PAJRI
PAN-AFRICAN JOURNAL OF RESEARCH AND INNOVATION

Pan-African Journal of Research and Innovation in Law, Policy and Development

ISSN: 3413-9431 | Vol. 1, Issue 2 | www.pajri.com | DOI: https://doi.org/10.0000/0000

"Predictive Peace": ECOWAS and the Use of Artificial Intelligence, Mobile Data and Community Resilience

Narayana Osei-Nyarko
Graduate School of Law, University of Gold Coast Accra, Ghana
· * Corresponding author: narayanaomkar@gmail.com

Received: 2026-10-04	Accepted: 2026-10-21	Published: 2026-10-22

ABSTRACT

This article proposes a policy-oriented "Predictive Peace" framework to ECOWAS. Differential capacity to share intelligence, combined with the porous nature of borders, transnational extremist networks, and rapid digital communications in West Africa, produces an environment that facilitates the growth of terrorist threats in the region. The "Predictive Peace" framework considers artificial intelligence (AI), mobile-data analytics and community resilience as mutually constraining elements of a regional early warning system. It analyzes qualitative documents in the field of peer-reviewed literature on cybersecurity and predictive analytics, and is complemented bycounter-terrorism and community intelligence. The legal and policy instruments of ECOWAS and the African Union are considered. The analysis identifies three key findings. First, AI is not sufficient to aid fully-automated Counter-Terrorism (CT) decisions, and mobile-data can help strengthen situational awareness. Second, there are legal and policy-related issues pertaining to the use of mobile-data to support situational awareness. Third, while community engagement can strengthen the quality, and legitimacy, of threat assessments, reporting systems, and other security architecture, this is true only if systems are designed to protect the citizen from retaliation and unaccountable and discriminatory decisions made by state actors based on algorithms. This article therefore positions predictive security as a model of governance. It argues that trust, a human-centered and rights-based approach, can be institutionally integrated into ECOWAS legislation and policy, and controlled by community oversight.
The contribution presents a well-grounded model, integrating the relationships between legal and policy authority, institutions, and social trust, with the right balance of technology.

KEYWORDS: ECOWAS, counter-terrorism, artificial intelligence, mobile data, predictive analytics, community resilience, data protection, predictive peace.

How to Cite
Osei-Nyarko, N. (2026). "Predictive Peace": ECOWAS and the Use of Artificial Intelligence, Mobile Data and Community Resilience. *Pan-African Journal of Research and Innovation in Law, Policy and Development, 1(1), 9-16.*

1. Introduction

In West Africa, transnational terrorism and violent extremism is on the increase, especially in the borderless spaces and digital frontiers. Armed groups operate transnationally by exploiting border spaces, informal networks and communications, including encrypted and online communications and networks, and propoganda, and local grievances to further their aims and objectives, often with capacity to outpace security systems designed for post-incident response. ECOWAS has also admitted that, if the region is to efficiently counter terrorism, it needs to synchronise efforts against terrorism, including through effective intelligence collaboration and cooperation, prevention, the rule of law and respect for human rights. The real issue is not about the scarcity of information to regional structures. The question is, how can the region improve the production of timely and accurate early warnings.

The use of Artificial Intelligence (AI) and big data in terrorism research is still nascent and developing. Existing research in cybersecurity and the dark web, however, indicate the potential of machine learning and deep learning in classifying threats (Halbouni et al., 2022; Ozkan-Okay et al., 2024; Sarker et al., 2021). Predictive analytics, in general, has the potential to complement security institutions that are overwhelmed and stressed by dispersed and flexible threats.

There is a clear difference between technical capacity and legitimate security authority. Predictive systems can be biased, false positive systems, opaque, and may be readily manipulated by adversaries (Rosenberg et al, 2021; Saeed and Omlin, 2023). Furthermore, mobile data technologies raise concerns, especially when location data is coupled with communication data. Considering behavioral data of individuals could reveal even more sensitive information about an individual or a community. For a regional organization like ECOWAS, all these concerns grow exponentially, particularly regarding the diversity in the legal, institutional, and oversight mechanisms among the member states.

Thus, the goal of the article is more specific and policy-oriented: what are the institutional, legal and community conditions that would allow the integration of AI- and mobile data-based early warning to improve ECOWAS's counter-terrorism efforts without turning predictive security into mass surveillance? The focus of the article is to integrate the three components of the Predictive Peace framework (AI-assisted analysis, mobile data and community resilience) and govern them based on legality, necessity, proportionality, explainability, data minimization, human oversight and security.

The article makes three contributions. First, it edits and consolidates the existing fragmented and disparate technical literature. It does not assume that the tools of cyberspace and counter-terrorism are equivalent and treats the field of cybersecurity and the field of counter-terrorism as separate. Secondly, it draws a clear line between evidence and value judgments. Finally, it inverts the present order in the framework, which places ethics and governance at the end, and places them at the core of the framework.

2. Literature Review and Analytical Framework

2.1 AI, Cyber Security and Threat Intelligence

AI is prominent in cyber security due to its ability to discover statistical patterns and abnormalities in large data sets. Sarker et al. (2021) discuss AI in cyber security as an intelligence modelling environment whereby automated methods help in detection and response. Ozkan-Okay et al. (2024) also show how AI and machine learning are permeating throughout the different domains of cyber security. Halbouni et al. (2022) point out that within the field of threat intelligence, threat patterns can quickly and continually evolve which makes it difficult to define them by fixed rules. In these situations, the use of deep learning methods becomes pertinent.

The research cited above directly relates to counter-terrorism. Cyber security research focuses on developing analytical frameworks and methods to identify and examine patterns, abnormalities, and threats in the cyber domain; this body of research, however, does not validate that the same analytical models, frameworks, and methods can be developed to identify and analyze terrorist intent in behavioral data of the civilian population. The policy potential of AI in ECOWAS lies in applying it to prioritize alerts for human analysts to correlate lawfully available intelligence and identify threats which require further analysis, as opposed to relying on AI to confirm threats.

2.2 Predictive Analytics and Terrorist-Network Disruption

Predictive counter-terrorism research focuses on network analysis and attack-risk ranking, as well as computational approaches to identify influential nodes. Collins et al. (2022) illustrate the potential for computational modelling to detect and, more critically, disrupt complex terrorist networks. On the other hand, Khan et al. (2023) illustrate how the integration of AI within predictive analytics has the potential to expand and strengthen threat identification. Overall, the work cited provides evidence of how terrorist networks and threats can be detected and, more importantly, how networks can be defused.

However, predictions must not be confused with absolute certainty. Different factors impact a model's performance including the quality, representativeness, and timeliness of the training data. The performance of a model may be different when it is deployed in a different geographical area. Therefore, when it comes to the actual ECOWAS policy question, the concern is not about a model's ability to predict risk. It is about whether the risk score is high enough to necessitate the use of coercive measures? In the absence of risk scores, prediction should warrant the use of graduated measures, rather than immediate measures.

2.3 Mobile Data and Situational Awareness

Various mobile and wireless devices can produce data that can aid in attaining situational awareness. There is existing research on the use of AI in security and the role of the IoT in security (Adil et al., 2024; Al-Hawawreh et al., 2021). For example, with properly acquired and appropriately minimized mobile data, researchers may be able to spot unusual cross-border movements, shifts in communicative behavior, and other geographic and behavioral concentrations of potential interest.

There are practical limits to how much mobile data are accessible to security agencies, and availability of such data does not give agencies automatic right to process them. Data, particularly metadata, can disclose sensitive relationships and patterns. Coverage of telecommunications networks is not uniform. Mobile devices can be shared. Identifiers do not always point to the individuals that they are supposed to represent. Behavioral patterns can have innocent explanations. Therefore, mobile data are not suitable as standalone indicators of terrorism. Mobile data are more adequately used as corroborating evidence.

2.4 Community Resilience and Digital Participation

Community resilience fosters contextual knowledge that can't be developed by a technology system alone. Members of a community can recognize and identify tendencies in their area, including changes in the way people are recruited and the presence of emerging tensions, even if they do not manifest in traditional intelligence. Other community-related factors of online radicalization are discussed in Berjawi et al (2023). Bridgelall (2022) and Uyheng and Carley (2021) discuss the application of computational analysis and network analysis respectively in information environments related to terrorism.

Participation, however, can create malicious reports. Unfortunate and unproductive reporting systems can promote ethnic and religious profiling and retaliation, especially if the systems do not have adequate mechanisms to prevent retaliation. This is even more the case if reports are done by a community which has already been marginalized, and the reporting system is not separated from the intelligence process to filter out unproductive reports.

2.5 Explainability, Adversarial Risk and Institutional Trust

Restricted optimistic accounts of predictive security primarily consist of two strands of literature. First, if the output of a system is to have an influence on an important decision, then explainability is still of primary importance. Saeed and Omlin (2023) and Moustafa et al. (2023) discuss explainable AI in the context of intrusion detection. Explainability, from an ECOWAS perspective, primarily has an institutional and a technical aspect to it: intelligence shared between agencies and between states should be accompanied by relevant information on provenance and confidence as well as analaytical rationales, to enable responsible use.

Second, AI systems are attack surfaces. Techniques such as evasion and poisoning can cause a model to lose trust and, therefore, potentially fail. Rosenberg et al. (2021) identify these threats and explain their impacts on security. Hu et al. (2021) describe the threats to security that exist for AI systems. If a predictive peace architecture relies on AI to manage insecurity, it should take into account the threats of manipulated or poisoned inputs. Model validation, access control, provenance logging, and red teaming are part of the security architecture and should not be viewed as discretionary improvements to the base design.

2.6 Synthesis and Research Gap

The body of knowledge outlines opportunities for AI to facilitate aspects of analytical work and integrates mobile and IoT data for improved situational awareness. It outlines various threats (adversarial and bias), as well as opacity and data protection. Where it is lacking is the development of an ECOWAS-specific framework that synthesizes and balances these where it is useful from an institutional perspective.

This article addresses a gap in the Predictive Peace framework. Instead of showing how the author combines three data sources to support their predictive framework, the article draws upon how the author separates their architecture into four layers, namely (1) lawful and purpose-limited data acquisition; (2) AI-

assisted fusion and risk analysis; (3) HUMINT and community context; (4) accountable decision-making. Each layer addresses how the author draws a line between technical inference and coercive authority.

3. Methodology

3.1 Research Design

This article takes a qualitative approach and documents analysis. It is more of a conceptual analysis than an empirical test of a predictive security system deployed by the Economic Community of West African States (ECOWAS). A qualitative approach is fitting since published studies on Predictive Peace are found more in the conceptual and policy framework rather than actual practice. Due to the nature of the research question, it is appropriate to analyze documents with focus on technology and policy.

3.2 Documentary Corpus and Source Selection

The documentary corpus is organized around two source groups. The first source group includes peer-reviewed journal articles and conference papers included in the manuscript's bibliography and accessible through major scholarly publishers, such as IEEE Xplore, ACM publications, Springer-linked journals, and other indexed journals. The second source group includes official regional instruments and policy documents of ECOWAS and the AU, including the ECOWAS Counter-Terrorism Strategy, the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, and the AU's Convention on Cyber Security and Personal Data Protection (the Malabo Convention). The focus of the legal literature is in 2021-2024, reflecting interests in adversarial AI, explainable AI, and predictive analytics. Other regional legal instruments are retained if they are of governance interest.

Source evaluation for the records reviewed included coverage of AI/machine learning in cybersecurity and threat intelligence or in predictive analytics for terrorism and network disruption, mobile/IoT data for security intelligence, explainable/adversarial AI, as well as community/crowd-sourced intelligence. Records pertaining to legal and policy frameworks in various regions for countering terrorism and data processing were also included. Excluded records were not related to security policy and/or decision-making, and/or were duplicates of other records without analytical added-value, and/or had insufficient bibliographic references, and/or covered AI applications unrelated to the research questions. The review does not aim for systematic-review exhaustiveness; the focus is on ensuring analytical triangulation for technical, policy and governance literature.

3.3 Analytical Procedure

The analysis consisted of four steps. The first step was coding each document based on the elements of its main contribution, i.e. technological capability, data source, operational use, institutional requirement, legal/ethical concern and implementation risk. The second step was identifying convergence and divergence in the claims. In the third step, technology capability was distinguished from author's policy interpretation; capability reported in the cyber security literature was not assessed for legality and operational suitability for counter-terrorism. The last step was classifying the themes under the Predictive Peace framework, and assessing them against the three cross-cutting criteria of operational usefulness, rights and legality, and institutional responsibility.

3.4 Quality, Validity, and Limitations

In Strengthening, it was noted that several design limitations existed. It did not assess a live ECOWAS AI system. It also did not assess predictive accuracy and determine causalities for terrorism incidents. Furthermore, it did not cover the differences in various national implementations of all the member states. Based on these limitations, it was suggested that the results presented should be regarded as policy and conceptual frameworks. The results and recommendations presented need to undergo legal reviews and be verified on a country-specific basis prior to any operationalization.

3.5 Ethical Orientation

Since there were no human subjects in this documentary study, therefore, no additional ethical considerations were required. Nevertheless, due to the nature of the focused architecture which is on risk surveillance and behavioral inference systems and possible sensitivity of the data, ethical considerations are warranted and will be done on the basis of legality, necessity and proportionality, non-discrimination, and human oversight and control, as well as the right to human review and access, etc. Therefore, in the design of the system, if it is possible to do so, consideration will be taken to include the aforementioned requirements.

4. Discussion and Analysis

4.1. From Reactive Counter-Terrorism to Governed Early Warning

There are several types of terrorism and terrorists that may exist across the ECOWAS region. Predictive Peace and other AI technologies may assist member states face their information-integration challenge with prioritization and pattern recognition.Regarding verification and community surveillance and governance functions, the system will provide intelligence leads, and further analysis and corroboration will be necessary to make an operational judgment.

4.2. Mobile Data: Utility Subject to Lawful Authority and Proportionality

Earlier versions of this document viewed mobile data as under-utilized intelligence. Although this is a valid viewpoint to some extent, a more appropriate position, conditional upon the existence of a legal authority and the purposes of countering terrorism, is more defensible. The ECOWAS Supplementary Act A/SA.1/01/10 establishes a regional legal framework for data protection, and the Malabo Convention provides for the remainder of Africa and enhances the principles for the protection of personal data and cybersecurity. As a result, regional innovations for security cannot be designed as if personal data governance is outside of the realm of counter-terrorism.

Therefore, a more rights-compatible program should ensure that distinctions are drawn for levels of data and intrusion. Collection, storage, and use of historical and/or real time location data, and communications data of identifiable individuals should be subjected to greater legal threshold, necessity, purpose limitation, and other related safeguards. Collection and use of mobility data should only be carried out for the purpose of identifying trends and patterns in health, humanitarian and complex emergencies. The data collected should not compromise the safety and/or security of the individuals concerned. Other safeguards, such as access logging, should be applied if there is a risk that collected data may compromise the security of identifiable individuals. Collection and storage of data should be carried out only for as long as is necessary to achieve the purposes for which the data have been collected. Other related safeguards, such as independent oversight, should be applied, to the extent possible.

These safeguards are as important operationally as they are legally. Predictive Peace assumes that more data means more security. However, data hoarding increases the risks of data breaches and trust compromises. Data minimization and relevancy to a defined threat hypothesis can reduce noise and enhance analytical discipline.

4.3 Human Oversight, Explainability, and Contestability

The degree of explainability required of systems varies. A system that, for example, prioritizes a queue of alerts, may require technical interpretability. In contrast, a system that operates coercively on individuals, such as systems that utilize surveillance, border and immigration intervention and/or detention, would require a greater level of explainability, human oversight and challenge.Saeed and Omlin (2023) present a bigger picture of explainability, while the context of ECOWAS provides a multi-agency accountability problem: the receiving agency must know the source and limits of an alert in order to make a decision if they can rely on it.

Therefore, no bad decision should be made by an opaque risk score. For the purpose of an audit, a system should be able to demonstrate to a human reviewer the data, model, and intellectual sources of the inputs, known model limitations and biases, and the reviewer's level of confidence. Audit logs should show who accessed the model, what version of the model was used, what output it generated, what the human reviewer's subsequent action was, and if the alert was later confirmed or denied. These logs should be kept in order to evaluate the performance of the system.

4.4 Community Resilience as a Verification and Legitimacy Layer

In many cases, local actors can add more context to a situation that helps explain movement and behavior. This context can help explain/verify movement that may otherwise appear suspicious. For example, strange movement may actually be seasonal migratory work, or religious activities. Community participation incorporates context that supports the surveillance system.

Predictive peace has to confront the possibility of abuse in community reporting. Predictive systems must create secure channels for reporting, protect reporting confidentiality, use proper triage mechanisms, and implement sanctions for willful misuse. Reports must be coded based on their verification status.

Characteristics based on ethnicity, religion or nationality should not be used in lieu of behavioral evidence of threat. Resilience-building and AML/CFT authorities should be able to describe the mechanisms in place to members of the communities they are targeting. Creating a system to report without trust results in an information deficit and decreases resilience.

4.5 Adversarial Resilience and Model Governance

Predictive Peace will also require extensive controls in order to achieve the resilience it predicts. Additionally, ECOWAS needs to consider the security of its models to counter terrorism. A set of base controls will likely resemble those of an advanced threat intelligence system and include: role-based access controls; secure end-to-end models and data; red teaming; anomaly detection; version control and model revalidation; procedures to suspend a model if its performance deteriorates; and model provenance checks. The focus here should be on identifying performance metrics that expand beyond an overall accuracy threshold. Those would include false positive and false negative rates for various uses. Federal agencies are required to capture whether model-generated alerts led to actionable intelligence. Hence, agencies need to document whether alerts produced by models resulted in actionable intelligence. If a model created numerous false alerts, it may cause information and automation biases among analysts, and thus should not be implemented broadly.

4.6 The Predictive Peace Architecture

The Predictive Peace architecture consists of four interconnected layers. The first layer is a lawful data layer. This layer contains only data collected for defined purposes and within the bounds of applicable legal authority. The second layer is an analytical layer. This layer utilizes various forms of AI and machine learning to reveal hidden patterns, relationships, and other priority signals. The third layer is a contextual-verification layer. This layer is composed of trained human analysis and other operational and community intelligence. The final layer is a governance and action layer. This layer authorizes responding institutions to determine the appropriate action, if any, to take and documents the decision for auditing and oversight.
A governance envelope surrounds these layers. This governance envelope is composed of various policies governing use of the architecture, including data protection, human oversight and redress, non-discrimination, and explainability. The principal conceptual extension of this article is that by incorporating community resilience and rights protection into a predictive architecture that governs the use of AI, legitimate preventive action may be established.

5. Policy Implications for ECOWAS

5.1 Establish a Regional Legal and Governance Baseline

There is a need to establish a regional legal and governance baseline for the use of AI-assisted Security Analytics. The baseline would determine the legal framework for the collection of data, the categories of data, the institutions responsible for data collection, the conditions for the transfer and access of data, the retention limits, the audit limits, and the procedures for oversight and review. This would be based on the ECOWAS Personal Data Protection framework and the existing regional counter-terrorism framework, rather than creating a parallel framework to establish a regional security exception.

5.2 Use a Tiered Data Access Model

The goal of the data access model should be to maintain the smallest scope of surveillance. It should be designed to ensure the functionality of early warning systems while, to the greatest extent possible, limiting analysis to aggregated or anonymized data. It should be designed to allow for access to communication or mobile data only in accordance with the threshold of legality, and when less intrusive data is not available. Emergency procedures should be time limited and subject to review. This model strikes the right balance for ensuring a sufficient scope of investigation while maintaining the smallest scope of surveillance.

5.3 Create Independent and Multi-Level Oversight

The audit and oversight functions cannot be delegated to the same entities operating the system. ECOWAS should create a regional oversight mechanism to set and enforce standards. The mechanism should be able to conduct audits and engage data-protection and oversight authorities. Member states will determine the institutional framework of the mechanism, but the functions to be performed are obvious: authorization, audit, complaints and review, and order remedy.

5.4 Adopt Human-in-the-Loop Decision Rules

Automated decision-making should support and improve, rather than replace, human judgment. Therefore, high impact actions should not be automatically triggered. Certain operations protocols should be in place to determine what level of human confirmation is required and what decision-making should be prohibited. Analysts should be trained on the possible legal and policy implications of the decisions stemming from the data, as well as bias and the possible alternatives.

5.5 Pilot Before Regional Scale-Up

Limited evidence from controlled pilots shows that a region-wide deployment is not warranted, thus in the short-term, ECOWAS should focus on bound use cases of artificial intelligence (AI) such as fusing security alerts and analysis of border crossing trends. Each use case should have performance and impact metrics. The use cases should be piloted to assess their potential utility and risk. The real time prioritization of cyber-threats may warrant a longer deployment time.

5.6. Institutionalize Community Safeguards

Civil society and local stakeholders should be involved in the design of community-based reporting systems, as a minimum, safeguards should be in place for protected channels and rules for confidentiality. These should only be used to report cases where discrimination and/or profiling does not occur. To bolster trust and resilience to covert mass surveillance, feedback mechanisms, and other community engagement and participation systems should be in place.

The Predictive Peace framework takes a different perspective and considers the challenge of designing treaties that use predictive security as a socio-technical architecture. The role of AI is to provide analytical support. Mobile data is legally sensitive and provides valuable but intrusive signals. Communities provide context and legitimacy. Governance is the factor that balances the legality, proportionality, accountability and reviewability of the measures. With this viewpoint, the debate shifts from whether ECOWAS should use AI to how regional institutions should use analyis and intelligence technologies to safeguard rights, build trust and ensure legitimacy of institutions on which sustainable security relies.

Due to the political nature of the issues covered in this paper, future studies should focus on testing the framework in relation to specific ECOWAS applications, assessing the legal and institutional preparedness of national systems and determining model performance and communities' perceptions and trust in AI-based early warning systems. Until there is proof to support the framework, Predictive Peace should be seen as an architecture for structured experimentation.

References

Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A., & Jin, Z. (2024). UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions. IEEE Transactions on Intelligent Vehicles, 9(4), 4583–4605. https://doi.org/10.1109/TIV.2023.3309548

Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2021). Deep learning-enabled threat intelligence scheme in the Internet of Things networks. IEEE Transactions on Network Science and Engineering, 8(4), 2968–2981. https://doi.org/10.1109/TNSE.2020.3032415

African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection.

Berjawi, O., Fenza, G., & Loia, V. (2023). A comprehensive survey of detection and prevention approaches for online radicalization: Identifying gaps and future directions. IEEE Access, 11, 120463–120491. https://doi.org/10.1109/ACCESS.2023.3326995

Bridgelall, R. (2022). Applying unsupervised machine learning to counterterrorism. Journal of Computational Social Science, 5(2), 1099–1128. https://doi.org/10.1007/s42001-022-00164-w

Collins, B., Hoang, D. T., Nguyen, N. T., & Hwang, D. (2022). A new model for predicting and dismantling a complex terrorist network. IEEE Access, 10, 126466–126478. https://doi.org/10.1109/ACCESS.2022.3224603

Economic Community of West African States. (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.

Economic Community of West African States. (2013). ECOWAS Counter-Terrorism Strategy and

Implementation Plan.

Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine learning and deep learning approaches for cybersecurity: A review. IEEE Access, 10, 19572–19585. https://doi.org/10.1109/ACCESS.2022.3151248

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. ACM Computing Surveys, 55(1), 1–36. https://doi.org/10.1145/3487890

Khan, F. A., Li, G., Khan, A. N., Khan, Q. W., Hadjouni, M., & Elmannai, H. (2023). AI-driven counter-terrorism: Enhancing global security through advanced predictive analytics. IEEE Access, 11, 135864–135879. https://doi.org/10.1109/ACCESS.2023.3336811

Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the Internet of Things. IEEE Communications Surveys & Tutorials, 25(3), 1775–1807. https://doi.org/10.1109/COMST.2023.3280465

Ozkan-Okay, M., Akin, E., Aslan, O., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions. IEEE Access, 12, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys, 54(5), 1–36. https://doi.org/10.1145/3453158

Saeed, W., & Omlin, C. (2023). Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities. Knowledge-Based Systems, 263, 110273. https://doi.org/10.1016/j.knosys.2023.110273

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00557-0

Uyheng, J., & Carley, K. M. (2021). Characterizing network dynamics of online hate communities around the COVID-19 pandemic. Applied Network Science, 6, Article 20. https://doi.org/10.1007/s41109-021-00362-x