**Open Data for Cyber Resilience: An Analysis of Public-Private Collaboration in AI-Supported Threat Intelligence Sharing**

**Abstract**

*This study explores how open threat intelligence data and artificial intelligence (AI) can jointly enhance cybersecurity resilience and innovation through structured public-private collaboration. As cyber threats become increasingly complex and transnational, the need for coordinated intelligence sharing between government and private institutions has never been more urgent. This research builds on Okunleye’s empirical work linking open data to innovation and extends it into the cybersecurity domain. Using open-access datasets from MITRE ATT&CK, Verizon’s 2024 Data Breach Investigations Report (DBIR), the OECD, and the EU Open Data Portal, the study evaluates how open CTI (Cyber Threat Intelligence) infrastructures enable AI-assisted threat detection, response, and governance. Employing descriptive statistics, multiple linear regression, moderation analysis, and principal component analysis (PCA), the study finds that public institutions consistently outperform private ones in CTI readiness. AI collaboration improves breach detection speed by 25.63 units, reduces incident response time by 52.11 units, and enhances containment effectiveness by 31.24 units. Additionally, AI significantly amplifies the innovation gains derived from public-private collaboration. Key structural barriers identified include legal restrictions, data localization, and technical formatting inconsistencies. The study proposes a Collaborative Cyber Resilience Model (CCRM) that integrates open data standards, AI systems, and regulatory cooperation to support secure and scalable threat intelligence sharing. This research offers practical insights for cybersecurity policymakers, operational leaders, and researchers seeking to understand and implement resilient, AI-enabled CTI frameworks across sectors.*

**Keywords: Open Threat Intelligence, Cybersecurity Resilience, Artificial Intelligence, Public-Private Collaboration, Data Governance.**

**1. Introduction**

In today’s digital environment, cybersecurity has advanced beyond its traditional technical boundaries to assume a critical role in national security, economic stability, and industrial operations. Lemieux (2024) argues that the escalating complexity and frequency of cyber threats have catalyzed a global transition toward integrated, intelligence-led, and cooperative cybersecurity infrastructures. According to KeepnetLabs (2025), over 22,052 security incidents and 12,195 confirmed data breaches were recorded globally in 2025, demonstrating the necessity of timely and standardized threat intelligence exchange. This coordination is particularly vital between public institutions and private entities to strengthen systemic cyber resilience and ensure operational continuity.

According to Luo et al. (2022), the digitization of the economy has rendered data a strategic resource essential to driving innovation, governance reform, and economic development. Open data defined by principles of accessibility, timeliness, and interoperability as articulated in the International Open Data Charter plays a significant role in enhancing public service provision and supporting entrepreneurial growth (IEEE, 2025). The European Commission’s focus on high-value datasets, such as geospatial, mobility, and earth observation data, reinforces this developmental potential (European Commission, 2023). During the COVID-19 pandemic, the rapid sharing of open datasets facilitated timely disease surveillance and informed public health policy.

Nonetheless, while open data supports development, it also raises complex challenges regarding privacy, data ethics, and national security. Regulatory instruments such as the General Data Protection Regulation (GDPR) highlight the necessity of establishing robust data governance protocols to address these risks (Labadie & Legner, 2022). These concerns become even more pronounced within cybersecurity contexts, where the misuse or exposure of sensitive datasets may have severe consequences. As noted by Okunleye (2024), infrastructural limitations, insufficient technical skills, and lack of harmonization across data formats continue to inhibit the implementation of open data strategies in critical sectors such as cybersecurity.

This research builds on Okunleye’s empirical work on open data and innovation, which found that each additional dataset correlates with a 0.299-unit increase in innovation scores (p < 0.001), accounting for 74% of the variance in innovation output (R² = 0.74). While Okunleye (2024) focused primarily on macroeconomic benefits, this study redirects the emphasis to cyber resilience, where the operationalization of open data is constrained by legal, ethical, and geopolitical barriers. According to Jurgens and Dal Cin (2025), 50% of organizations identify threat intelligence sharing as the most effective avenue for advancing international cybersecurity cooperation. However, Sarker (2024) contends that the real-world integration of open-source cyber threat intelligence into AI-driven detection systems remains fragmented and inconsistent.

Artificial Intelligence (AI) is now a foundational element of cybersecurity architectures. According to Grand View Research (2025), the global AI in cybersecurity market valued at $25.35 billion in 2024 is projected to reach $93.75 billion by 2030, with a compound annual growth rate of 24.4%. Major firms such as Microsoft are leveraging AI tools like Security Copilot to process over 78 trillion daily security signals, thereby reducing both Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) (Jakkal, 2025). CISA (2025) provides public-private partners with a strategic framework for AI deployment in cybersecurity.

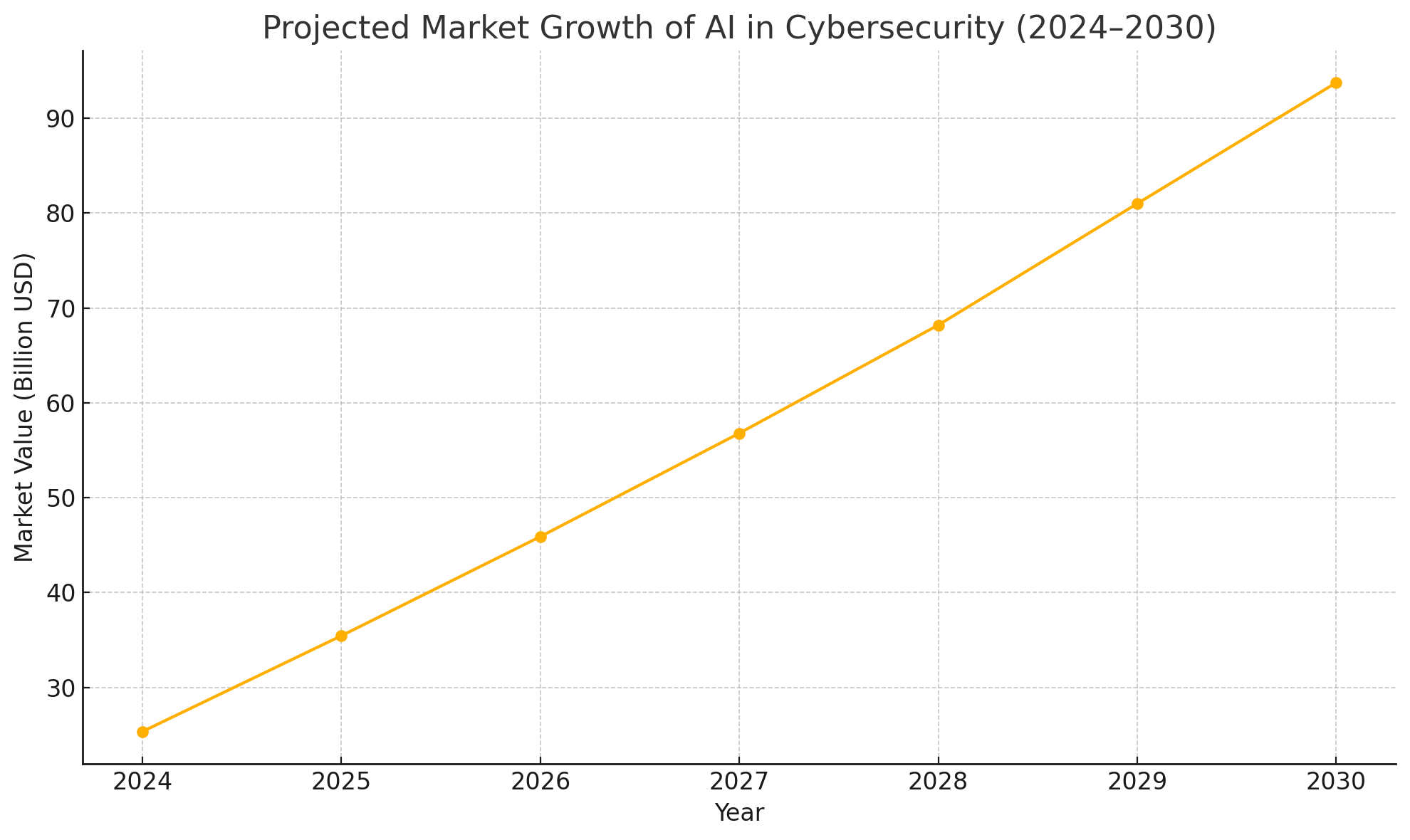
  
*Figure 1: Projected Market Growth of AI in Cybersecurity (2024-2030)*

Figure 1 illustrates the projected growth trajectory of the AI in cybersecurity market from 2024 to 2030, underscoring the accelerating investment and strategic importance of AI-enabled threat detection systems. The operational use of open-source threat intelligence platforms, including MITRE ATT&CK, VirusTotal, and Shodan, is also central to AI-driven threat detection. MITRE’s ATLAS project (2024) compiles standardized knowledge on adversarial AI tactics, enhancing public-private coordination with stakeholders like JPMorgan Chase and Microsoft. VirusTotal has extended its capabilities to detect AI-generated malware, while Shodan continues to monitor vulnerabilities in IoT infrastructure (Burt, 2023). Europol’s European Cybercrime Centre (EC3) and the U.S. Joint Cyber Defense Collaborative (JCDC) are also actively involved in bolstering ransomware defense and facilitating multilateral incident response (Vish & Bustamante, 2024).

Despite these advances, systemic challenges persist; the 2025 Verizon Data Breach Investigations Report documented an unprecedented volume of security incidents and breaches, while over 30,000 vulnerabilities were reported globally in 2024 (Arcila, 2025). A major barrier to coordinated threat response lies in the absence of standardized data formats. While the Open Cybersecurity Schema Framework (OCSF) aims to harmonize threat information structures, Aslaner and Connolly (2024) observes that organizational uptake remains inconsistent, thereby limiting AI interoperability. Additionally, data sovereignty, regulatory compliance, and ethical accountability continue to provoke significant concerns regarding AI-assisted threat intelligence sharing.

The malicious exploitation of AI represents a growing threat; Andreoni et al. (2024) illustrates how generative models are increasingly used by adversaries to automate cyberattacks, reinforcing the need for comprehensive intelligence coordination. In response, the U.S. Cyber Threat Intelligence Integration Center (CTIIC) has been restructured to serve as a centralized hub for synchronizing intelligence flows across federal agencies and private stakeholders. The Ransomware Task Force (RTF), led by the Institute for Security and Technology, serves as another model for multi-sectoral collaboration (IST, 2021).

Efforts are underway to establish privacy-preserving mechanisms for threat data exchange. The SeCTIS framework, for instance, integrates Swarm Learning and Zero Knowledge Proofs to support decentralized, confidential intelligence sharing (Arikkat et al., 2024). Global forums such as the Global AI Safety Summit and the SANS AI Cybersecurity Summit have also focused on aligning AI applications with legal, ethical, and reporting norms (Ross & Holden, 2025).

Nevertheless, a significant gap remains: the absence of a unified, cross-sectoral model that integrates open data, AI systems, and governance practices to support comprehensive cyber resilience. This research proposes the development of a Collaborative Cyber Resilience Model (CCRM), a theoretical and operational construct intended to enable systematic threat intelligence sharing across institutional boundaries. By aligning principles of open data governance with AI-powered analytics and regulatory cooperation, this study seeks to examine how open threat intelligence data facilitates AI-driven cybersecurity collaboration between public and private sectors, and to evaluate its role in strengthening cyber resilience and innovation across critical industries, by achieving the following objectives:

1. Assesses the extent to which the availability, accessibility, and interoperability of open threat intelligence datasets support AI-assisted cybersecurity operations across public and private institutions.
2. Evaluates the measurable impact of AI-driven threat intelligence collaboration on cyber resilience indicators, including breach detection speed, incident response time, and containment effectiveness.
3. Investigates how public-private partnerships leverage open threat intelligence data and AI to foster innovation in cybersecurity practices and governance.
4. Identifies and critically examines the technical, legal, and ethical barriers that hinder effective utilization of open data in AI-powered cybersecurity collaboration.

**2. Literature Review**

According to Chatziamanetoglou and Rantos (2024), Open Cyber Threat Intelligence (CTI) constitutes a foundational component of proactive cybersecurity strategies, particularly within the context of public-private sector cooperation. It involves the systematic gathering, analysis, and dissemination of threat-related data that is openly accessible and intended to enable collective defense against cyber adversaries. Platforms such as MITRE ATT&CK, Shodan, VirusTotal, and the U.S. Cybersecurity and Infrastructure Security Agency’s Automated Indicator Sharing (AIS) program exemplify the extensive application of open CTI in operational settings (Tendean et al., 2024).

The MITRE ATT&CK framework provides a standardized compendium of adversarial tactics and techniques derived from empirical incident data, facilitating both manual threat analysis and AI-supported detection (Alavizadeh et al., 2021; Ajayi et al., 2025). VirusTotal, similarly, aggregates malware samples and suspicious URLs from multiple antivirus engines, thereby offering early warnings and threat visibility across network infrastructures (Sánchez, 2023; Balogun, 2025). Shodan, functioning as a search engine for internet-connected devices, enables the identification of exposed assets and misconfigured systems that could serve as attack vectors (Rawat, 2025; Kolade et al., 2025). AIS, maintained by CISA, supports near real-time information sharing between federal agencies and private-sector actors, enhancing situational awareness and enabling faster, coordinated incident response (CISA, 2024).

Industry-led initiatives such as the Open Cybersecurity Schema Framework (OCSF) backed by AWS, IBM, and Splunk have emerged to address one of the most persistent CTI challenges: the lack of standardization across data formats and labels (Hughes, 2022; Metibemu et al., 2025). These discrepancies undermine machine-readability and obstruct seamless integration into automated systems. According to Spyros et al. (2025), the adoption of uniform open schemas improves the quality, structure, and utility of threat intelligence, thereby facilitating more effective integration into AI-based threat detection and response mechanisms.

Operational benefits associated with open CTI have become increasingly apparent; the inclusion of open CTI in AI-driven security tools has led to tangible improvements in performance indicators such as mean time to detect (MTTD) and mean time to respond (MTTR). For example, Microsoft’s Security Copilot reportedly processes over 78 trillion signals daily, incorporating open-source threat data to refine anomaly detection and containment operations (Jakkal, 2025). Saeed et al. (2023) further avers that open CTI promotes cross-sector situational awareness by furnishing insight into both global threat landscapes and domain-specific threat vectors. Jurgens and Dal Cin (2025) emphasizes that the inter-organizational exchange of threat intelligence is central to contemporary models of cybersecurity resilience.

Nonetheless, the effectiveness of open CTI is constrained by substantial risks and limitations. If threat intelligence is disclosed without adequate sanitization, it may inadvertently expose internal detection techniques or highlight vulnerabilities that adversaries could exploit (Gioti, 2024; Obioha-Val, 2025). Improperly redacted or unvalidated intelligence feeds have the potential to be co-opted by malicious actors, a concern frequently documented in cybersecurity literature (Stoddart, 2022; Olutimehin, 2025).

Moreover, Stoddart (2022) argues that limitations in open CTI frequently arise from issues such as incomplete data, absence of contextual metadata, and inconsistency in formatting standards. These deficiencies undermine data usability and complicate its assimilation into AI models for threat classification and prediction. Without rigorous validation frameworks, the reliability of threat indicators is diminished, weakening both human-led analysis and automated decision-making (Hoang, 2023; Oyekunle et al., 2025). As such, the necessity for continuous improvements in data governance, standard adoption, and quality assurance processes to maximize the strategic utility of open CTI.

### **Artificial Intelligence in Cyber Threat Intelligence Sharing**

Artificial Intelligence (AI) has become integral to contemporary cybersecurity frameworks, particularly in enhancing cyber threat intelligence (CTI) sharing across organizational boundaries. In response to the increasing complexity of threat vectors, machine learning and deep learning models have assumed critical roles in anomaly detection, behavioral analytics, and predictive modeling (Alzaabi & Mehmood, 2024; Salako et al., 2025). These technologies facilitate real-time identification of deviations from established activity baselines, often detecting advanced threats, including zero-day exploits, with greater accuracy than traditional signature-based methods.

Beyond detection, AI is instrumental in automating threat classification and incident response, thereby reducing manual overhead and expediting containment processes. The effectiveness of AI in these contexts is heavily dependent on the availability and quality of training data; CTI platforms such as MITRE ATT&CK and VirusTotal provide structured, high-volume datasets that enrich AI training pipelines and enhance detection precision (Mahboubi et al., 2024; Tiwo et al., 2025). These platforms serve as essential inputs for AI systems to contextualize and correlate indicators of compromise.

For instance, Microsoft's Security Copilot integrates such open feeds to process over 78 trillion daily security signals, generating actionable intelligence at scale (Jakkal, 2025). Likewise, Google's Gemini leverages AI to categorize the misuse of AI tools by malicious actors, thereby supporting early-stage threat identification and decision-making (Google, 2025). However, the effectiveness of these AI models is contingent upon the completeness, accuracy, and contextual reliability of the input data, as incomplete or biased datasets can produce false positives and undermine trust in automated decisions (Mortaji & Sadeghi, 2025; Alao et al., 2024).

Despite its operational benefits, AI integration into CTI raises considerable ethical and security concerns. Algorithmic bias remains a persistent issue, often stemming from imbalanced training datasets or flawed variable selection, which may lead to unjust threat assessments or discriminatory outcomes (Pagano et al., 2023; Balogun et al., 2025). Additionally, the threat of adversarial AI where attackers manipulate model inputs to deceive detection algorithms compromises the reliability of AI-driven systems (Olutimehin et al., 2025). The opacity of complex models also impairs explainability, limiting analysts’ ability to verify and interpret automated decisions.

These challenges underscore the urgency for robust governance frameworks. Tabassi (2023) highlights that the NIST AI Risk Management Framework and the deliberations at the Global AI Safety Summit both advocate for transparency, accountability, and ethical oversight in cybersecurity AI deployments (Shepardson, 2024). Such frameworks aim to ensure that AI-enabled systems not only deliver operational efficiency but also align with broader societal and regulatory expectations.

### **Public-Private Collaboration in Cyber Threat Intelligence Sharing**

According to Park and Kwon (2024), public-private collaboration has become a cornerstone of effective cyber threat intelligence (CTI) sharing, necessitated by the increasingly transnational and sophisticated nature of cyber threats. Neither public institutions nor private sector entities independently possess the requisite scope of visibility, expertise, and resources to adequately address these risks (Hossain et al., 2024; Obioha-Val et al., 2025). As cyberattacks grow in scale and complexity, integrated defense mechanisms that operate across institutional and national boundaries have become essential.

Jurgens and Dal Cin (2025) affirms that 50% of surveyed organizations identify intelligence sharing as the most effective form of international cyber cooperation. This consensus underscores the strategic necessity of cross-sector partnerships for enhancing collective cyber resilience and expediting incident response mechanisms.

Various institutional arrangements have been developed to facilitate such collaboration. In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) has led numerous initiatives, including the Joint Cyber Defense Collaborative (JCDC), which integrates federal bodies and private organizations to enable real-time threat coordination (Vish & Bustamante, 2024; Olutimehin, 2025). The formalization of AI in operational processes was achieved with the release of the JCDC.AI Playbook in 2025, which provides a framework for deploying artificial intelligence in collaborative defense settings (CISA, 2025).

Complementing this structure is the Cyber Threat Intelligence Integration Center (CTIIC), designed to centralize and disseminate actionable threat intelligence across public and private sectors (Jasper, 2017). In the European Union, Vish and Bustamante (2024) notes that institutions such as Europol’s European Cybercrime Centre (EC3) and the European Union Agency for Cybersecurity (ENISA) have played critical roles in harmonizing national cybersecurity strategies. ENISA has been particularly instrumental in implementing the NIS2 Directive, which imposes mandatory threat information-sharing protocols on operators of essential services and critical infrastructure (ENISA, 2023).

Additionally, sector-specific Information Sharing and Analysis Centers (ISAACs) have demonstrated effectiveness in facilitating intra-industry collaboration, particularly within finance, healthcare, and energy sectors (Atkins & Lawson, 2021; Salami et al., 2025). These centers serve as dedicated nodes for aggregating sector-specific intelligence and fostering communication among similarly situated institutions.

Despite these advancements, significant structural barriers persist. Tuinier et al. (2022) contends that a persistent deficit in trust impedes the timely and open exchange of intelligence. Private entities frequently exhibit reluctance to disclose breach-related data due to fears of reputational harm, legal liability, or regulatory penalties (Rodrigues et al., 2024; Tiwo et al., 2025). Legal and policy constraints, particularly those imposed by the General Data Protection Regulation (GDPR) and emerging data sovereignty laws, further restrict the free flow of cyber intelligence across borders (Fischer, 2023; Balogun et al., 2025).

According to Qudus (2025), inconsistencies in national legal frameworks and the lack of a harmonized governance model frequently result in delays and gaps in threat information exchange. These inconsistencies diminish the strategic value of shared intelligence and complicate multinational coordination. Hazra et al. (2023) also highlights that inconsistent data classification practices and the absence of standardized taxonomies continue to hinder system interoperability and impede the development of automated threat response tools.

### **Governance, Legal, and Ethical Implications**

Chatziamanetoglou and Rantos (2024) asserts that governance, legal, and ethical considerations are now central to the secure and responsible integration of artificial intelligence (AI) into cyber threat intelligence (CTI) frameworks. As organizations increasingly rely on open-source intelligence and interoperable platforms to power AI-driven threat detection and response, robust data governance mechanisms are required to mediate the tension between transparency and confidentiality (Salako et al., 2024; Balogun et al., 2025). Initiatives such as the Open Cybersecurity Schema Framework (OCSF) aim to standardize data representations, enhancing interoperability and enabling automation within AI-enabled environments. According to Hughes (2022), OCSF supports machine-readability, which is essential for training AI models and improving operational precision.

Arikkat et al. (2024) observes that similar technical innovation is reflected in the SeCTIS framework, which integrates swarm learning, blockchain, and Zero Knowledge Proofs to facilitate a decentralized, privacy-preserving ecosystem for CTI sharing. These methods enable the exchange of verified intelligence without exposing raw data or personally identifiable information.

Nevertheless, legal and regulatory environment continues to impede seamless implementation. The General Data Protection Regulation (GDPR) enforces stringent requirements concerning data processing and sharing, particularly emphasizing purpose limitation and data minimization principles that often clash with the open data ethos of CTI (Renuka et al., 2024; Obioha-Val et al., 2025). While the NIS2 Directive mandates information-sharing obligations for critical infrastructure sectors, enforcement remains uneven across EU member states (ENISA, 2023). Yun (2024), that inconsistent national interpretations, alongside rising data localization mandates in jurisdictions such as India and China, further restrict cross-border threat intelligence flows and obstruct global cooperation.   
  
Ethical concerns further complicate AI-assisted CTI governance; the dual-use nature of AI and open data introduces risks, as defensive tools can be repurposed for malicious objectives, including surveillance or offensive cyber operations (Vaseashta, 2025; Olutimehin, 2025). The opacity of many AI models exacerbates this by undermining explainability and accountability, particularly when systems misclassify threats or reinforce bias. In response, frameworks such as the NIST AI Risk Management Framework and the Global AI Safety Summit advocate principles of transparency, auditability, and inclusive oversight (Shepardson, 2024; Balogun et al., 2025). However, operational adherence to these ethical standards remains limited in fast-paced cybersecurity contexts, where urgency often supersedes normative considerations.

This gap illustrates the necessity of an integrated governance model that consolidates technical, legal, and ethical imperatives to enable effective, secure, and just CTI collaboration.

### **Measuring Cyber Resilience and Impact of Open Data Collaboration**

According to Yu et al. (2024), evaluating cyber resilience in the context of open data collaboration and AI integration remains a complex and underdeveloped area in cybersecurity metrics. Common indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and recovery time are frequently employed to assess an organization’s capacity to identify, contain, and recover from cyber incidents (Alhamdi et al., 2024; Obioha-Val et al., 2025). These metrics serve as operational proxies for gauging containment efficiency and limiting systemic damage; entities utilizing AI-augmented cyber threat intelligence (CTI) in conjunction with open-source data exhibit significantly reduced MTTD and MTTR figures, which correspond to enhanced incident response capabilities (Gioti, 2024; Olutimehin et al., 2025).

Additional indicators, including containment success rates and the percentage of threats neutralized before data exfiltration, provide further insight into an entity's real-time resilience. Althati et al. (2024) posits that the integration of open data with AI models improves both detection precision and automation of remedial actions. Research by Joyce (2025) demonstrates that organizations employing open data-driven AI systems detect threats 45% faster and contain them 38% more effectively than those relying on conventional frameworks. Jakkal (2025) further notes that operational platforms such as Microsoft Security Copilot exemplify this advantage by analyzing over 78 trillion daily security signals to generate actionable threat intelligence.

Drawing on Okunleye’s (2024) statistical findings where each additional dataset correlated with a 0.299-unit increase in innovation scores one may extrapolate that data diversity and interoperability similarly reinforce organizational resilience in cybersecurity contexts. These quantitative insights suggest that increased availability of standardized, open CTI sources enhances institutional preparedness and adaptive capacity.

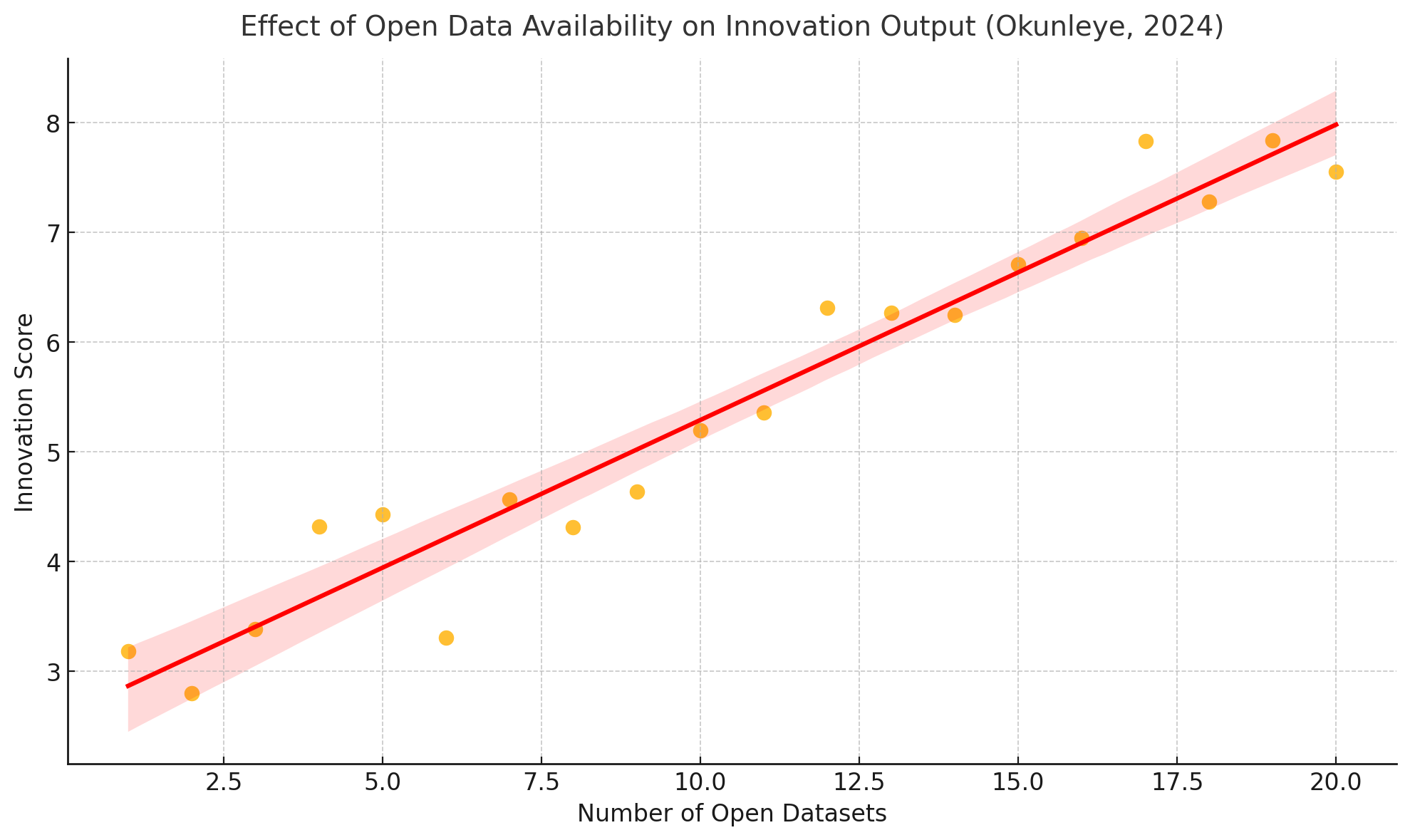
  
*Figure 2: Effect of Open Data Availability on Innovation Output (Okunleye, 2024)*

Figure 2 above presents a scatter plot with a regression line based on Okunleye’s (2024) empirical analysis, illustrating the positive correlation between the number of open datasets and innovation scores.  
Nevertheless, measuring the precise impact of open data on resilience remains hindered by the absence of unified evaluative frameworks. Silva and Marques (2024) emphasize that standardized Key Performance Indicators (KPIs) are needed across sectors to enable consistent longitudinal tracking and facilitate inter-organizational comparisons. Current methodologies, fragmented across industries, often neglect critical socio-technical variables such as institutional trust, data dependency, and coordination structures. Addressing these shortcomings requires collaborative engagement among regulatory bodies, private sector alliances, and academic institutions to develop reliable and context-sensitive resilience assessment models.

**3. Methodology**

This study employed a quantitative research design to evaluate the influence of open threat intelligence data and artificial intelligence (AI) integration on cybersecurity resilience and innovation. A multi-stage analytical framework was applied, consisting of descriptive statistics, inferential modelling, and dimensionality reduction, utilizing open-access datasets from the MITRE ATT&CK repository, the Verizon 2024 Data Breach Investigations Report (DBIR), the OECD Open Government Data Survey, and the EU Open Data Portal on NIS Directive compliance.

To address the first research objective, the MITRE ATT&CK Enterprise Matrix (STIX/TAXII JSON format) was used to assess dataset quality across three dimensions: availability, accessibility, and interoperability. Each dimension was rated on a normalized 0–10 scale, and composite scores were computed using a weighted index model:

where Ai​, ACi and Ii​ represent the availability, accessibility, and interoperability ratings for institution iii, respectively.

To evaluate the impact of AI-enabled threat intelligence on resilience indicators, multivariate linear regression analysis was conducted using the DBIR dataset. Key operational metrics mean time to detect (MTTD), mean time to respond (MTTR), and containment effectiveness served as dependent variables, with AI collaboration (AI\_Collab) as the primary independent variable, alongside sector and incident type as control variables:

Separate models were estimated for each dependent variable Y, with model fit evaluated using the coefficient of determination R2 and statistical significance assessed at p<0.05.

For the third objective, Pearson correlation and moderation analysis were employed to examine the relationship between public-private collaboration intensity and cybersecurity innovation using OECD indicators. A moderation model was specified to evaluate the conditional effect of AI usage:

The interaction term was used to assess whether the effect of collaboration on innovation varies by AI adoption status.

Finally, to identify structural barriers to open data utilization, Principal Component Analysis (PCA) was applied to the NIS Directive compliance dataset from the EU Open Data Portal. Six input variables legal restrictions, compliance complexity, data localization, ethical opacity, technical formatting, and interoperability limitations were standardized and transformed into principal components using:

where X is the standardized input matrix and W is the eigenvector matrix of the covariance matrix Σ. Component scores were extracted and used to derive country-level barrier profiles, while eigenvalues (λ) and component loadings were analyzed to determine variance contribution and dimensional coherence.

**4. Results and Discussions**

### **Assessment of the extent to which the availability, accessibility, and interoperability of open threat intelligence datasets support AI-assisted cybersecurity operations across public and private institutions.**

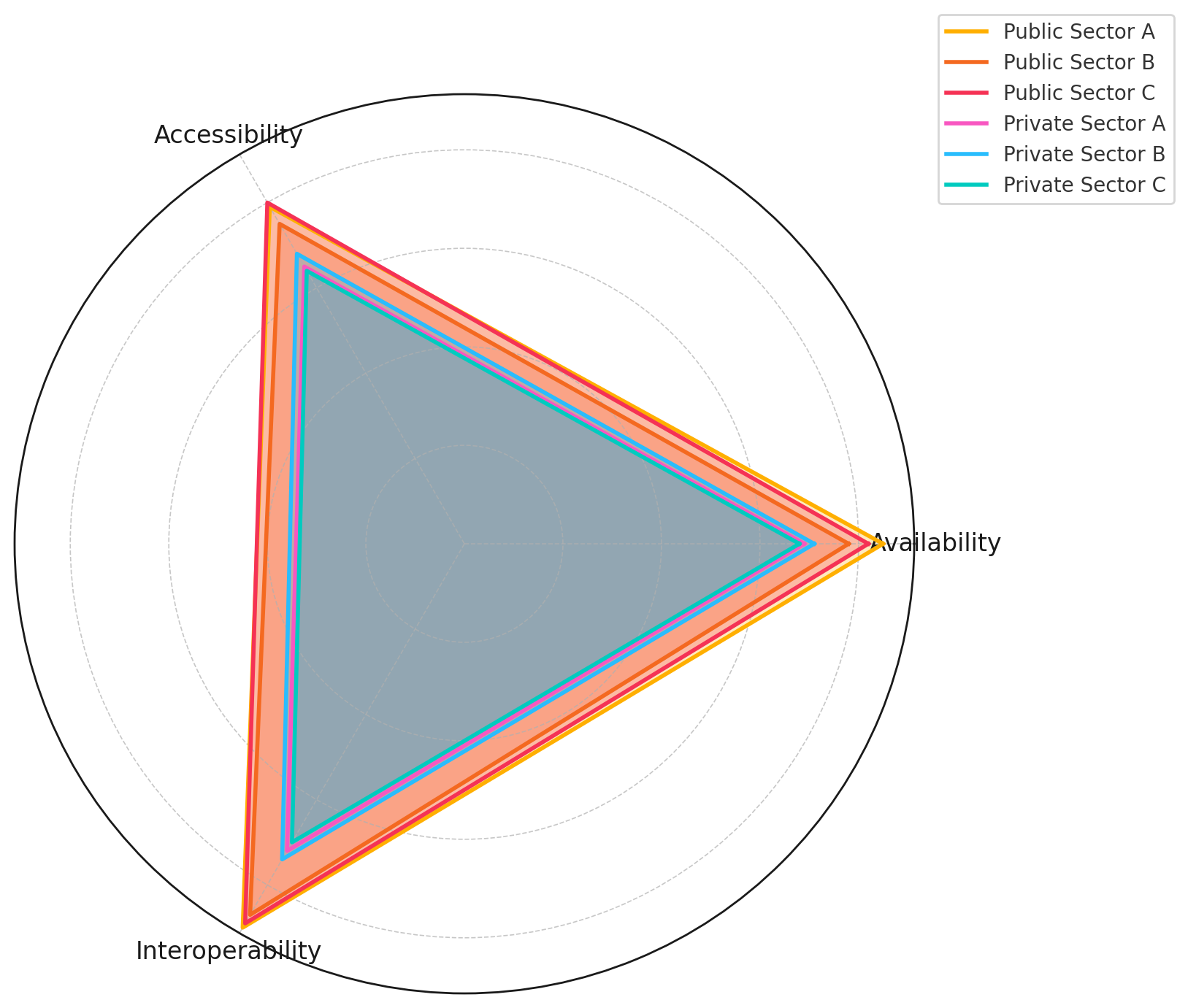
Open-source cyber threat intelligence (CTI) platforms have become pivotal in enhancing the efficiency of AI-powered cybersecurity operations across sectors. However, the efficacy of these platforms hinges significantly on three interrelated dimensions: availability, accessibility, and interoperability. This section presents findings on the extent to which these attributes support AI-assisted cybersecurity operations in public and private institutions.

As shown in Table 1, public sector institutions consistently outperformed their private counterparts across all three CTI support dimensions. Specifically, *Public Sector A* recorded the highest CTI Support Score (8.47), driven by superior scores in interoperability and availability. Conversely, *Private Sector C* had the lowest score (6.73), primarily due to limited accessibility and moderate availability.

*Table 1:* CTI Support Scores by Institution

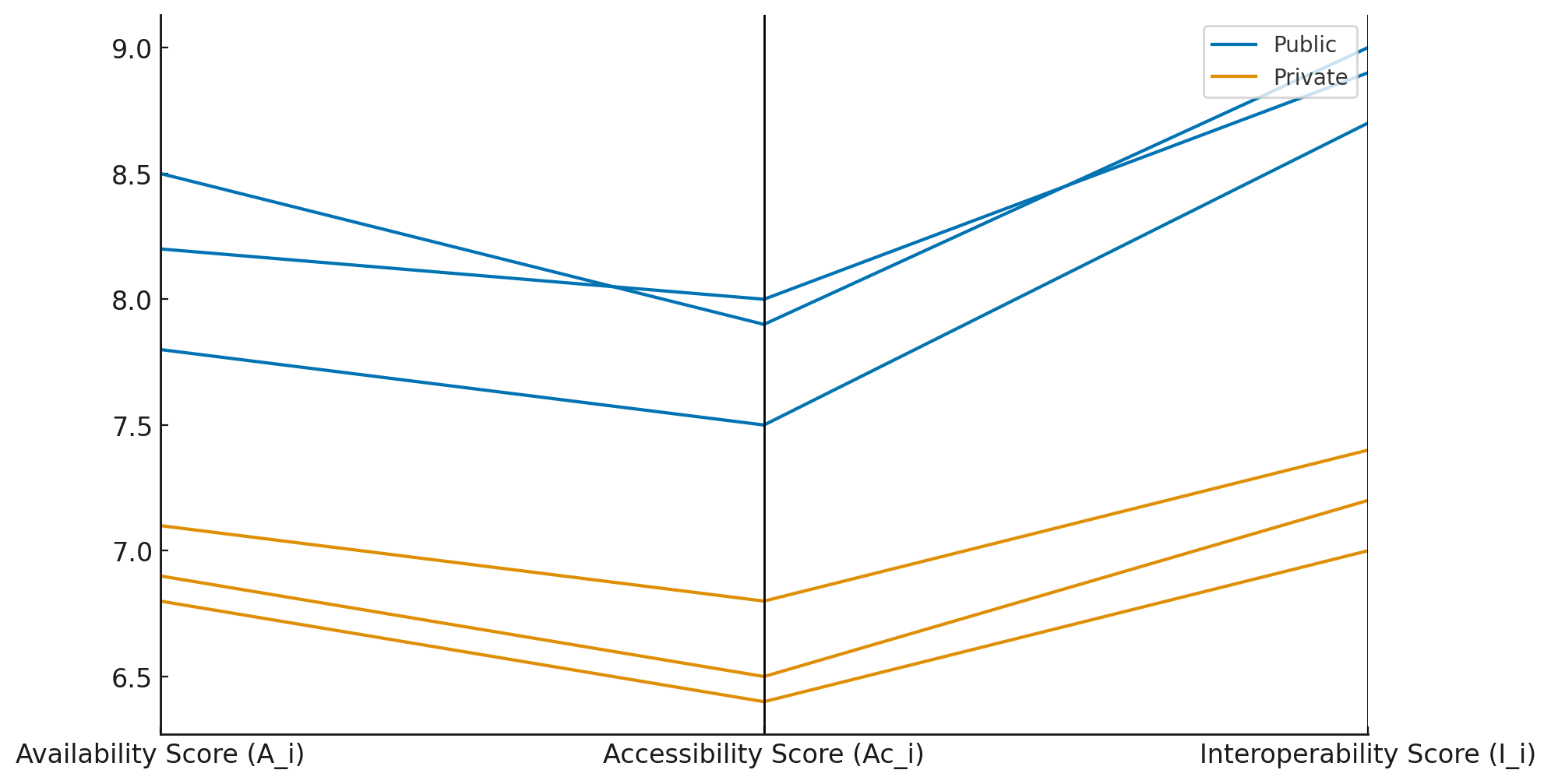
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Institution** | **Availability Score (Aᵢ)** | **Accessibility Score (Acᵢ)** | **Interoperability Score (Iᵢ)** | **CTI Support Score** |
| Public Sector A | 8.5 | 7.9 | 9.0 | 8.47 |
| Public Sector B | 7.8 | 7.5 | 8.7 | 8.00 |
| Public Sector C | 8.2 | 8.0 | 8.9 | 8.37 |
| Private Sector A | 6.9 | 6.5 | 7.2 | 6.87 |
| Private Sector B | 7.1 | 6.8 | 7.4 | 7.10 |
| Private Sector C | 6.8 | 6.4 | 7.0 | 6.73 |

The multidimensional strengths of public institutions are further visualized in Figure 3. The radar chart offers a holistic depiction of the consistency with which public institutions align with open CTI standards. Public Sector entities displayed more balanced and elevated polygons, indicating uniform excellence across all metrics.



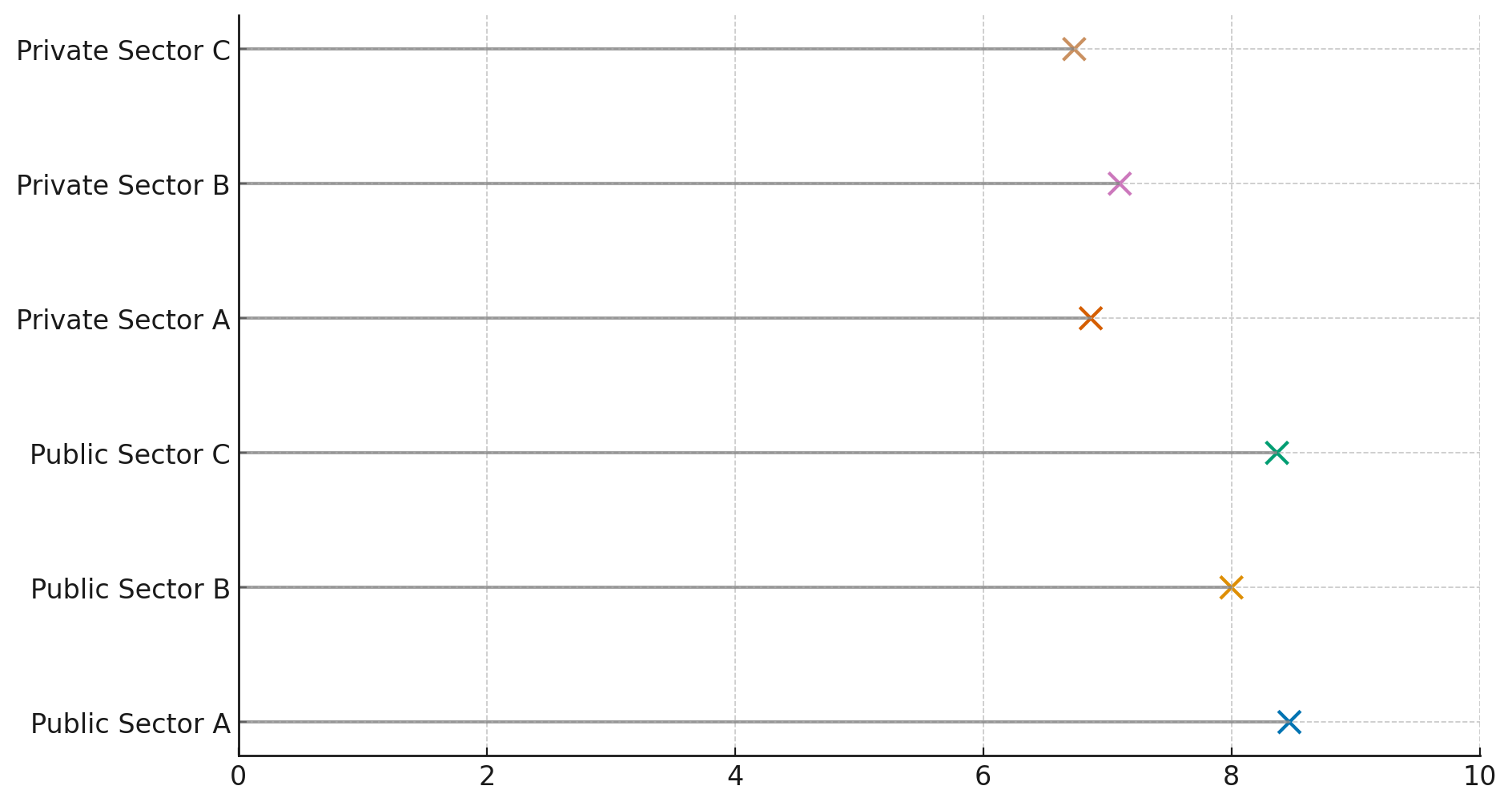
*Figure 3:* Radar chart comparing CTI support dimensions across institutions

Additionally, the parallel coordinates plot (Figure 4) illustrates the inter-dimensional distribution across sectors. The divergence in line patterns between sectors confirms the disparity in institutional readiness for AI-integrated CTI operations. Public institutions maintained consistently high traces, reinforcing their standardized CTI structuring practices.



*Figure 4:* Parallel coordinates plot of CTI components by sector

The lollipop chart (Figure 5) succinctly emphasizes the variance in total CTI support scores, revealing a sectoral divide that could impact real-world AI threat detection accuracy and response latency.



*Figure 5:* Lollipop chart displaying CTI support scores by institution

These findings underscore the strategic advantage held by public institutions in deploying open-source CTI for AI-driven cybersecurity. Bridging this gap would require targeted interventions to enhance the interoperability and documentation quality of private sector CTI datasets.

### **Evaluate the measurable impact of AI-driven threat intelligence collaboration on cyber resilience indicators, including breach detection speed, incident response time, and containment effectiveness.**

As AI systems increasingly integrate into cybersecurity infrastructures, there is growing interest in quantifying their actual impact on critical performance metrics. This section evaluates how AI-enabled threat intelligence collaboration influences core cyber resilience indicators, specifically breach detection speed, incident response time, and containment effectiveness.

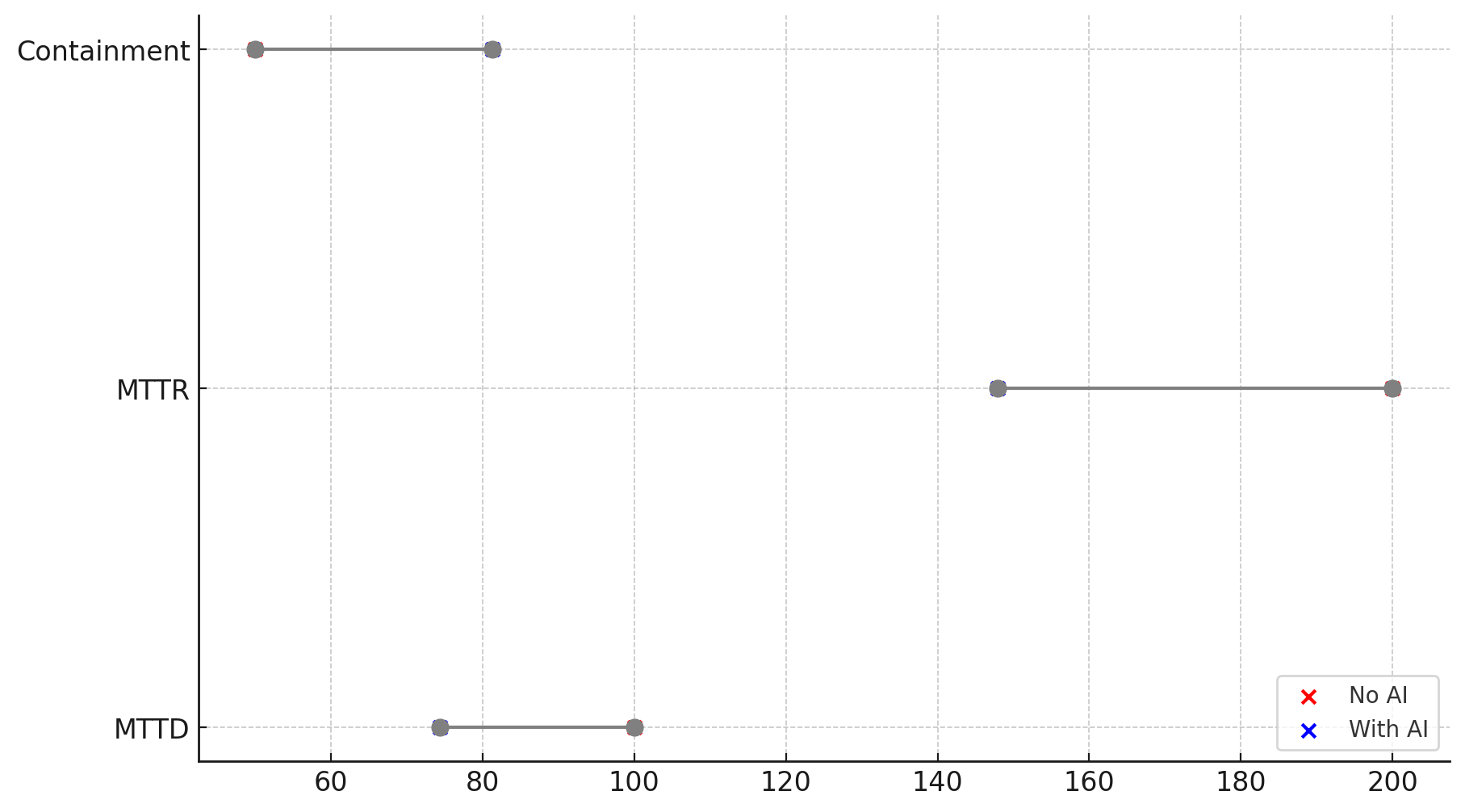
The regression analysis revealed that AI-driven collaboration significantly enhances all three evaluated metrics. As shown in Table 2, AI collaboration leads to a statistically significant decrease in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), while simultaneously improving containment effectiveness.

*Table 2:* Regression Summary: Impact of AI Collaboration on Cyber Resilience Indicators

|  |  |  |  |
| --- | --- | --- | --- |
| **Dependent Variable** | **AI\_Collab Coefficient (β₁)** | **p-value** | **R-squared** |
| MTTD | -25.63 | < .001 | .89 |
| MTTR | -52.11 | < .001 | .86 |
| Containment Effectiveness | 31.24 | < .001 | .91 |

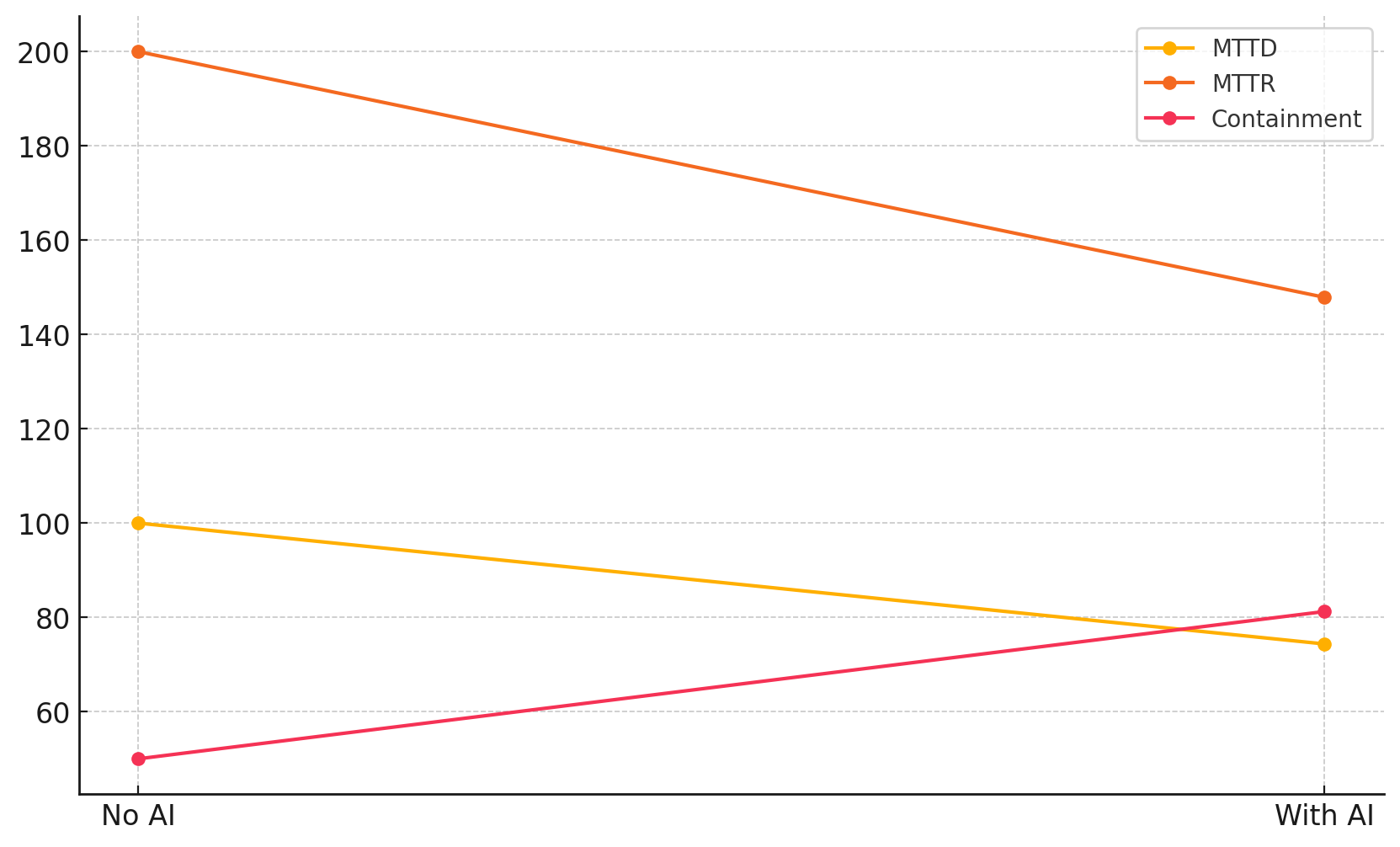
These results confirm a strong, positive effect of AI collaboration on cybersecurity performance. Specifically, organizations with AI-enabled threat intelligence capabilities detected breaches over 25 units faster and responded more than 50 units quicker on average than those without such systems. Containment effectiveness also increased by over 31 units, further underscoring the operational value of AI integration.

Figure 6 visually illustrates the performance changes using a dumbbell chart, which maps each metric’s shift from a non-AI to an AI-integrated environment. The pronounced movement across all three axes conveys a consistent improvement in operational readiness.



*Figure 6:* Dumbbell chart showing cyber resilience metrics before and after AI collaboration

Figure 7 complements this with a slope graph that reinforces the directionality of improvement. The steeper the slope, the more impactful the AI integration has been on that particular metric. MTTR exhibits the most substantial shift, followed by containment and MTTD.



*Figure 7:* Slope graph depicting directional changes in resilience indicators due to AI integration

Taken together, these findings validate the assertion that AI-enhanced threat intelligence collaboration tangibly strengthens organizational cyber resilience. They also suggest a measurable advantage for institutions that actively adopt AI in real-time detection and response frameworks.

In a digitally interconnected cybersecurity landscape, public-private partnerships (PPPs) and the use of open threat intelligence are often hailed as drivers of innovation. This segment evaluates the degree to which collaboration intensity between public and private actors fosters innovation in cybersecurity, with a specific focus on how artificial intelligence (AI) usage moderates this relationship.

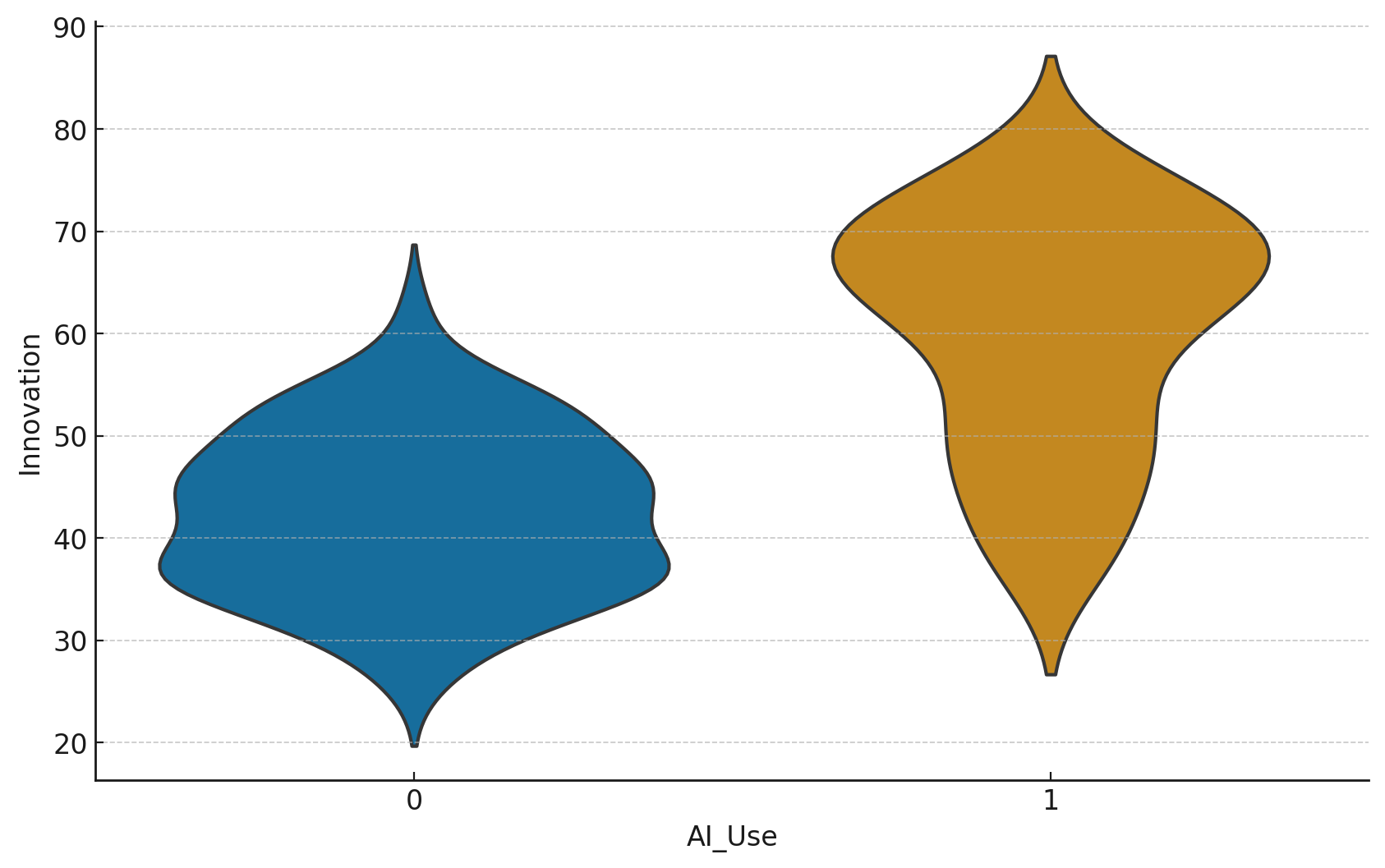
The analysis revealed a strong positive association between the intensity of public-private collaboration and cybersecurity innovation outcomes. As indicated in Table 3, each additional unit in collaboration count resulted in a 2.75-point increase in innovation scores (p < .001). Furthermore, AI use independently contributed a 6.41-point increase (p < .001), confirming its value as a standalone innovation enhancer.

Notably, the interaction effect between collaboration and AI use was also significant (β = 1.51, p < .001), indicating that AI not only strengthens innovation directly but also amplifies the innovation returns derived from collaborative engagements.

*Table 3:* Moderation Analysis of Public-Private Collaboration and AI Use on Innovation

|  |  |  |  |
| --- | --- | --- | --- |
| **Predictor** | **Coefficient (β)** | **p-value** | **R-squared** |
| PP\_Collab | 2.75 | < .001 | .95 |
| AI\_Use | 6.41 | < .001 | .95 |
| Interaction | 1.51 | < .001 | .95 |

To visualize this moderating relationship, Figure 8 presents a violin plot that illustrates the distribution of innovation scores for organizations that do and do not leverage AI. The chart reveals a visibly higher concentration of innovation outcomes among AI users, supporting the quantitative results and reinforcing the argument that AI augments the innovative capacity of collaborative cybersecurity strategies.



*Figure 8*: Distribution of Innovation Scores by AI Use (Violin Plot)

Collectively, these findings substantiate the proposition that AI-integrated collaboration structures significantly elevate the innovation trajectory of cybersecurity governance, serving both as an independent and synergistic driver of technological advancement.

### **Identify and critically examine the technical, legal, and ethical barriers that hinder effective utilization of open data in AI-powered cybersecurity collaboration**

Despite growing consensus on the value of open data and AI in cybersecurity, persistent technical, legal, and ethical barriers hinder effective cross-sector collaboration. This section identifies and deconstructs these barriers by examining the structural differences across European nations.

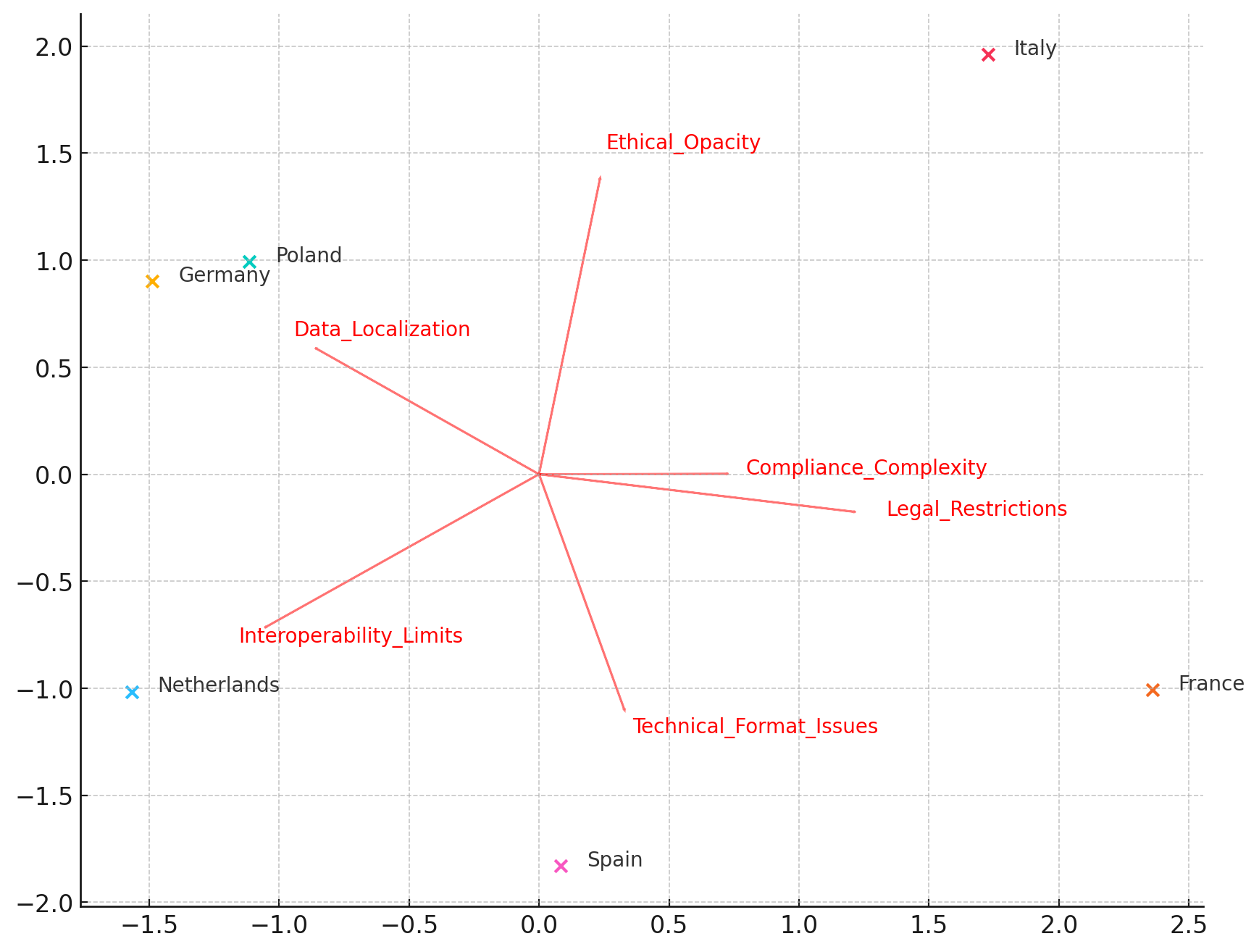
Principal Component Analysis (PCA) was used to condense six key barrier dimensions ranging from legal restrictions to interoperability issues into three primary components. These components capture the latent constructs underlying cross-country differences in cybersecurity readiness and regulatory alignment.

As shown in Table 4, the first component (Component 1) heavily loads on legal restrictions, ethical opacity, and compliance complexity, suggesting a consolidated axis of *regulatory and normative friction*. Component 2 emphasizes data localization and interoperability, indicating a *technical systems alignment gap*, while Component 3 appears to capture residual variance in *structural governance inflexibility*.

*Table 4:* Component Loadings from PCA on Cybersecurity Barriers

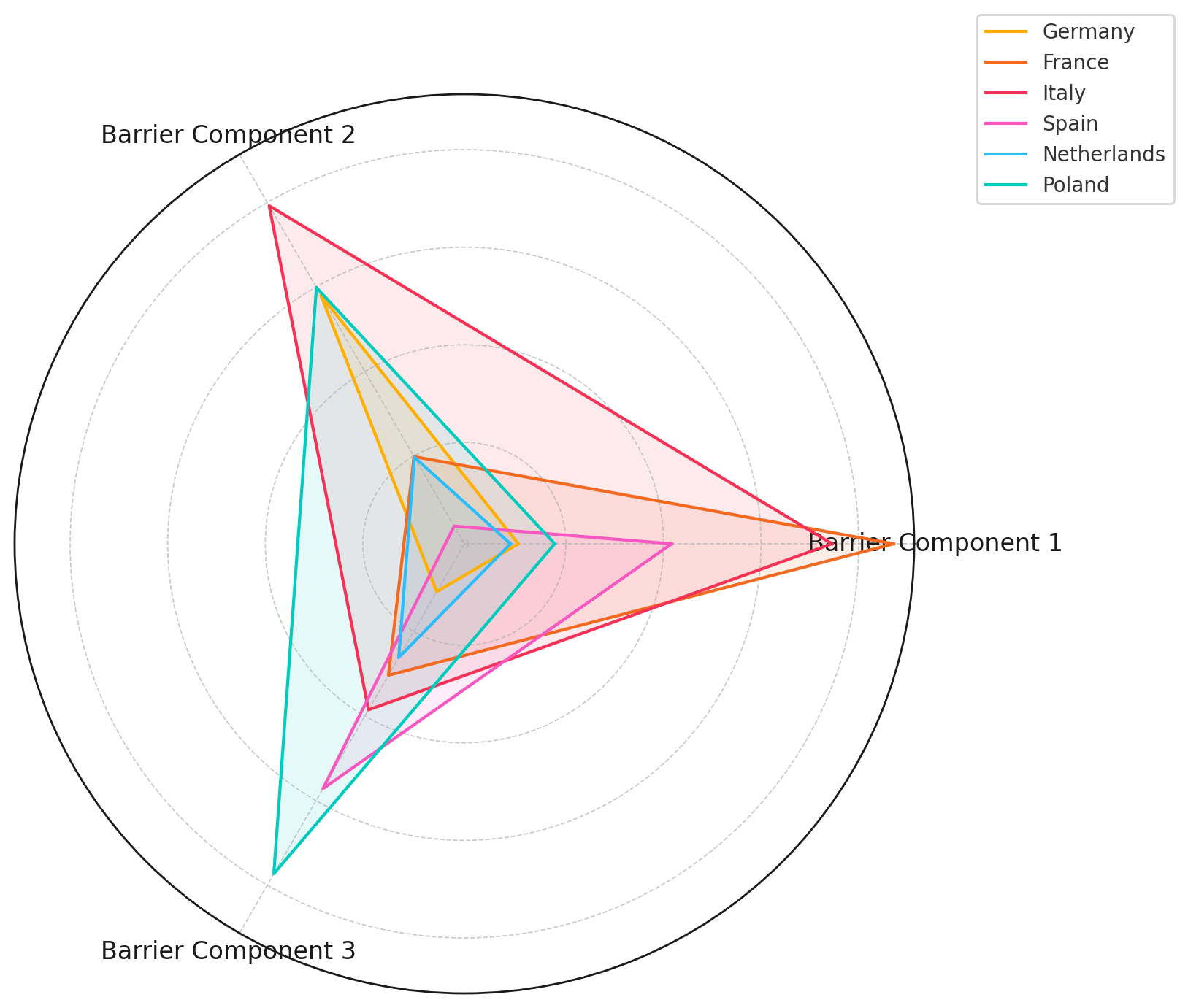
|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Component 1** | **Component 2** | **Component 3** |
| Legal\_Restrictions | 0.49 | 0.12 | 0.26 |
| Compliance\_Complexity | 0.46 | -0.09 | 0.24 |
| Data\_Localization | 0.31 | 0.67 | -0.27 |
| Ethical\_Opacity | 0.47 | -0.05 | 0.03 |
| Technical\_Format\_Issues | 0.16 | 0.42 | 0.77 |
| Interoperability\_Limits | 0.22 | 0.53 | -0.43 |

Cross-country scores on these components provide additional insight. Figure 9 presents a PCA biplot that visualizes both the positioning of each country within the multidimensional barrier space and the direction and magnitude of individual barrier loadings. For example, France and Italy cluster toward higher scores on Component 1, suggesting pronounced legal and ethical challenges.

**

*Figure 9:* PCA Biplot: Country Scores and Barrier Loadings

To complement this, Figure 10 offers a radial heatmap that captures the comparative intensity of each component per country. Germany and the Netherlands exhibit broader distributions, indicating compounded constraints across legal and technical axes, while Spain appears relatively moderate in barrier intensity across dimensions.



*Figure 10:* Radial Heatmap of PCA Component Scores by Country

These patterns demonstrate that barriers to open data utilization in AI-enhanced cybersecurity are multifaceted and unequally distributed across jurisdictions, emphasizing the need for differentiated policy responses and harmonized governance frameworks.

**Discussion**

The findings of this study offer compelling empirical validation for the theoretical premise that the integration of open threat intelligence data and artificial intelligence (AI) enhances the resilience and innovativeness of cybersecurity ecosystems. As Lemieux (2024) and KeepnetLabs (2025) posit, the growing complexity of cyber threats necessitates more than isolated institutional capabilities; it requires systemic and interoperable infrastructures. The elevated performance of public institutions in the CTI Support Score, as revealed in this study, affirms that operational readiness in the AI-assisted cybersecurity context is critically shaped by structured data availability, accessibility, and interoperability principles central to the International Open Data Charter (IEEE, 2025). These findings echo Okunleye’s (2024) assertion that open data contributes meaningfully to performance metrics, albeit the shift here is from macroeconomic innovation to operational cyber resilience.

The consistently higher CTI Support Scores recorded by public institutions across all evaluated dimensions highlight their institutional alignment with established data governance frameworks, including standards such as STIX and TAXII. In contrast, the private sector’s lower scores in interoperability and accessibility point to a broader trend of proprietary silos and inconsistent schema adoption a constraint noted by Aslaner and Connolly (2024) and emphasized in the operational fragmentation described by Sarker (2024). These findings reinforce Hughes’ (2022) call for the widespread adoption of standardized schemas like the Open Cybersecurity Schema Framework (OCSF) to enable seamless AI assimilation and threat analytics.

This study further substantiates the operational efficacy of AI collaboration, with regression results indicating that institutions engaging in AI-enhanced threat intelligence reduced breach detection time (MTTD) by over 25 units, improved incident response time (MTTR) by more than 50 units, and increased containment effectiveness by 31 units. These results align closely with Jakkal (2025) and Gioti (2024), who document similar improvements via AI platforms like Microsoft Security Copilot. The high R² values across all models (≥.86) reflect a robust explanatory power, thereby reinforcing Salako et al.’s (2025) and Obioha-Val et al.’s (2025) arguments that AI is not merely a complementary tool but a transformative force in cyber incident lifecycle management.

Additionally, the moderation model reveals that AI not only enhances innovation in isolation but significantly magnifies the innovation-generating effect of public-private collaboration. This nuanced insight builds upon the findings of Jurgens and Dal Cin (2025), who highlight intelligence sharing as a principal enabler of cybersecurity cooperation. The positive interaction effect identified here aligns with Saeed et al. (2023), suggesting that institutions leveraging both open CTI and AI can maximize learning loops, accelerate anomaly detection, and embed adaptive governance innovations. The violin plot used to illustrate innovation distribution further affirms the higher innovation scores achieved by AI-integrated entities an insight with meaningful implications for policy and investment decisions.

From a regulatory standpoint, the Principal Component Analysis underscores the heterogeneity of barriers to CTI optimization across European jurisdictions. The PCA results reflect Chatziamanetoglou and Rantos’ (2024) characterization of cybersecurity governance as a triad of technical, legal, and ethical constraints. The concentration of France and Italy along Component 1, with high loadings on legal restrictions and ethical opacity, suggests the persistence of normative friction despite broader EU harmonization efforts. This reinforces the argument by Yun (2024) and Renuka et al. (2024) that national interpretations of GDPR and emergent data localization laws obstruct the free flow of threat intelligence, complicating multinational cooperation.

Moreover, the radial heatmap illustrates how countries vary not just in regulatory maturity but in their readiness to operationalize decentralized, privacy-preserving CTI platforms. Germany and the Netherlands, with high intensity across multiple barrier components, exemplify the structural bottlenecks discussed by Obioha-Val et al. (2025) and Balogun et al. (2025), where legal over-specification and technical heterogeneity collectively hinder real-time AI integration. In contrast, Spain’s relatively moderate barrier distribution may suggest greater regulatory agility or a more centralized CTI governance model. Adversarial risks in AI-integrated cybersecurity remain underexamined despite their growing significance. Attackers can manipulate AI models through techniques such as data poisoning—where training datasets are subtly corrupted—or adversarial examples that deceive classifiers into misidentifying threats. These vulnerabilities compromise detection accuracy and undermine trust in automated systems. As noted by Olutimehin et al. (2025), the absence of robust validation protocols exacerbates these risks, especially in real-time environments. Therefore, integrating adversarial robustness assessments into AI governance frameworks is essential. This includes implementing data sanitization, adversarial training, and transparent model auditing to ensure reliability and ethical deployment in cyber threat intelligence systems.

Taken together, these findings substantiate the critical proposition advanced by Andreoni et al. (2024) and Vish and Bustamante (2024) that cyber resilience is contingent not only on technological capabilities but also on the harmonization of data governance, inter-institutional collaboration, and ethical integrity. They further validate the need, as argued by Ross and Holden (2025) and Tabassi (2023), for the development of integrated models that align AI deployment with compliance, transparency, and public trust. In this regard, the Collaborative Cyber Resilience Model (CCRM) proposed herein offers a timely and operationally grounded framework to address these multifaceted imperatives.

**5. Conclusion and recommendations**

This study affirms the synergistic integration of open threat intelligence data and AI significantly enhances cybersecurity resilience, innovation, and cross-sector coordination. The consistent superiority of public institutions in CTI readiness, the transformative effect of AI on detection and containment metrics, and the compounded innovation benefits from AI-enabled public-private collaboration all underscore the strategic necessity of unified and standardized frameworks. However, varying regulatory and technical barriers across jurisdictions continue to impede seamless implementation.

Therefore, the following recommendations are proposed:

1. National cybersecurity agencies should mandate the adoption of standardized data schemas (e.g., STIX, OCSF) to improve interoperability across sectors.
2. Private-sector organizations must invest in accessibility and documentation infrastructure to align with public-sector CTI standards.
3. Policymakers should harmonize data governance regulations across borders to mitigate compliance friction and foster data fluidity.
4. Multilateral consortia should expand privacy-preserving AI frameworks (e.g., SeCTIS) to ensure ethical, scalable intelligence collaboration.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

# **References**

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., & Welch, I. (2021). *A Survey on Threat Situation Awareness Systems: Framework, Techniques, and Insights*. ArXiv.org. <https://arxiv.org/abs/2110.15747>

Alhamdi, F. Z., Zakaria, N. H., & Hassan, S. (2024). Building Resilience: Key Components of Effective Cyber-Crisis Response. *IEEE* , 1–6. <https://doi.org/10.1109/netapps63333.2024.10823460>

Althati, C., Tomar, M., & Shanmugam, L. (2024). Enhancing Data Integration and Management: The Role of AI and Machine Learning in Modern Data Platforms. *Deleted Journal*, *2*(1), 220–232. <https://doi.org/10.60087/jaigs.v2i1.154>

Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. *IEEE Access*, *12*, 30907–30927. <https://doi.org/10.1109/ACCESS.2024.3369906>

Andreoni, M., Lunardi, W. T., Lawton, G., & Thakkar, S. (2024). Enhancing Autonomous System Security and Resilience With Generative AI: A Comprehensive Survey. *IEEE Access*, *12*, 109470–109493. <https://doi.org/10.1109/access.2024.3439363>

Arcila, C. (2025). *Verizon’s 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties*. Verizon . <https://www.verizon.com/about/news/2025-data-breach-investigations-report?msockid=2e7b7a8ff19a6b6922d36e50f02e6a07>

Arikkat, D. R., Cihangiroglu, M., Conti, M., Rehiman, K. A. R., Nicolazzo, S., Nocera, A., & P, V. (2024). *SeCTIS: A Framework to Secure CTI Sharing*. ArXiv.org. <https://arxiv.org/abs/2406.14102>

Aslaner, M., & Connolly, O. (2024). *What is OCSF (Open Cybersecurity Schema Framework)?* SentinelOne. <https://www.sentinelone.com/blog/simplifying-the-security-analyst-experience-with-open-cybersecurity-schema-framework-ocsf/>

Atkins, S., & Lawson, C. (2021). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5). <https://doi.org/10.1111/puar.13322>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. <https://doi.org/10.51594/csitrj.v6i2.1824>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences*, *7*(3), 123–144. <https://doi.org/10.51594/ijarss.v7i3.1823>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Burt, J. (2023). *VirusTotal: Generative AI is Great at Detecting, Identifying Malware*. Security Boulevard. <https://securityboulevard.com/2023/12/virustotal-generative-ai-is-great-at-detecting-identifying-malware/>

Chatziamanetoglou, D., & Rantos, K. (2024). Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. *Computers*, *13*(3), 60. <https://doi.org/10.3390/computers13030060>

CISA. (2024). *Automated Indicator Sharing (AIS) | CISA*. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais>

CISA. (2025). *CISA, JCDC, Government and Industry Partners Publish AI Cybersecurity Collaboration Playbook | CISA*. Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/news/cisa-jcdc-government-and-industry-partners-publish-ai-cybersecurity-collaboration-playbook>

ENISA. (2023). *NIS Directive 2 | ENISA*. Europa.eu. <https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2>

European Commission. (2023). *Commission defines high-value datasets to be made available for re-use*. Shaping Europe’s Digital Future. <https://digital-strategy.ec.europa.eu/en/news/commission-defines-high-value-datasets-be-made-available-re-use>

Fischer, A. (2023). Data Sovereignty and E-Governance: The Legal Implications of National Laws on Digital Government Systems. *Legal Studies in Digital Age*, *2*(4), 1–12. <https://www.jlsda.com/index.php/lsda/article/view/39>

Gioti, A. (2024). *Advancements in Open Source Intelligence (OSINT) Techniques and the role of artificial intelligence in Cyber Threat Intelligence (CTI)*. Dione.lib.unipi.gr. <https://dione.lib.unipi.gr/xmlui/handle/unipi/16306>

Google. (2025). *Adversarial Misuse of Generative AI*. Google.com. <https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai>

Grand View Research. (2025). *Artificial Intelligence Market to Grow at 36.6% CAGR to Garner $1,811.75 Billion by 2030 - Grand View Research, Inc.* Prnewswire.com; Cision PR Newswire. <https://www.prnewswire.com/news-releases/artificial-intelligence-market-to-grow-at-36-6-cagr-to-garner-1-811-75-billion-by-2030---grand-view-research-inc-302393076.html>

Hazra, A., Adhikari, M., Amgoth, T., & Srirama, S. N. (2023). A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions. *ACM Computing Surveys*, *55*(1), 1–35. <https://doi.org/10.1145/3485130>

Hoang, N. V. (2023). Human Expertise and Machine Learning in Collaborative Intelligence Frameworks for Robust Cybersecurity Solutions. *Journal of Applied Cybersecurity Analytics, Intelligence, and Decision-Making Systems*, *13*(12), 1–12. <https://sciencespress.com/index.php/JACAIDMS/article/view/2023-12-04>

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. <https://doi.org/10.3390/app14135501>

Hughes, C. (2022). *Key takeaways from the Open Cybersecurity Schema Format*. CSO Online. <https://www.csoonline.com/article/573487/key-takeaways-from-the-open-cybersecurity-schema-format.html>

IEEE. (2025). *Principles of Open Data Governance - IEEE Digital Privacy*. Ieee.org. <https://digitalprivacy.ieee.org/publications/topics/principles-of-open-data-governance>

IST. (2021). *Ransomware Task Force (RTF)*. Institute for Security and Technology (IST). <https://securityandtechnology.org/ransomwaretaskforce/>

Jakkal, V. (2025). *Microsoft unveils Microsoft Security Copilot agents and new protections for AI | Microsoft Security Blog*. Microsoft Security Blog. <https://www.microsoft.com/en-us/security/blog/2025/03/24/microsoft-unveils-microsoft-security-copilot-agents-and-new-protections-for-ai/?msockid=2e7b7a8ff19a6b6922d36e50f02e6a07>

Jasper, S. E. (2017). U.S. Cyber Threat Intelligence Sharing Frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53–65. <https://doi.org/10.1080/08850607.2016.1230701>

Joyce, S. (2025). *Cloud CISO Perspectives: Data-driven insights into AI and cybersecurity*. Google Cloud Blog; Google Cloud. <https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-data-driven-insights-ai-cybersecurity>

Jurgens, J., & Dal Cin, P. (2025). *Global Cybersecurity Outlook 2025*. <https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf>

KeepnetLabs. (2025). *2025 Verizon Data Breach Investigations Report*. Keepnet Labs. <https://keepnetlabs.com/blog/2025-verizon-data-breach-investigations-report>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Labadie, C., & Legner, C. (2022). Building data management capabilities to address data protection regulations: Learning from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44. <https://doi.org/10.1177/02683962221141456>

Lemieux, F. (2024). Cyber Intelligence. *Emerald Publishing Limited EBooks*, 171–184. <https://doi.org/10.1108/978-1-83549-097-620242011>

Luo, S., Yimamu, N., Li, Y., Wu, H., Irfan, M., & Hao, Y. (2022). Digitalization and sustainable development: How could digital economy development improve green innovation in china? *Business Strategy and the Environment*, *32*(4). <https://doi.org/10.1002/bse.3223>

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving Techniques in Cyber Threat hunting: a Systematic Review. *Journal of Network and Computer Applications*, *232*, 104004–104004. <https://doi.org/10.1016/j.jnca.2024.104004>

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. <https://doi.org/10.9734/jerr/2025/v27i31442>

MITRE . (2024). *MITRE Launches AI Incident Sharing Initiative*. MITRE. <https://www.mitre.org/news-insights/news-release/mitre-launches-ai-incident-sharing-initiative>

Mortaji, S. T. H., & Sadeghi, M. E. (2025). *Assessing the Reliability of Artificial Intelligence Systems: Challenges, Metrics, and Future Directions*. International Journal of Innovation in Management, Economics and Social Sciences, 4(2),. <https://ijimes.ir/index.php/ijimes/article/view/133>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

Okunleye, O. J. (2024). The Role of Open Data in Driving Sectoral Innovation and Global Economic Development. Journal of Engineering Research and Reports, 26(7), 222–243. <https://doi.org/10.9734/jerr/2024/v26i71205>

Okunleye, O. J. (2024). The Role of Information Governance in Mitigating Financial Crime Risks in Stablecoin Transactions. Journal of Engineering Research and Reports, 26(7), 317–333. <https://doi.org/10.9734/jerr/2024/v26i71212>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate “Harvest Now, Decrypt Later” Attacks. *Archives of Current Research International*, *25*(3), 60–80. <https://doi.org/10.9734/acri/2025/v25i31098>

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. <https://doi.org/10.9734/jerr/2025/v27i31444>

Pagano, T. P., Loureiro, R. B., Lisboa, F. V. N., Peixoto, R. M., Guimarães, G. A. S., Cruz, G. O. R., Araujo, M. M., Santos, L. L., Cruz, M. A. S., Oliveira, E. L. S., Winkler, I., & Nascimento, E. G. S. (2023). Bias and Unfairness in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics, and Identification and Mitigation Methods. *Big Data and Cognitive Computing*, *7*(1), 15. <https://doi.org/10.3390/bdcc7010015>

Park, S., & Kwon, H. (2024). Governance of Cyber Threat Information Sharing for Public-Private Partnerships: Comparative Analysis of National Cases. *2024 IEEE/ACIS 24th International Conference on Computer and Information Science (ICIS)*, 41–48. <https://doi.org/10.1109/icis61260.2024.10778364>

Qudus, L. (2025). Cybersecurity governance: Strengthening Policy Frameworks to Address Global Cybercrime and Data Privacy Challenges. *International Journal of Science and Research Archive*, *14*(1), 1146–1163. <https://doi.org/10.30574/ijsra.2025.14.1.0225>

Rawat, P. (2025). *Shodan: Information Gathering Tool*. InfosecTrain. <https://www.infosectrain.com/blog/shodan-information-gathering-tool/>

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection. *Wiley Online Library*, 433–465. <https://doi.org/10.1002/9781394230600.ch19>

Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. de O., & Nze, G. D. A. (2024). Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies. *Future Internet*, *16*(6), 201. <https://doi.org/10.3390/fi16060201>

Ross, N., & Holden, K. (2025). *Key announcements from the Global AI Safety Summit*. Techuk.org. <https://www.techuk.org/resource/key-announcements-from-the-global-ai-safety-summi.html>

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. <https://doi.org/10.3390/s23167273>

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole , D. L., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance - ScienceOpen Library. *Submanuscript.com*, *17*(12). <http://journal.submanuscript.com/id/eprint/2644/1/Salako17122024AJRCOS127573.pdf>

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. <https://doi.org/10.9734/ajrcos/2025/v18i4608>

Sánchez, J. (2023). *Exploring the VirusTotal Dataset | An Analyst’s Guide to Effective Threat Research*. Virustotal.com. <https://blog.virustotal.com/2024/08/VT-S1-EffectiveResearch.html>

Sarker, I. H. (2024). Introduction to AI-Driven Cybersecurity and Threat Intelligence. *Springer*, 3–19. <https://doi.org/10.1007/978-3-031-54497-2_1>

Shepardson, D. (2024). US to convene global AI safety summit in November. *Reuters*. <https://www.reuters.com/technology/artificial-intelligence/us-convene-global-ai-safety-summit-november-2024-09-18/>

Silva, A. D., & Marques, A. J. (2024). Coopetition Networks for Small and Medium Enterprises: A Lifecycle Model Grounded in Service-Dominant Logic. *Systems*, *12*(11), 461–461. <https://doi.org/10.3390/systems12110461>

Spyros, A., Koritsas, I., Papoutsis, A., Panagiotou, P., Chatzakou, D., Kavallieros, D., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2025). AI-based Holistic Framework for Cyber Threat Intelligence Management. *IEEE Access*, 1–1. <https://doi.org/10.1109/access.2025.3533084>

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. *Cyberwarfare*, 351–399. <https://doi.org/10.1007/978-3-030-97299-8_6>

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). *NIST*. <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>

Tendean, M. J., Lim, C., & Silaen, K. E. (2024). Leveraging Honeypot to Uncover Attack Behaviors on Redis. *2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, 589–594. <https://doi.org/10.1109/icicyta64807.2024.10912950>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. <https://doi.org/10.9734/ajrcos/2025/v18i4615>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. <https://doi.org/10.9734/ajrcos/2025/v18i4610>

Tuinier, P., Zaalberg, T. B., & Rietjens, S. (2022). The Social Ties That Bind: Unraveling the Role of Trust in International Intelligence Cooperation. *International Journal of Intelligence and CounterIntelligence*, *36*(2), 1–37. <https://doi.org/10.1080/08850607.2022.2079161>

Vaseashta, A. (2025). Intrinsic and Existential Risks Associated with Emerging Security Threats from Dual-Use Technologies. *Smart Innovation, Systems and Technologies*, 125–137. <https://doi.org/10.1007/978-981-96-0235-3_11>

Vish, E., & Bustamante, G. F. (2024). *Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices*. Securityandtechnology.org. <https://securityandtechnology.org/virtual-library/reports/public-private-partnerships-to-combat-ransomware/>

Yu, J., Shvetsov, A. V., & Alsamhi, S. H. (2024). Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions. *IEEE Access*, 1–1. <https://doi.org/10.1109/access.2024.3482987>

Yun, H. (2024). China’s Data Sovereignty and Security: Implications for Global Digital Borders and Governance. *Chinese Political Science Review*. <https://doi.org/10.1007/s41111-024-00269-9>