants to companies that are going to take the time educate their staff on information relevant to AI. This includes but is not limited to machine learning operations, AI and threat analysis unique to AI. We would execute this by providing funding for collaborations between academic institutions, tech schools and other entities that create programs that promote AI in cybersecurity. • We would establish Safe Harbors and Regulatory Sandboxes that are concise and clear. Companies would be able to test their cybersecurity solutions. • Data Governance can be improved as well. We would create uniform data exchange procedure and deidentification methods customized for cybersecurity threat intelligence. • Implementation of a cybersecurity AI literacy program. This would be done establish a nationally acclaimed supported certification program aimed at c suite executives. The course would go into a risk assessment model explanation report interpretation. • Another option

we can do is consider Global Data Anonymization and sharing standards for threat intelligence policy. When it comes to this approach, we would create a global standard for anonymizing cybersecurity threats. We would also have AI model's train on more comprehensive set of worldwide data that doesn't compromise privacy. • The last contribution is AI Specific cybersecurity standards. A lot of the policies for cybersecurity are outdated or doesn't apply to AI at all. These standards would be updated. We would have frameworks that are always adapting. We would also have compliance audits as well. The remainder of the paper will illustrate the various issues with trying to implement AI to cybersecurity policies for organizations and the barriers to it. We will discuss the different ways to overcome each barrier. The paper will be structed in a way in which it's similar to the points that were highlighted in proceeding paragraph.

1 Background Work related

2.1 Background

Organizations are managing cybersecurity in a whole different way because of artificial intelligence (AI), which makes systems more predictive, flexible, and able to react to attacks instantly. However, there are additional risks and complications associated with this innovation. Credibility, responsibility, and transparency issues have surfaced as AI is used more and more into security operations. Innovation and trust are hard to reconcile in many organizations, particularly when AI models act like "black boxes," yielding outcomes that are hard to interpret or validate. Threats are becoming more automated, faster, and noisier than ever before, therefore organizations are racing to integrate AI into their security posture. AI can sort logs, identify unusual activity, and even recommend or initiate a response more quickly than an analyst. The dependability of AI-driven systems is crucial in cybersecurity, since choices have a direct impact on privacy, economic stability, and national security. A single error in judgment, whether caused by a biased dataset or an overfitted algorithm, might have dire repercussions. Therefore, confidence in AI is a governance and policy issue as much as a technical one. Frameworks that guarantee AI is both efficient and responsible are becoming more and more necessary, according to policymakers, IT managers, and cybersecurity experts. However, current cybersecurity policies frequently fall behind the advancements in technology. AI's special qualities, such as its self-learning behavior, reliance on massive datasets, and capacity to develop beyond its initial design, are often overlooked by regulators that still prioritize traditional risk models. Because of this disparity, it is challenging for businesses to fully reap the benefits of AI while upholding institutional and public confidence. Therefore, creating effective cybersecurity policy requires combining innovation, creativity, adaptability, and technology advancement with credibility, trust, transparency, and responsibility. This kind of integration guarantees that AI systems safeguard digital infrastructures while adhering to legal requirements, human oversight, and ethical norms. This context lays the groundwork for creating legislative frameworks

that direct businesses toward the responsible deployment of AI, where innovation enhances cybersecurity integrity rather than compromises it. 2.2. AI as a tool to improve cybersecurity AI can assist security teams in transitioning from reactive to proactive defense, according to early and general works like [1] Artificial intelligence and machine learning in cybersecurity: applications, challenges, and opportunities for MIS academics (2022) and [2] Artificial intelligence and cybersecurity: past, presence, and future (2020). Although they acknowledge that integration into actual businesses is not always simple, they demonstrate that machine-learning models may identify trends in logs, identify anomalies, and assist SOC analysts. The main AI techniques (supervised learning, anomaly detection, and reinforcement learning) are mapped to common cyber tasks (malware detection, phishing, intrusion detection, and CTI) in technical-leaning studies like [3] Harnessing artificial intelligence capabilities to improve cybersecurity (2020), [8] Machine learning techniques applied to cybersecurity, [9] AI and Cybersecurity: Opportunities, Challenges, and Governance, and [19] Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. These studies demonstrate that artificial intelligence (AI) "works," at least in controlled or experimental environments. 2.3 Adoption in real organizations and SMEs A second group of studies looks at adoption barriers, especially in real-world settings like SMEs and banking. [4] Machine learning cybersecurity adoption in small and medium enterprises in developed countries (2021) and [5] Evaluation of AI-based use cases for enhancing the cyber security defense of SMEs (2022) both say the same thing in different words: small firms like the idea of AI, but they struggle with cost, skills, data quality, and integration with old infrastructure. [17] A Roadmap for SMEs to Adopt an AI-Based Cyber Threat Intelligence even tries to give them a step-by-step path, sector specific studies as [10] What Prevents AI Adoption for Cybersecurity in the Banking Sector demonstrates that reluctance in regulated businesses is not just technological but also related to risk, accountability, and compliance. When an AI blocks or fails to block a transaction, banks are concerned about "who is responsible." That is not just a technological issue; it is also a policy issue. [11] Organization-Level Adoption of Advanced Cybersecurity Tools: Drivers, Obstacles, and Leader Reactions and [12] A Five-Phase Iterative Process Model for Effective AI Implementation in Cybersecurity Instead of asking, "Can AI do it?" ask, "How do we roll it out?" They note that adoption is facilitated by gradual deployment, clear use cases, and leadership backing. However, even these process models don't cover incident review, explainability standards, or how to record AI judgments. 2.4. The managerial perspective, cost, and incentives The economics of AI in cybersecurity (2021) offers a further perspective: even if AI enhances detection, it must be profitable. Businesses contrast AI tools with manual analysts, SIEM add-ons, and MSSPs. [6]Therefore, a cybersecurity AI strategy cannot just state, "use XAI." It must additionally specify when AI should be used, how it will be assessed, and who will cover model maintenance. 2.5. Responsible AI, explainability, and ethics One of the first publications to state that artificial intelligence in security is not neutral was Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity (2019). [7]

It has the potential to produce new attack surfaces, make biased decisions, and be abused for spying. Later pieces [14] Cybersecurity and Explainable AI: A Comprehensive Review of the Literature [15] Opportunities and Difficulties in Artificial Intelligence Security and Privacy [16] Conscientious AI for Cybersecurity. 2.6. Threat intelligence powered by AI and generative AI More recent publications like [13] Cybersecurity: A Systematic Review of Organizational Adaptation to Generative AI, [18] Cybersecurity Revolution with Generative AI: An Extensive Analysis of Threat Intelligence and Operations (2025), and in part [17] AI in cybersecurity is now more than just detection models, as demonstrated by a roadmap for SMEs to adopt an AI-based CTI. Red-teaming with LLMs, automated reporting, AI-assisted threat intelligence, content creation, and even AI-generated attacks are now the focus. According to these publications, the assault side will grow more inventive as AI advances in creativity. 2.7. Methodical assessments and plans [19]. A thorough literature mapping of artificial intelligence for cybersecurity and [20] Artificial Intelligence Adoption in Organizational Cybersecurity: The goal of the roadmap and barriers is to bring the field together. Their list of obstacles, which includes regulatory uncertainty, skills gaps, integration problems, lack of data, and trust difficulties, is excellent. Even [20], however, which is most similar to your work, appears to be more of an adoption guide than a policy guide. For instance, "all AI-based detections must generate an audit trail," "business critical services must allow for human override," "third-party AI models must disclose training data class," and so on. It not only identifies what policy clauses are difficult to write but also what they should not be.

array booktabs [table,xcdraw]xcolor caption

1.R. Sen, "Artificial intelligence and machine learning in cybersecurity: applications, challenges, and opportunities for MIS academics," Communications of the Association for Information Systems, vol. 51, no. 1, . . . , 2022. aisel.aisnet.org +1

2. Artificial intelligence and cybersecurity: Past, presence, and future," 2020.

3. Harnessing artificial intelligence capabilities to improve cybersecurity, 2020.

4. Machine learning cybersecurity adoption in small and medium enterprises in developed countries, 2021.

. . . , "Evaluation of AI-based use cases for enhancing the cyber security defense of SMEs," 2022.

. . . , "Economics of artificial intelligence in cybersecurity," 2021. (. . . journal. . .)

. . . , "Three ethical challenges of applications of artificial intelligence in cybersecurity," 2019.

. . . , "Machine learning techniques applied to cybersecurity," (year . . .).

. . . , "AI and Cybersecurity: Opportunities, Challenges, and Governance," (year . . .).

. . . , "What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector," (year . . .).

Table 1: **Table 2: Literature Gaps Related to AI–Driven Cybersecurity**

2gray!10white

No.	Paper	Main Theme of the Paper	Identified Research Gap
1	Artificial intelligence and machine learning in cybersecurity: applications, challenges, and opportunities for MIS academics (2022)	Overview of AI/ML applications in cybersecurity for MIS scholars.	Discusses benefits and challenges but does not convert them into organizational policy or governance framework.
2	Artificial intelligence and cybersecurity: Past, presence, and future (2020)	Historical and technical overview of AI in cybersecurity.	Focuses on system performance but ignores accountability and explainability dimensions.
3	Harnessing artificial intelligence capabilities to improve cybersecurity (2020)	Demonstrates how AI enhances SOC speed and detection efficiency.	Concentrates on capability; lacks model validation, trust, and post-incident review policy.
4	Machine learning cybersecurity adoption in SMEs (2021)	Explores adoption challenges in small and medium enterprises.	Identifies barriers but provides no SME-specific AI governance or policy structure.
5	Evaluation of AI-based use cases for enhancing cybersecurity defense of SMEs (2022)	Maps AI use cases to SME contexts.	Overlooks explainability, accountability, and liability standards.
6	Economics of artificial intelligence in cybersecurity (2021)	Examines cost–benefit and ROI of AI security tools.	Economic viewpoint only; lacks link to governance or cost-based policy thresholds.
7	Three ethical challenges of applications of artificial intelligence in cybersecurity (2019)	Analyzes fairness, accountability, and surveillance concerns.	Ethics discussed conceptually; lacks operationalized policy framework for enforcement.
8	Machine learning techniques applied to cybersecurity	Technical survey of ML for intrusion, malware, and anomaly detection.	Focused on technical capability, ignoring transparency, dataset bias, and model explainability.
9	AI and Cybersecurity: Opportunities, Challenges, and Governance	Links AI innovation with governance and risk.	Governance addressed broadly; lacks specific organizational compliance mechanisms.
10	What Hinders Adoption of Artificial Intelligence for Cybersecurity in the Banking Sector	Studies barriers within the financial sector.	Identifies risks but omits sector-specific AI accountability or regulatory integration.
11	Adoption of Advanced Cybersecurity Tools by Organizations: Motivations, Barriers, and Leader Responses	Examines leadership impact on adoption.	Leadership emphasized; lacks connection to explainability or documentation requirements.
12	An Iterative Five-Phase Process Model to Successfully Implement AI for Cybersecurity	Presents stepwise AI adoption model.	Comprehensive rollout plan, but missing compliance, monitoring, and audit dimensions.
13	Organizational Adaptation to Generative AI in Cybersecurity: A Systematic Review	Reviews adaptation to Generative AI tools.	No policy controls for prompt misuse, model drift, or hallucination risks.

. . . , “Adoption of Advanced Cybersecurity Tools by Organizations: Motivations, Barriers, and Leader Responses,” (year . . .).

. . . , “An Iterative Five-Phase Process Model to Successfully Implement AI for Cybersecurity,” (year . . .).

Christopher Nott, “Organizational Adaptation to Generative AI in Cybersecurity: A Systematic Review,” arXiv preprint arXiv:2506.12060, May 2025. arXiv

. . . , “Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review,” (year . . .).

A. Oseni, N. Moustafa, H. Janicke, P. Liu, Z. Tari A. Vasilakos, “Security and Privacy for Artificial Intelligence: Opportunities and Challenges,” arXiv preprint arXiv:2102.04661, Feb. 9 2021. arXiv

. . . , “Responsible AI for Cybersecurity: Assessing the Barriers, Biases and Governance Gaps,” (year . . .).

. . . , “A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence,” (year . . .). – (research gate paper) ResearchGate

. . . , “Generative AI Revolution in Cybersecurity: A Comprehensive Review of Threat Intelligence and Operations,” 2025.

. . . , “Artificial intelligence for cybersecurity: a systematic mapping of literature,” (year . . .).

. . . , “Adoption of Artificial Intelligence in Cybersecurity for Organizations: Barriers and Roadmap,” 2025, Critical Perspectives on International Business, vol. ?, no. ?, pp. . . . , 2025.