ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

INVESTIGATING THE ROLE OF AI-POWERED CYBER THREAT INTELLIGENCE SHARING FRAMEWORKS IN ENHANCING NATIONAL SECURITY ACROSS U.S. PUBLIC SECTOR ENTITIES

Mariatu Mahmoud[1], Barbara Aryeley Aryee[2], Kwadwo Adu Agyemang[3]
[1] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*
[2] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*
[3] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*

Article DOI: https://doi.org/10.36713/epra25500
DOI No: 10.36713/epra25500

ABSTRACT
This study examines the role of artificial intelligence-powered cyber threat intelligence sharing frameworks in enhancing national security across the United States public sector entities. Empirically, traditional silo-based cybersecurity approaches have proven insufficient for protecting government networks and critical infrastructure against the growing scale and sophistication of contemporary cyber threats. Although information sharing is widely recognized as an essential defensive strategy, existing frameworks face significant challenges, including delayed information dissemination, overwhelming data volumes, system interoperability issues, privacy protection requirements and inadequate inter-agency coordination. This study employed a comprehensive systematic literature review methodology, analyzing peer-reviewed journal articles, conference proceedings, government reports and policy documents published between 2016 and 2024, with a specific focus on information sharing frameworks, artificial intelligence architectures and empirical evidence from United States public sector organizations. The study found that AI-driven threat intelligence sharing frameworks significantly improve early warning capabilities, enhance threat detection accuracy and enable more timely cybersecurity decision-making across government agencies through automated threat detection and enhanced analytical capabilities. The findings of the study also indicated that adoption remains inconsistent across agencies due to resource disparities, fragmented governance structures and regulatory privacy constraints that limit effective data sharing among organizations. The study therefore concludes that effective AI-driven intelligence sharing requires coordinated governance frameworks, interoperable technical systems, privacy-preserving technologies and continued human oversight to strengthen national cyber defense posture, with important implications for policymakers, cybersecurity professionals and government administrators responsible for protecting critical national infrastructure.

KEYWORDS: *AI-Powered Cyber Threat Intelligence, Information Sharing Frameworks, National Security, Public Sector Cybersecurity, Machine Learning, Inter-Agency Collaboration*

INTRODUCTION
The national security infrastructure of the United States faces significant challenges due to the growing sophistication of cyber threats. Public sector entities like federal agencies, state governments and operators of vital infrastructure continue to be targeted by nation-state actors, organized crime groups and individual threat actors (Lanz, 2022). The volume and complexity of contemporary cyber threats have proven too much for traditional cybersecurity strategies based on distinct defense mechanisms to handle (Okoli et al., 2024). Automated intelligence sharing frameworks and AI-powered platforms like those developed by Manoharan and Sarker (2023) offer new ways to detect and respond to threats. Real-time threat indicator analysis, pattern recognition across dispersed networks and the prompt delivery of useful intelligence to stakeholders are all made possible by these AI-powered platforms (Manda, 2024; Ajayi-Kaffi, 2024).

Over the last decade, the concept of cyber threat intelligence sharing has grown significantly, as entities recognize that coordinated defense tactics provide better security than compartmentalized alternatives. Information sharing allows entities to benefit from pooled knowledge about new dangers, attack vectors and defensive remedies (Eltayeb, 2024). Traditional threat intelligence sharing channels, on the other hand, have significant constraints, such as information distribution delays, data standardization hurdles and difficulty processing huge amounts of threat data (Rehman & Hashmi, 2023). The use of artificial intelligence in these frameworks overcomes many of these restrictions by automating data gathering, processing and distribution (Parycek et al., 2024; Ajayi-Kaffi et al., 2025). AI can spot dangers faster than humans, find hidden patterns in data and decide what is most important. (Aramide, 2023).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Notwithstanding the potential benefits of AI-powered threat intelligence sharing, considerable impediments prevent widespread implementation across U.S. public sector groups. Privacy considerations, regulatory constraints on data sharing and interagency coordination challenges impede effective collaboration (Pickering & Fox, 2022). Public sector entities must strike a balance between the need to share threat information and the duty to preserve sensitive data and maintain public trust. Technical constraints, such as the necessity for interoperable systems, standardized data formats and secure communication channels capable of handling both classified and unclassified material, remain a challenge for information sharing (Hazra et al., 2021).

Furthermore, concerns persist concerning the trustworthiness of AI-generated threat assessments because of the possibility of adversarial manipulation of machine learning systems and the resources required to install and maintain these advanced frameworks (Rana & Chicone, 2025).

This study looks at the role of AI-powered cyber threat intelligence sharing frameworks in improving national security among U.S. public sector entities. The study summarizes existing research on the technical capabilities of AI-driven threat intelligence systems, assesses the efficacy of current sharing frameworks and highlights organizational and regulatory variables influencing acceptance and deployment. Through examining both the opportunities and challenges associated with these systems, this study seeks to give insights into policymakers, security professionals and researchers seeking to improve the cyber defense posture of the nation. The findings contribute to a better understanding of how emerging technologies can be used to address complex security concerns while remaining within the practical restrictions of public sector operations.

METHODOLOGY

This study employs a systematic approach to identifying, evaluating and synthesizing existing research on AI-powered cyber threat intelligence sharing frameworks in the United States public sector. Terms like "artificial intelligence," "cyber threat intelligence," "information sharing," and "public sector cybersecurity" were searched in academic databases like IEEE Xplore, ACM Digital Library, Google Scholar and government repositories. The review focuses on peer-reviewed journal publications, conference proceedings, government reports and policy documents published between 2016 and 2024 to reflect recent advancements in AI technologies and threat intelligence procedures. Selected sources were analyzed thematically to highlight significant technical capabilities, implementation issues, policy considerations and efficacy metrics for AI-powered threat intelligence sharing frameworks.

LITERATURE REVIEW

AI and Machine Learning Architectures for Cyber Threat Intelligence

Several machine learning architectures that handle various facets of threat detection and analysis are necessary for the application of artificial intelligence to cyber threat intelligence. Support vector machines and random forests are two examples of supervised learning algorithms that have been used to categorize known threat patterns using labelled training data from prior cyber occurrences (Dey & Bhakta, 2023). By comparing observed behaviors to past attack datasets, these algorithms allow systems to detect malware signatures, phishing attempts and network intrusions (Tampinongkol et al., 2024). When analyzing complicated, high-dimensional security data like network traffic logs and system call sequences, deep learning architectures, such as convolutional neural networks and recurrent neural networks, have proven to perform better (Rithani et al., 2023). These neural networks autonomously extract features from unprocessed data, eliminating the need for human feature engineering and making it possible to identify complex threats that elude traditional rule-based systems (Essien et al., 2021).

Unsupervised learning approaches are crucial for finding previously unknown threats and zero-day vulnerabilities that lack historical precedence. Clustering techniques like k-means and hierarchical clustering aggregate comparable network behaviors and system activities to create baseline patterns of regular operations (Miraftabzadeh et al., 2023). Deviations from defined baselines are flagged as potential security problems using autoencoder and isolation forest-based anomaly detection algorithms (Kumar et al., 2025). These unsupervised approaches solve the restriction of supervised models, which can only detect threats similar to those in their training data (Usama et al., 2019). Generative adversarial networks have emerged as a potential method for creating synthetic threat scenarios that increase training datasets and model resilience to adversarial attacks (Kumar & Sinha, 2023).

AI systems extract threat intelligence from unstructured text sources, like security reports, vulnerability databases, dark web forums and social media platforms, by using natural language processing capabilities. From narrative descriptions, named entity recognition and information extraction algorithms find pertinent threat indicators such as malware names, attack methods and targeted vulnerabilities (Marinho & Holanda, 2023). In order to predict new attack trends and comprehend adversary intentions, sentiment analysis and topic modelling algorithms examine conversations among threat actors (Zhong et al., 2024). To capture relationships between threats, vulnerabilities, attack vectors and impacted systems, knowledge graph creation techniques can arrange extracted data into organized representations (Sikos, 2023). Large amounts of textual intelligence are converted by these natural language processing skills into machine-readable formats that can be used for automated reasoning and decision assistance (Kumar, 2024).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

The integration of different AI architectures into ensemble systems improves overall threat intelligence capabilities by integrating the advantages of many techniques. Hybrid models that combine supervised and unsupervised learning techniques improve detection rates while preserving acceptable false positive rates (Landress, 2016). Attention methods and transformer structures, which were originally designed for language processing, have been modified to prioritize relevant characteristics in security data and capture long-range dependencies in attack sequences (Latibari et al., 2024). Reinforcement learning frameworks allow adaptive defense systems to acquire optimal response tactics by interacting with simulated threat environments (Kalejaiye, 2022). The ongoing advancement of AI systems gives both potential for improved threat intelligence and limitations in terms of processing needs, model interpretability and vulnerability to adversarial manipulation (Babatunde et al., 2020)

Table 1: AI and Machine Learning Architectures in Cyber Threat Intelligence

AI Architecture	Primary Application	Key Capabilities	Limitations
Supervised Learning (SVM, Random Forest)	Known threat classification	High accuracy for labeled threats; pattern matching from historical data	Requires extensive labeled datasets; cannot detect novel threats
Deep Learning (CNN, RNN)	Malware analysis and complex pattern recognition	Automatic feature extraction; processing of high-dimensional data; assists analysts with malware triage and indicator extraction	High computational cost; limited interpretability; vulnerability to adversarial attacks
Unsupervised Learning (Clustering, Anomaly Detection)	Zero-day threat identification and network anomaly detection	Detects unknown threats; establishes behavioral baselines; identifies potential malicious activity in network traffic	Higher false positive rates; difficulty distinguishing anomalies from benign variations
Natural Language Processing	Intelligence extraction from text and automated PII detection	Processes unstructured data; identifies threat indicators from reports; flags potential personally identifiable information in submissions	Context interpretation challenges; language ambiguity; requires human review for accuracy
Decision Tree Models	Confidence scoring for threat indicators	Assigns reliability scores to cyber threat submissions; helps analysts prioritize information for review	Limited to predefined scoring criteria; may not capture nuanced threat characteristics
Machine Learning Analytics	Data fusion and correlation	Automates correlation processes; highlights potential anomalies; narrows the scope of analysis for security analysts	Requires integration with existing systems; dependent on data quality
Ensemble and Hybrid Models	Comprehensive threat detection	Combines multiple approaches; balances detection and false positives; enables threat hunting across federal networks	Increased system complexity; resource-intensive; requires sophisticated governance

Source: Adapted from NIST Cybersecurity Framework Profile for Artificial Intelligence (NIST IR 8596, 2025) and CISA AI Use Case Inventory (DHS, 2025)

Organizational and Policy Frameworks for Inter-Agency Cybersecurity Collaboration

In response to growing cyber threats, the legal and administrative framework governing cybersecurity information sharing among U.S. public sector entities has changed significantly during the past 20 years. In addition to offering participants liability safeguards, the Cybersecurity Information Sharing Act of 2015 created fundamental procedures for the voluntary exchange of cyber threat indicators between public and private sector entities (Barnhill, 2023; Aryee et al., 2025). In order to coordinate cybersecurity efforts within their particular critical infrastructure sectors, Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience designated several federal entities as sector-specific agencies (Simon, 2020; Gokah et al, 2025). The National Cyber Strategy, which was issued in 2018 and modified throughout time, emphasizes the importance of information-sharing partnerships and outlines goals for federal cybersecurity activities such as network and critical infrastructure protection (Dion, 2020). These policy instruments establish the formal structure for AI-powered threat intelligence sharing frameworks by specifying roles, duties and legal constraints for inter-agency collaboration (Ewuola, 2025; Gokah et al., 2025).

Organizational constraints have a substantial impact on the effectiveness of inter-agency cybersecurity collaboration, notwithstanding supporting policy frameworks. Federal agencies have distinct missions, organizational cultures and technical infrastructure, which complicates coordinating efforts (Wilson & Mergel, 2022). Agencies' trust deficits come from worries about data sensitivity, classification levels and the potential exploitation of shared information for purposes other than cybersecurity (Dlamini et al., 2024). Bureaucratic barriers such as uneven data formats, incompatible communication platforms and fragmented governance structures limit smooth information transmission (Vallabhaneni, 2025). Because smaller entities might not have personnel or technical capabilities to properly participate in sophisticated threat intelligence sharing platforms, resource discrepancies among agencies create further obstacles (Jesus et al., 2023). However, the federal government's adoption and utilization rates of AI-powered sharing systems are influenced by these organizational characteristics (Rosengren & Kvarnmarker, 2024; Akande & Enyejo, 2024).

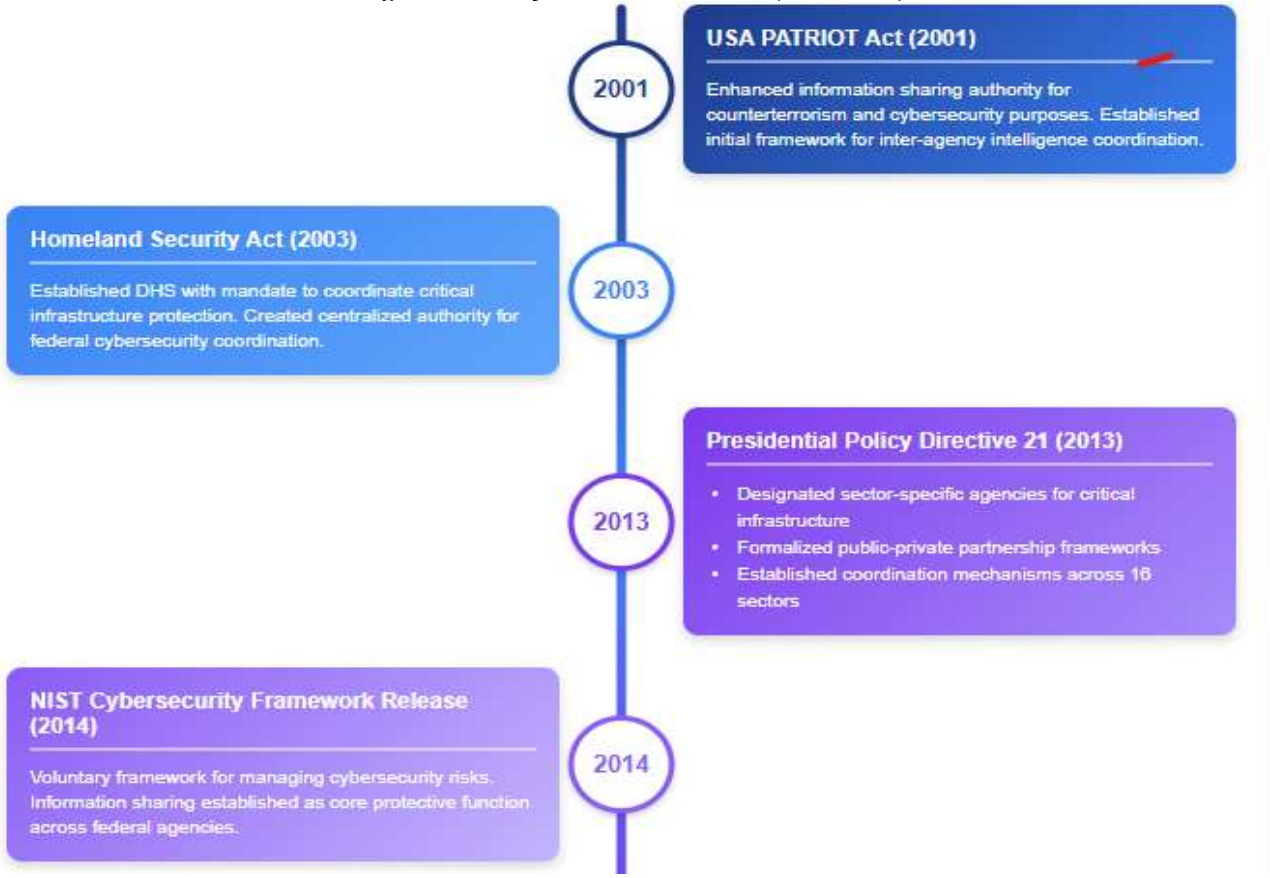
Theoretical frameworks for comprehending how public sector entities coordinate cybersecurity efforts across organizational borders are provided by collaborative governance models. The

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Network governance theory states that in order to achieve a successful interagency collaboration, horizontal coordination methods are preferred over conventional hierarchical command structures (Laegreid & Rykkja, 2022). Governance systems for information sharing must strike a balance between decentralized flexibility to meet agency-specific requirements, limitations and centralized coordination to guarantee standardization and interoperability (Al-Maamar, 2025). The social capital required for long-term cooperation is facilitated by trust-building strategies such as cooperative training programs, staff exchanges and joint exercises (Daghar et al., 2021). Institutional initiatives help to provide centralized leadership while considering agency autonomy, as shown in the creation of coordinating agencies like the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (Campbell, 2023). These governance frameworks have an impact on the development, deployment and upkeep of AI-powered threat intelligence platforms across the interagency ecosystem (Sundaramurthy et al., 2022).

Cybersecurity information sharing frameworks are subject to significant limitations that affect the system design and operational procedures due to privacy and civil liberties considerations. The Privacy Act of 1974 limits the gathering, use and sharing of personally identifiable information by federal agencies, necessitating cautious procedures when such information is present in threat intelligence data (Pulver & Medina, 2018). Government cybersecurity operations are subject to the Fourth Amendment's prohibitions against arbitrary searches and seizures, which call for legal frameworks that strike a balance between security requirements and constitutional rights (Chambers, 2023). Executive orders and presidential directives provide requirements for civil liberties protections and privacy effect assessments in cybersecurity programs (Schertler & Bronfman, 2018). Transparency and accountability systems, including oversight by Congress, inspectors general and privacy officers, help to guarantee that information-sharing activities remain lawful and ethical (Graham et al., 2016). To address legitimate concerns while retaining operational efficacy, AI-powered threat intelligence systems must contain privacy-preserving approaches such as data anonymization, access controls and audit trails (Adeyeye et al., 2024; Akande & Enyejo, 2023).

Figure 1a: Early Foundation Period (2001-2014)

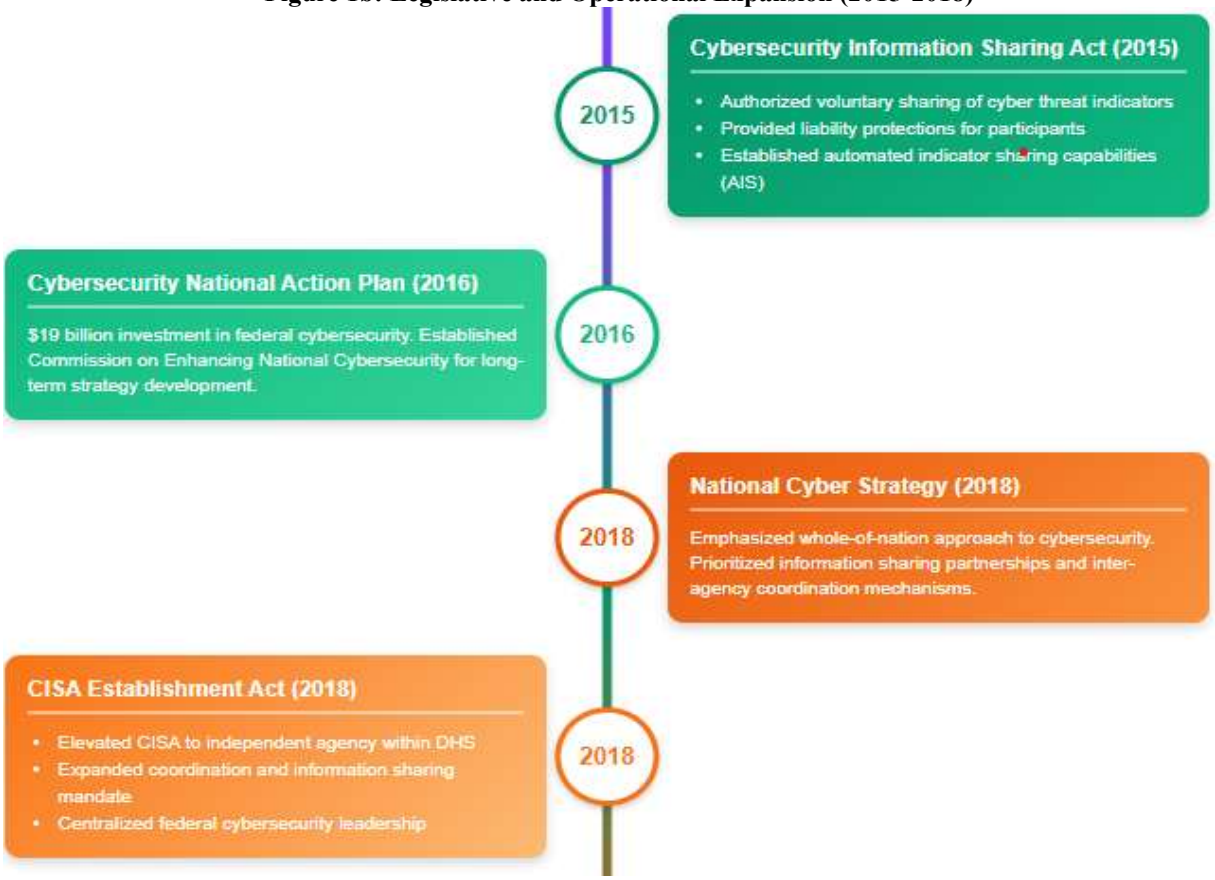


Source: Compiled from White House (2013, 2018, 2021, 2023), DHS (2018), CISA (2015, 2024).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Between 2001 and 2014, the legislative and administrative framework for federal cybersecurity information sharing was built in response to post-9/11 security concerns. The USA PATRIOT Act of 2001 and the Homeland Security Act of 2003 established preliminary frameworks for inter-agency intelligence coordination and identified DHS as the primary authority for critical infrastructure protection. Presidential Policy Directive 21 of 2013 formalized the sector-specific agency framework, assigning federal institutions in charge of coordinating cybersecurity efforts within their various critical infrastructure sectors. The NIST Cybersecurity Framework, released in 2014, presented a voluntary, standardized method for addressing cybersecurity risks and established information exchange as a primary protective function across federal agencies.

Figure 1b: Legislative and Operational Expansion (2015-2018)



Source: Compiled from White House (2013, 2018, 2021, 2023), DHS (2018), CISA (2015, 2024).

The Cybersecurity Information Sharing Act of 2015 marked a watershed moment, establishing voluntary mechanisms for sharing cyber threat indicators between government and private sector entities while also providing critical liability protections that addressed longstanding participation barriers. The Cybersecurity National Action Plan of 2016 indicated federal commitment by investing $19 billion in cybersecurity infrastructure and establishing the Commission on Enhancing National Cybersecurity for long-term strategic planning. The 2018 National Cyber Strategy emphasized a whole-of-nation approach to cybersecurity, highlighting information-sharing partnerships and inter-agency coordination mechanisms as critical components of national defense. CISA's elevation to an independent agency within DHS in 2018 offered committed institutional leadership with enhanced requirements for coordination and information sharing among federal institutions and critical infrastructure sectors.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Figure 1c: Modernization and Mandatory Requirements (2021-2024)

Source: Compiled from White House (2013, 2018, 2021, 2023), DHS (2018), CISA (2015, 2024).

Executive Order 14028, which was issued in 2021, represented a significant modernization effort by mandating the implementation of zero-trust architecture across federal agencies, requiring enhanced information sharing on cyber incidents and establishing the Cyber Safety Review Board to investigate major cybersecurity events. The 2023 National Cybersecurity Strategy represented a developing policy approach, transferring responsibility to entities best positioned to decrease risks and emphasizing harmonized legislation to enable a more efficient public-private partnership. The Cyber Incident Reporting for Critical Infrastructure Act, which went into effect in 2024, required mandatory reporting of covered cyber incidents and ransomware payments, addressing persistent voluntary participation gaps that reduced threat intelligence coverage. This period shows a policy shift away from completely voluntary frameworks toward hybrid methods that mix incentive involvement with required requirements for critical infrastructure firms, reflecting lessons learned from previous implementation challenges.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Figure 1d: Key Impacts on Inter-Agency Collaboration

Source: Compiled from White House (2013, 2018, 2021, 2023), DHS (2018), CISA (2015, 2024).

The evolution of federal cybersecurity policy frameworks has resulted in a robust legal underpinning for trusted information exchange, including liability safeguards, standardized procedures and unambiguous authority for both voluntary and mandatory sharing methods. The creation of CISA as a centralized coordinating authority while retaining sector-specific agency autonomy demonstrates a balanced governance approach that fits varied agency missions and organizational cultures within a cohesive national cybersecurity strategy. Technical capabilities have advanced significantly thanks to automated sharing platforms like AIS and standardized frameworks like NIST CSF, allowing for real-time collaboration and reducing the manual coordination burden that previously hampered effective inter-agency information exchange. The gradual transition from purely voluntary mechanisms to hybrid models that include mandatory reporting requirements is a policy response to persistent participation gaps, recognizing that comprehensive threat intelligence coverage necessitates both incentivized collaboration and baseline obligations for critical infrastructure protection.

Implementation and Adoption of AI-Powered Threat Intelligence Platforms in U.S Government Agencies

Petriashvili and Piotrowski (2025) examined AI implementation across U.S. federal agencies following the 2019 American AI Initiative, using an original dataset of 1,757 AI applications from 37 civilian agencies. Their study found that 21 agencies used AI for anticorruption and security goals such as fraud detection, risk assessment, process automation and transparency reporting, whereas 16 agencies showed little or no interest in AI deployment. Their study discovered that AI is increasingly being used to uncover financial irregularities and increase oversight, particularly in high-risk policy domains like healthcare and homeland security (Sani & Aryee, 2025). However, the findings revealed fragmented implementation patterns, with agencies adopting discrete tools in the absence of a cohesive governance structure, raising questions about equity, efficacy and accountability throughout the federal landscape.

Similarly, Adepoju and Chinonyerem (2024) conducted a study on AI-powered oversight implementation in U.S. public institutions using a mixed-methods approach that included quantitative content analysis of documents from 30 federal and state agencies as well as qualitative insights from 22 semi-structured interviews conducted between 2020 and 2024. The quantitative investigation revealed that 83% of sampled agencies used at least one AI oversight tool, including fraud detection algorithms in 60%, natural language processing for policy compliance in 50% and predictive analytics in 40%. Their study assessed unambiguous operational outcomes, including a 35% reduction in audit cycle durations, a 28% increase in anomaly detection rates and a 12% average cost savings. Their qualitative findings revealed opportunities for increased transparency and accountability through AI dashboards and logging systems. They also identified significant challenges such as algorithmic bias affecting small contractors, data privacy concerns when combining multiple datasets and automation complacency, in which staff relied too heavily on automated outputs without adequate human verification.

Equally, Amomo (2022) investigated how artificial intelligence enhances threat intelligence to enable early warning of intrusions into federal U.S. information systems, specifically in the use of machine learning models on network traffic and endpoint

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

telemetry. His study focused on identifying signs of system compromise, including lateral movement and privilege escalation, before serious attacks took place. His research was to build a federated learning system that would protect data privacy as well as allow intelligence sharing among federal agencies. There were participants from CISA, DHS and DoD. People trust not only what they can see, but also what they hear directly. This model served as an enabler for the Zero-Trust security architecture proposed by Executive Order 14028 that hardened federal systems to address evolving cyber threats without sacrificing privacy. The desired result was a more robust, efficient system that could block massive breaches of critical government computer networks by detecting and containing sophisticated threats from abroad or disgruntled government employees more quickly.

Adewusi et al. (2024) conducted a comprehensive review of artificial intelligence applications in cybersecurity for protecting the U.S. national infrastructure, examining various AI-driven cybersecurity strategies such as anomaly detection and predictive analysis, threat intelligence and automated response mechanisms. Their study found that using AI in cybersecurity increased the speed and accuracy of threat identification while addressing the dynamic nature of cyber threats to critical infrastructure. Their study examined how particular AI technologies employed in the United States, like neural networks, machine learning and natural language processing, support the robustness of the country's infrastructure. However, the review also examined the challenges and ethical considerations associated with widespread AI adoption, emphasizing the need for strong regulatory frameworks to govern AI deployment in sensitive domains, as well as the importance of collaboration among government agencies, private enterprises and research institutions to foster innovation and combat emerging threats.

Comparative Analysis of Threat Intelligence Sharing Outcomes across Jurisdictions and Sectors

Dykstra et al. (2023) conducted a study on an analytical analysis of the financial advantages that entities receive from obtaining and analyzing cyber threat intelligence provided by the U.S. government in various organizational situations. Their study found a significant relationship between the advantages of acquiring CTI and the difference between the threat level indicated by the CTI and the threat level previously perceived by the receiving organization. Their study also discovered that the magnitude of adjustments to cybersecurity investments is inversely related to the organization's prior belief of the threat level, for the same difference between threat levels indicated by CTI and the organization's prior belief. This means that greater benefits can be obtained when the receiving organization's prior belief of a threat level is lower. These results cast doubt on the widely held belief that federal agencies should only share CTI about vulnerabilities with the highest threat level. Instead, they suggested that the benefits of CTI sharing could be enhanced if producers gain a better understanding of the prior beliefs of entities and concentrate on sharing intelligence that differs significantly from those beliefs.

Another research, by Bobish (2023), focused on the exchange of cyber threat information among U.S. critical infrastructure public and private entities, while analyzing benefits and disadvantages within several sectors. His research sought to understand why operational technology networks in critical infrastructure are a growing target for adversaries and assess the effectiveness of existing information-sharing programs. His study found that U.S. critical infrastructure entities encounter more advanced cyber threats each year, which brings a division between the government, the private sector and the cybersecurity industry over whether sharing information improves or lessens an organization's security. A comparative analysis between sectors revealed that participation and effectiveness in exchanging threat information differed, suggesting strategies for legislative guidance and programs to enhance the exchange of threat information for public and private owners of critical infrastructures. His results highlighted sector-specific obstacles that impede consistent patterns of use of the sharing of threat intelligence across the critical infrastructure.

Furthermore, a study by Yatagan (2023) looked at cyber threat intelligence sharing between the U.S. Intelligence Community and the private sector using qualitative analysis and comparative case studies to examine the flow of intelligence sharing across different organizational contexts. To demonstrate patterns of successful and poor intelligence cooperation, the researchers used process-tracing methodologies with declassified government papers, publicly available reports, policy declarations and media reporting. According to their study, intelligence sharing between the Intelligence Community and the private sector is critical to successful cyber defense against threat actors before, during and after attacks. Their comparative research showed that as the quantity and quality of fast, accurate and actionable intelligence supplied through proper ways grows, so does the likelihood of successful defense, including prevention, detection and timely response. Their study revealed significant differences in the efficacy of sharing among various public-private partnerships, with success mostly reliant on well-established trust relationships and suitable information exchange channels.

Also, Ashfaq (2024) conducted a quantitative cross-sectional analysis of 200–300 acute-care hospitals using cloud-based analytics pipelines and enterprise electronic health record ecosystems to address privacy-preserving data sharing across U.S. hospital networks. His study examined the relationship between analytic utility, exchange quality and security posture across several healthcare entities, AI setups and privacy-enhancing strategies. The results in his study showed that higher privacy technology maturity was positively related to both analytic utility and exchange quality, with governance maturity enhancing positive impacts and utility partially mediating the privacy-to-exchange link. The comparative analysis revealed that breach risk is lower in high-maturity, well-governed settings and that privacy-enhancing techniques such as differential privacy,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

federated learning with secure aggregation, homomorphic encryption and secure multi-party computation allow for trustworthy sharing while maintaining security. These findings show that privacy engineering and governance maturity transform privacy concerns into enablers of reliable analytics and information sharing across organizational borders in sensitive settings.

FINDINGS

The results of this study show that by facilitating quicker identification of known and unknown threats, enhancing situational awareness and bolstering proactive defense strategies, AI-powered cyber threat intelligence sharing frameworks greatly improve the detection, analysis and response capabilities of U.S. public sector entities. The evaluated studies provide evidence that machine learning and natural language processing approaches reduce analyst effort and response times while improving threat classification, anomaly detection and intelligence extraction accuracy. However, organizational, legal and governance factors such as inter-agency trust, data standardization, privacy safeguards and resource capacity have a significant impact on how effective these frameworks are.

Although many entities have embraced AI tools with quantifiable operational advantages like enhanced anomaly detection and cost savings, the public sector's adoption of these tools is still dispersed and unequal. The study also demonstrates that collaborative governance frameworks and privacy-preserving technology can improve information-sharing outcomes and lessen data protection problems. Overall, the study concludes that AI-powered threat intelligence sharing has great potential to improve national security; nevertheless, its full potential requires interoperable systems, coordinated regulatory frameworks and a balanced combination of automation and human control.

CONCLUSION

This study concludes by showing how AI-powered cyber threat intelligence sharing frameworks present a revolutionary chance to improve national security for all U.S. public sector entities. These solutions address key shortcomings of traditional, compartmentalized cybersecurity approaches by facilitating prompt, accurate and cooperative threat detection and response. However, their efficacy depends on favorable policy frameworks, robust privacy protections, strong interagency governance and sufficient technical capability. Building a robust and flexible national cyber defense architecture requires the coordination and implementation of morally sound AI-driven intelligence sharing, supported by human oversight.

REFERENCES

1. *Adepoju, A. S., & Chinonyerem, C. A. (2025). Advancing good governance through AI-powered oversight in the United States: Risks and opportunities for public institutions. International Journal of Humanities, Literature and Art Research.*
2. *Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. World Journal of Advanced Research and Reviews, 21(1), 2263-2275.*
3. *Adeyeye, O. J., Akanbi, I., Emeteveke, I., & Emehin, O. (2024). Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection. International Journal of Research and Publication and Reviews, 5(10), 3208-3223.*
4. *Al-Maamari, A. (2025). Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China. arXiv preprint arXiv:2503.05773.*
5. *Amomo, C. (2022). AI-enabled threat intelligence for early detection of intrusions in US federal information systems. International Journal of Science and Research Archive, 7(2), 912-923.*
6. *Akande, S. A., & Enyejo, J. O. (2024). Leveraging predictive analytics to improve demand forecasting and inventory management in healthcare supply chains. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), Article IJSRSET2512184624. https://doi.org/10.32628/IJSRSET2512184624*
7. *Akande, S. A., & Enyejo, J. O. (2023). Artificial intelligence in supply chain management: A systematic review of emerging trends and evidence in healthcare operations. International Journal of Scientific Research and Modern Technology, 3(12), 257–272. https://doi.org/10.38124/ijsrmt.v3i12.1055*
8. *Aramide, O. O. (2023). Predictive Analytics and Automated Threat Hunting: The Next Frontier in AI-Powered Cyber Defense. International Journal of Technology, Management and Humanities, 9(04), 72-93.*
9. *Ashfaq, S. (2025). Artificial Intelligence Based Models For Secure Data Analytics And Privacy-Preserving Data Sharing In US Healthcare And Hospital Networks. International Journal of Business and Economics Insights, 5(3), 65-99.*
10. *Ajayi-Kaffi, O. V. (2024). Is Agile methodology better than waterfall approach in enhancing effective communication in healthcare process improvement projects? International Journal of Research Publication and Reviews, 5(11), 3648–3651.*
11. *Ajayi-Kaffi, O., Emmanuel, I., Azonuche, T. I., & Ijiga, O. M. (2025). Agile-Driven Digital Transformation Frameworks for Optimizing Cloud-Based Healthcare Supply Chain Management Systems. International Journal of Scientific Research and Modern Technology, 4(5), 138–156. https://doi.org/10.38124/ijsrmt.v4i5.1002*
12. *Aryee, B. A., Agyemang, K. A., & Mahmoud, M. (2025). Enhancing operational efficiency of U.S. healthcare data centers through advanced analytics and automation. Finance & Accounting Research Journal, 7(10), 524–539. https://doi.org/10.51594/farj.v7i10.2102*
13. *Babatunde, L. A., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2020). Adversarial machine learning in cybersecurity: Vulnerabilities and defense strategies. Journal of Frontiers in Multidisciplinary Research, 1(2), 31-45.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

14. *Barnhill, B. (2023). Cyber Threat Data Sharing Practices Within the Federal Sector (Doctoral dissertation, Capella University).*
15. *Bobish, M. (2023). Sharing Cyber Threat Information Between the United States' Public and Private Sectors (Master's thesis, Utica University).*
16. *Campbell, I. A. (2023). A Federalist Approach: Exploring the Department of Homeland Security's Role in Securing Critical Infrastructure and Key Resources (Doctoral dissertation, Capitol Technology University).*
17. *Chambers, F. (2023). An Ongoing Seizure: The Struggle to Uniformly Protect Fourth Amendment Interests from Unreasonable Searches of Legally Seized Digital Data. Hous. L. Rev., 61, 153.*
18. *Daghar, A., Alinaghian, L., & Turner, N. (2021). The role of collaborative interorganizational relationships in supply chain risks: a systematic review using a social capital perspective. Supply Chain Management: An International Journal, 26(2), 279-296.*
19. *Dey, P., & Bhakta, D. (2023). A new random forest and support vector machine-based intrusion detection model in networks. National Academy Science Letters, 46(5), 471-477.*
20. *Dion, M. (2020). Cybersecurity policy and theory. In Theoretical Foundations of Homeland Security (pp. 257-284). Routledge.*
21. *Dlamini, T., Maseko, L., Nkosi, S., Khumalo, Z., Ndlovu, J., Smith, A., & Tshabalala, A. (2024). Evaluation of Collaborative Data Sharing Mechanisms for Comprehensive Cyber Threat Mitigation in National Security Crises. Int. J. Appl. Soc. Anal, 9, 1-22.*
22. *Dykstra, J., Gordon, L. A., Loeb, M. P., & Zhou, L. (2023). Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments. Journal of Cybersecurity, 9(1), tyad003.*
23. *Eltayeb, O. (2024). The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks. Journal of Ecohumanism, 3(4), 2422-2434.*
24. *Essien, I. A., Etim, E. D., Obuse, E., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2021). Neural network-based phishing attack detection and prevention systems. Journal of Frontiers in Multidisciplinary Research, 2(2), 222-238.*
25. *Ewuola, A. (2024). Developing Intelligence-Led Security Protocols for Multinational Pipeline Operations in Fragile Environments. DOI: https://doi. org/10.54660/. IJMRGE, 2-1086*
26. *Gokah, B. E., Amoako, E. K., Adom, S. G., Abakah, L. K., & Sampson, E. (2025). AI-driven user experience (UX) frameworks to enhance trust and security in U.S. online banking. Finance & Accounting Research Journal, 7(9), 465–478. https://doi.org/10.51594/farj.v7i9.2069*
27. *Gokah, B. E., Abakah, L. K., & Akinsanya, O. B. (2025). AI-driven detection of fraudulent activities in aged accounts within the U.S. financial system. **Finance & Accounting Research Journal,** **7**(11), 589–601. https://doi.org/10.51594/farj.v7i11.2148*
28. *Graham, F. S., Gooden, S. T., & Martin, K. J. (2016). Navigating the transparency–privacy paradox in public sector data sharing. The American Review of Public Administration, 46(5), 569-591.*
29. *Hazra, A., Adhikari, M., Amgoth, T., & Srirama, S. N. (2021). A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. ACM Computing Surveys (CSUR), 55(1), 1-35.*
30. *Jesus, V., Bains, B., & Chang, V. (2023). Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. IEEE Transactions on Engineering Management, 71, 6854-6873.*
31. *Kalejaiye, A. N. (2022). Reinforcement learning-driven cyber defense frameworks: Autonomous decision-making for dynamic risk prediction and adaptive threat response strategies. International Journal of Engineering Technology Research & Management (IJETRM), 6(12), 92-111.*
32. *Kumar, A. (2024). Language intelligence: Expanding frontiers in natural language processing. John Wiley & Sons.*
33. *Kumar, A., Kumar, A., Raja, R., Dewangan, A. K., Kumar, M., Soni, A., ... & Saudagar, A. K. J. (2025). Revolutionising anomaly detection: a hybrid framework for anomaly detection integrating isolation forest, autoencoder, and Conv. LSTM. Knowledge and Information Systems, 67(12), 11903-11953.*
34. *Kumar, V., & Sinha, D. (2023). Synthetic attack data generation model applying generative adversarial network for intrusion detection. Computers & Security, 125, 103054.*
35. *Lægreid, P., & Rykkja, L. H. (2022). Accountability and inter-organizational collaboration within the state. Public Management Review, 24(5), 683-703.*
36. *Landress, A. D. (2016, March). A hybrid approach to reducing the false positive rate in unsupervised machine learning intrusion detection. In SoutheastCon 2016 (pp. 1-6). IEEE.*
37. *Lanz, Z. (2022). Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories. International Journal of Cybersecurity Intelligence & Cybercrime, 5(1), 43-70.*
38. *Latibari, B. S., Nazari, N., Chowdhury, M. A., Gubbi, K. I., Fang, C., Ghimire, S., ... & Sasan, A. (2024). Transformers: A security perspective. IEEE Access.*
39. *Malik, A., Arshid, K., Noonari, N., & Munir, R. (2025). Artificial Intelligence-Driven Cybersecurity Framework Using Machine Learning for Advanced Threat Detection and Prevention. Sch J Eng Tech, 6, 401-423.*
40. *Manda, J. K. (2024). AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. Available at SSRN 5003638.*
41. *Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.*
42. *Marinho, R., & Holanda, R. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access, 11, 58915-58936.*
43. *Miraftabzadeh, S. M., Colombo, C. G., Longo, M., & Foiadelli, F. (2023). K-means and alternative clustering methods in modern power systems. Ieee Access, 11, 119596-119633.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

44. *Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286-2295.*
45. *Parycek, P., Schmid, V., & Novak, A. S. (2024). Artificial Intelligence (AI) and automation in administrative procedures: Potentials, limitations, and framework conditions. Journal of the Knowledge Economy, 15(2), 8390-8415.*
46. *Pemmasani, P. K., & Abd Nasaruddin, M. A. (2022). Strengthening Public Sector Data Governance: Risk Management Strategies for Government Entities. International Journal of Modern Computing, 5(1), 108-118.*
47. *Petriashvili, I., & Piotrowski, S. J. (2025). Role of AI in Combating Corruption in the U.S. Federal Government: Case Study 2019–2024. Public Integrity, 1–8.*
48. *Pickering, J. C., & Fox, A. M. (2022). Enabling collaboration and communication across law enforcement jurisdictions: Data sharing in a multiagency partnership. Criminal Justice Policy Review, 33(7), 732-755.*
49. *Pulver, A., & Medina, R. M. (2018). A review of security and privacy concerns in digital intelligence collection. Intelligence and National Security, 33(2), 241-256.*
50. *Rana, S., & Chicone, R. (2025). Generative AI Security: Defense, Threats, and Vulnerabilities. John Wiley & Sons.*
51. *Rehman, F., & Hashmi, S. (2023). Enhancing cloud security: A comprehensive framework for real-time detection analysis and cyber threat intelligence sharing. Advances in Science, Technology and Engineering Systems Journal, 8(6), 107-119.*
52. *Rithani, M., Kumar, R. P., & Doss, S. (2023). A review on big data based on deep neural network approaches. Artificial Intelligence Review, 56(12), 14765-14801.*
53. *Rosengren, H., & Kvarnmarker, J. (2024). Key Factors Influencing AI Implementation in Large Entities.*
54. *Sani, Z. N., & Aryee, B. A. (2025). Optimizing drug supply chains to prevent shortages in rural U.S. hospitals. EPRA International Journal of Economics, Business and Management Studies. https://doi.org/10.36713/epra24022*
55. *Schertler, M., & Bronfman, J. (2018). US cybersecurity and privacy regulations. In Human-Computer Interaction and Cybersecurity Handbook (pp. 273-294). CRC Press.*
56. *Sikos, L. F. (2023). Cybersecurity knowledge graphs. Knowledge and Information Systems, 65(9), 3511-3531.*
57. *Simon, I. G. (2020). Effectiveness of National Cyber Policy to Strengthen the Security and Resilience of Critical Infrastructure Against Attacks.*
58. *Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-powered operational resilience: Building secure, scalable, and intelligent enterprises. Artificial Intelligence and Machine Learning Review, 3(1), 1-10.*
59. *Tampinongkol, F. F., Kamila, A. R., Wardhana, A. C., Kusuma, A. W. C., & Revaldo, D. (2024). Implementation of random forest classification and support vector machine algorithms for phishing link detection. Journal of Informatics Information System Software Engineering and Applications (INISTA), 7(1), 127-137.*
60. *Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. L. A., Elkhatib, Y., ... & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access, 7, 65579-65615.*
61. *Vallabhaneni, R. (2025). Breaking Data Silos: Creating Interoperable Government Systems for Holistic Insights.*
62. *Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: mapping the strategies of digital champions. Government Information Quarterly, 39(2), 101681.*
63. *Yatagan, C. (2022). Interaction between the US intelligence community and the private sector in sharing cyber threat intelligence. American University.*
64. *Zhong, C., Liu, H., & Kam, H. J. (2024). Mining Reddit users' perspectives on cybersecurity competitions: a mixed method approach. Information & Computer Security, 32(5), 636-655.*