OPEN ACCESS
Computer Science & IT Research Journal
P-ISSN: 2709-0043, E-ISSN: 2709-0051
Volume 5, Issue 3, P.681-692, March 2024
DOI: 10.51594/csitrj.v5i3.928
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

THEORETICAL FRAMEWORKS FOR THE ROLE OF AI AND MACHINE LEARNING IN WATER CYBERSECURITY: INSIGHTS FROM AFRICAN AND U.S. APPLICATIONS

Fatai Adeshina Adelani[1], Enyinaya Stefano Okafor[2], Boma Sonimiteim Jacks[3,] & Olakunle Abayomi Ajala[4]

[1]Lagos Water Corporation, Lagos, Nigeria
[2]Independent Researcher, Phoenix, Arizona, USA
[3]Independent Researcher, Nigeria
[4]Indiana Wesleyan University, USA

*Corresponding Author: Fatai Adeshina Adelani
Corresponding Author Email: fadelani@gmail.com
Article Received: 10-01-24 **Accepted:** 02-03-24 **Published:** 22-03-24

ABSTRACT

This review paper explores the theoretical frameworks underpinning the application of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing cybersecurity within the water sector, with a focus on both African and U.S. contexts. It delves into the unique cybersecurity challenges faced by the water sector, emphasizing the critical role of AI and ML in identifying, predicting, and mitigating cyber threats. The paper discusses the ethical considerations and regulatory frameworks influencing the deployment of these technologies alongside the technical, socioeconomic, and data privacy challenges encountered. Future directions and emerging trends in AI and ML that could impact water cybersecurity are examined, offering insights into potential

research areas and strategies for overcoming existing barriers. This comprehensive review underscores the importance of integrating AI and ML into water cybersecurity strategies to safeguard critical water infrastructure.

Keywords: Artificial Intelligence, Machine Learning, Water Cybersecurity, Ethical Considerations, Regulatory Frameworks, Emerging Trends.

INTRODUCTION

In an era where digital technologies underpin critical infrastructure, the water sector stands out as both vital and vulnerable. Ensuring the cybersecurity of water management systems is paramount, given their essential role in public health, economic stability, and community well-being. As threats to these systems evolve in complexity and sophistication, traditional cybersecurity measures often fall short, necessitating innovative solutions. This is where Artificial Intelligence (AI) and Machine Learning (ML) come into play, offering advanced capabilities to predict, detect, and respond to cyber threats with unprecedented efficiency and accuracy (George, George, & Baskar, 2023; Sommer & Brown, 2011).

The water sector encompasses a wide range of activities, from supply and distribution to wastewater treatment and flood management. These activities rely heavily on interconnected digital and physical systems, making them susceptible to cyberattacks that could disrupt water supply, contaminate water quality, or even cause environmental disasters (Cosgrove & Loucks, 2015; Leflaive et al., 2012; Niemczynowicz, 1999; Zehnder, Yang, & Schertenleib, 2003). The implications of such attacks are far-reaching, affecting not just individual communities but entire regions. Enhancing cybersecurity in the water sector is not merely a technical challenge but a critical public safety priority (Shapira, Ayalon, Ostfeld, Farber, & Housh, 2021).

AI and ML are at the forefront of transforming cybersecurity approaches. Their ability to learn from data, identify patterns, and make predictions enables proactive identification of potential threats and vulnerabilities. In the context of water cybersecurity, AI and ML can monitor system behaviours in real time, detect anomalies that may indicate a cyberattack, and automate responses to mitigate risks. These technologies also offer the potential to adapt and evolve in response to new threats, ensuring that cybersecurity measures remain effective over time.

This paper aims to:

a) Explore the theoretical foundations of AI and ML in cybersecurity, with a focus on their application within the water sector.
b) Examine the current landscape of cybersecurity threats facing the water sector and the role of AI and ML in addressing these challenges.
c) Highlight the unique considerations and potential of AI and ML in enhancing water cybersecurity, with particular emphasis on applications in African and U.S. contexts.
d) Discuss the ethical, regulatory, and practical challenges of implementing AI and ML solutions in water cybersecurity.
e) Propose future directions for research and practice aimed at leveraging AI and ML to secure water systems effectively.

Background and Significance

The water sector, critical to sustaining life and economic activities, increasingly relies on digital technologies for its operations. This includes Supervisory Control and Data Acquisition (SCADA) systems, Internet of Things (IoT) devices, and cloud computing, which enhance efficiency and reliability. However, this digital integration also exposes the sector to cyber threats, ranging from malware and ransomware attacks to sophisticated nation-state-sponsored cyber espionage. Cybersecurity incidents can lead to service disruptions, compromised water quality, and unauthorized access to sensitive data, posing significant public health and safety risks.

The cybersecurity landscape in the water sector is marked by a diverse range of threats, including but not limited to:

- System Intrusions: Unauthorized access to water utility networks, potentially leading to the manipulation of water treatment processes.
- Data Breaches: Theft or exposure of sensitive data, including customers' personal information and utilities' operational data.
- Denial of Service (DoS) Attacks: Disruption of digital services, hindering the operation of online monitoring and control systems.
- Insider Threats: Risks posed by individuals within the organization who may intentionally or unintentionally compromise cybersecurity.

These challenges are compounded by the sector's unique characteristics, such as the widespread geographic distribution of assets and the integration of legacy systems with newer technologies, which create numerous entry points for cyberattacks.

Importance of Cybersecurity in Water Management in Africa and the U.S.

In both Africa and the U.S., the importance of cybersecurity in water management cannot be overstated. In Africa, the increasing digitalization of water management systems, rapid urbanization, and the critical need for sustainable water resources make cybersecurity a paramount concern. Cyberattacks can severely impact the availability and quality of water, with dire consequences for public health and economic development (Adedeji, Ponnle, Abu-Mahfouz, & Kurien, 2022; Aivazidou et al., 2021).

In the U.S., the complexity and critical nature of water infrastructure make it a target for cyber threats. The U.S. government has recognized water and wastewater systems as one of the critical infrastructure sectors at the highest risk for cyberattacks. The consequences of such attacks can range from local disruptions to widespread environmental and economic impacts, underscoring the need for robust cybersecurity measures.

AI and ML offer significant potential to enhance cybersecurity measures in the water sector by providing advanced tools for threat detection, analysis, and response (Bécue, Praça, & Gama, 2021; Shah, 2021). Their capabilities include:

- Anomaly Detection: AI and ML algorithms can monitor network and system activities in real time, identifying deviations from normal operations that may indicate a cyberattack.
- Predictive Analytics: These technologies can analyze trends and patterns in data to predict potential security incidents before they occur, allowing for proactive measures.

- Automated Response: AI systems can be programmed to automatically respond to detected threats, mitigating their impact without the need for human intervention.
- Enhanced Security Posture: By continuously learning from new data, AI and ML can adapt to evolving threats, ensuring that cybersecurity measures remain effective over time.

The application of AI and ML in the water sector's cybersecurity efforts represents a shift from reactive to proactive and predictive security strategies. This paradigm shift can significantly reduce the vulnerability of water management systems to cyberattacks, ensuring the continued provision of safe and reliable water services (Bécue et al., 2021; Shah, 2021).

In conclusion, the backdrop of cybersecurity in the water sector highlights a landscape fraught with challenges but also opportunities for innovation. The integration of AI and ML technologies into cybersecurity strategies offers a promising path forward, potentially transforming the sector's ability to safeguard against cyber threats. This underscores the critical importance of cybersecurity in water management, particularly in regions as diverse as Africa and the U.S., and highlights the transformative potential of AI and ML in enhancing security measures.

Theoretical Frameworks

AI and Machine Learning Concepts

Artificial Intelligence (AI) encompasses a broad range of technologies that enable machines to mimic human intelligence. This includes learning from data, making decisions, and performing tasks that typically require human intelligence (Hassani, Silva, Unger, TajMazinani, & Mac Feely, 2020). Machine Learning (ML), a subset of AI, involves algorithms and statistical models that enable computers to perform specific tasks without using explicit instructions, instead relying on patterns and inferences derived from data.

In cybersecurity, AI and ML are applied to automate the detection of threats and anomalies, predict potential vulnerabilities, and respond to cyber incidents. These technologies can process and analyze vast amounts of data at speeds far beyond human capabilities, identifying subtle patterns indicative of cyber threats. For example, ML algorithms can learn from past cybersecurity incidents to recognize the characteristics of malware, phishing attempts, and unusual network traffic that may signify a breach (Abdullahi et al., 2022; Sarker, 2023).

Cybersecurity Challenges in the Water Sector

- Specific Cybersecurity Threats to the Water Sector: The water sector faces unique cybersecurity threats, including attacks on industrial control systems (ICS) and SCADA systems that monitor and control the treatment and distribution of water. Threat actors may attempt to manipulate these systems to disrupt the water supply, contaminate water quality, or demand ransom by threatening public health (Asghar, Hu, & Zeadally, 2019).
- Importance of Addressing These Threats Through Advanced Technologies: The critical nature of water infrastructure necessitates the adoption of advanced technologies for cybersecurity. Traditional security measures are often inadequate against sophisticated cyber threats. AI and ML offer the ability to enhance security protocols and monitoring systems in real-time and adapt to new threats as they emerge, ensuring the resilience of water systems against cyberattacks (Djenna, Harous, & Saidouni, 2021; Lewis, 2019).

AI and Machine Learning in Cybersecurity

The theoretical underpinnings of AI and ML in cybersecurity are based on their capability to learn from data, recognize patterns, and make predictions. This is particularly relevant for cybersecurity, where threat patterns can be complex and constantly evolving. ML algorithms can be trained on datasets of security incidents to identify the features of malicious activity, enabling the prediction and detection of threats with high accuracy.

Advantages

AI and ML can quickly analyze large datasets, identifying threats more rapidly than humans. These technologies can predict and identify threats before they cause harm, allowing for proactive defence measures. AI and ML systems can continuously learn and adapt to new and evolving cyber threats, improving their detection capabilities over time. Advanced ML models can differentiate between benign and malicious activities with greater accuracy, reducing the number of false positive alerts (Kaloudi & Li, 2020).

Limitations

ML models' effectiveness heavily depends on the quality and quantity of the data they are trained on. Inadequate or biased data can lead to inaccurate predictions. Developing, training, and maintaining AI and ML systems require significant computational resources and expertise. As AI and ML are used in cybersecurity, attackers also use these technologies to develop more sophisticated attack methods, potentially outpacing defensive measures. The use of AI and ML in cybersecurity raises questions about privacy, data protection, and the potential for misuse (Tschider, 2018).

In conclusion, while AI and ML present significant advantages in enhancing the cybersecurity of the water sector, they also come with challenges that must be carefully managed. Theoretical frameworks underpinning these technologies emphasize their potential to transform cybersecurity practices by enabling more proactive, efficient, and adaptive security measures. However, addressing their limitations and ensuring their ethical use remains critical for their successful implementation in the water sector's cybersecurity efforts.

Applications and Implications

General Applications of AI and Machine Learning in Cybersecurity

AI and machine learning have revolutionized the field of cybersecurity, offering sophisticated solutions to protect digital assets and infrastructure from cyber threats. Their applications span various domains, reflecting their versatility and effectiveness (Gorment, Selamat, Cheng, & Krejcar, 2023; Vähäkainu & Lehto, 2022).

- Threat Detection and Analysis: AI and ML algorithms excel at identifying patterns indicative of cyber threats, such as malware, ransomware, phishing attacks, and anomalous network behaviour. By analyzing vast datasets, these algorithms can detect threats more rapidly and accurately than traditional methods.
- Predictive Security: Leveraging historical data, AI and ML can predict potential vulnerabilities and future attack vectors, allowing organizations to fortify their defences proactively.
- Automated Incident Response: AI-driven systems can automatically respond to detected threats, mitigating their impact. This can include isolating affected systems, blocking malicious traffic, or deploying patches to vulnerabilities.

- Security Policy Enforcement: AI can monitor compliance with security policies across an organization's digital infrastructure, ensuring that all systems adhere to established security standards.
- User Behavior Analytics (UBA): By analyzing patterns of user behaviour, AI and ML can identify deviations that may indicate a security threat, such as a compromised user account or an insider threat.

Potential Implications for Water Cybersecurity in African and U.S. Contexts

The application of AI and ML in water cybersecurity holds significant implications for African and U.S. contexts, each facing unique challenges and opportunities.

In Africa, where resources for cybersecurity may be limited, and water infrastructure is often vulnerable, AI and ML can offer cost-effective solutions to enhance security. These technologies can help in the early detection of threats, reducing the potential for large-scale disruptions. Moreover, AI and ML can assist in overcoming the lack of specialized cybersecurity personnel by automating threat detection and response processes. However, the implementation of these technologies must be tailored to local contexts, considering the availability of data, infrastructure challenges, and the need for capacity building in AI and ML (Kabanda, 2022).

In the U.S., with its complex and highly digitized water management systems, AI and ML can play a crucial role in protecting against sophisticated cyber threats. The technologies can enhance the resilience of critical water infrastructure against targeted attacks, including state-sponsored cyber espionage. The implications include improved security and regulatory compliance as federal and state regulations increasingly mandate robust cybersecurity measures. The adoption of AI and ML in the U.S. must address concerns around privacy, data protection, and the ethical use of AI, ensuring that security enhancements do not compromise civil liberties (ElBaih, 2023; Manheim & Kaplan, 2019).

Tailoring AI and ML to Meet Unique Regional Challenges

To effectively leverage AI and ML in water cybersecurity, these technologies must be adapted to meet the unique challenges of different regions (Fagnan et al., 2019; Sambasivan et al., 2021).

- Data Accessibility and Quality: In regions where high-quality data may be scarce, efforts should focus on gathering and curating relevant datasets to effectively train AI and ML models. This might involve partnerships between governments, international organizations, and the private sector to share data and expertise.
- Infrastructure Compatibility: Solutions must be compatible with existing water management and cybersecurity infrastructure. In regions with legacy systems, hybrid approaches that integrate AI and ML with traditional security measures may be required.
- Capacity Building: Investing in education and training is essential to build local expertise in AI and ML, ensuring that regions can deploy, maintain, and update AI-driven cybersecurity solutions.
- Cultural and Regulatory Considerations: Tailoring AI and ML applications must also consider cultural sensitivities and comply with local regulations, especially regarding data privacy and security.

In conclusion, the application of AI and ML in water cybersecurity offers promising solutions to enhance the resilience of water infrastructure against cyber threats. However, realizing their full potential requires careful consideration of the unique challenges and opportunities present in different regions, particularly in Africa and the U.S. By adapting these technologies to local contexts, it is possible to address the pressing need for robust cybersecurity measures in the water sector, ensuring the safety and reliability of this critical resource.

Ethical and Regulatory Considerations

Ethical Considerations in Deploying AI and Machine Learning for Cybersecurity

The deployment of AI and machine learning (ML) technologies in cybersecurity raises several ethical considerations that must be addressed to ensure their responsible use. These considerations include:

- Privacy: AI and ML systems often require access to vast amounts of data, including potentially sensitive personal information. Ensuring these technologies respect user privacy and comply with data protection laws is essential. This involves implementing data minimization principles, ensuring data anonymization, and obtaining consent.
- Bias and Fairness: AI and ML models can inadvertently perpetuate or amplify biases in their training data, leading to unfair or discriminatory outcomes. Efforts must be made to identify and mitigate biases in datasets and algorithms to ensure that cybersecurity measures do not unfairly target or exclude certain groups (Packin & Lev-Aretz, 2018).
- Transparency and Accountability: There is a need for transparency in using AI and ML in cybersecurity, particularly regarding how decisions are made. This includes understanding how models detect threats and respond to them. Ensuring accountability for the decisions made by AI systems, including avenues for redress when errors occur, is also crucial.
- Security of AI Systems: The AI and ML models can become targets for cyberattacks, including adversarial attacks designed to manipulate model behaviour. Ensuring the security of these systems is an ethical imperative to prevent misuse and ensure they function as intended (Rosenberg, Shabtai, Elovici, & Rokach, 2021).

Overview of Regulatory Frameworks Governing the Use of AI in Cybersecurity in Africa and the U.S.

Regulatory frameworks for AI and cybersecurity are still in development in many African countries, with significant variation across the continent. Some countries have begun to draft national strategies for AI that include cybersecurity considerations, focusing on promoting innovation while ensuring security and privacy. The African Union's Cyber Security and Personal Data Protection Convention, known as the Malabo Convention, provides a broad framework for data protection and cybersecurity. However, its adoption and implementation vary by country.

In the U.S., there is no unified federal framework specifically governing the use of AI in cybersecurity. However, several initiatives and policies address aspects of AI security and ethics. For example, the National Institute of Standards and Technology (NIST) has developed guidelines for AI security and ethical considerations. Additionally, sector-specific regulations, such as those governing critical infrastructure, including the water sector, may indirectly influence how AI and ML are deployed for cybersecurity.

Challenges and Opportunities in Policy and Regulation

Challenges

One of the primary challenges is the rapid pace of technological advancement in AI and ML, which often outstrips the ability of regulatory frameworks to keep up. This can lead to gaps in regulation that may not adequately address emerging ethical and security concerns. Cybersecurity is a global issue, yet differences in regulatory approaches between regions, such as Africa and the U.S., can complicate international cooperation and the development of unified standards. Finding the right balance between encouraging innovation in AI and ML and implementing regulations that ensure ethical and secure use is challenging. Over-regulation may stifle innovation, while under-regulation could lead to ethical breaches and security vulnerabilities.

Opportunities

There is an opportunity to develop international standards and best practices for the use of AI and ML in cybersecurity. Such standards can help harmonize regulatory approaches and ensure high security and ethical consideration globally. Regulatory frameworks can play a crucial role in promoting the development and use of ethical AI, including principles of fairness, accountability, transparency, and privacy. Through regulation, governments can mandate security standards for AI and ML systems, ensuring that these technologies are deployed securely and responsibly.

In conclusion, ethical and regulatory considerations are paramount in the deployment of AI and ML for cybersecurity. Addressing these considerations requires a multifaceted approach, including developing and implementing robust regulatory frameworks, promoting international cooperation, and ensuring that ethical principles are embedded in the development and deployment of AI technologies. As AI and ML continue to evolve, so must the ethical and regulatory landscapes that govern their use, ensuring that these technologies contribute positively to cybersecurity efforts without compromising ethical standards or individual rights (Carter, 2020; Wong, 2021).

Challenges and Barriers

Technical Challenges in Implementing AI and Machine Learning Solutions

- Data Quality and Availability: Effective AI/ML models require large volumes of high-quality, representative data. Collecting comprehensive and clean datasets in the water sector can be difficult due to fragmented infrastructure and varying data collection standards.
- Integration with Existing Systems: Many water utilities operate on legacy systems that may not seamlessly integrate with advanced AI/ML solutions, necessitating significant upgrades or custom solutions.
- Model Complexity and Interpretability: AI/ML models, especially deep learning algorithms, can be complex and act as "black boxes," making it challenging to understand decisions. This complexity can hinder trust and adoption among stakeholders.
- Scalability: Solutions need to be scalable across different sizes and types of water systems, which can vary widely in their infrastructure and cybersecurity needs.

Socio-Economic Barriers in Africa and the U.S.

In many African countries, limited budgets for water management can restrict investments in advanced cybersecurity technologies. In contrast, in the U.S., while funding may be more available, allocating resources efficiently across numerous competing priorities remains challenging. Both regions face a shortage of skilled professionals trained in AI/ML and

cybersecurity, although this issue is more pronounced in Africa. Developing local expertise is essential for implementing and maintaining AI/ML solutions. Understanding and support for investing in cybersecurity, particularly in the water sector, can vary, impacting the willingness of governments and organizations to allocate resources towards these technologies (Harshadeep & Young, 2020; Tagert, 2010).

Data Privacy and Security Concerns

- Sensitive Data Handling: AI/ML systems process vast amounts of data, raising concerns about handling sensitive information. Ensuring data privacy and complying with regulations like GDPR in Europe or varying local laws in Africa and the U.S. presents ongoing challenges.
- Vulnerability to Attacks: AI/ML systems themselves can be targets for cyberattacks, including data poisoning and model evasion strategies. Protecting these systems requires constant vigilance and updates (Hartmann & Steup, 2020).

Future Directions

Emerging Trends in AI and Machine Learning that Could Impact Water Cybersecurity

- Explainable AI (XAI): Advances in explainable AI can make AI/ML models more transparent and their decisions easier to interpret, building trust among stakeholders.
- Federated Learning: This approach allows AI models to be trained across multiple decentralized devices or servers holding local data samples, enhancing privacy and reducing data centralization risks.
- Quantum Computing: Though still in its infancy, quantum computing promises to dramatically increase the processing power available for AI/ML models, potentially transforming cybersecurity by enabling the analysis of even more complex datasets and threats.

Potential Research Areas for Further Exploration

- Developing AI/ML models that can predict failures in water infrastructure before they lead to vulnerabilities.
- Research into sharing threat intelligence across sectors could enhance the detection of cyber threats that impact water systems.
- Investigating frameworks and methodologies for designing AI/ML systems that are inherently secure and ethical.

Strategies for Overcoming Existing Challenges and Barriers

- Investing in education and training programs to build local expertise in AI/ML and cybersecurity within the water sector.
- Encouraging collaboration between governments, academia, and industry to share knowledge, resources, and best practices.
- Developing and implementing policies that encourage the ethical use of AI/ML in cybersecurity while providing clear data privacy and security guidelines.

CONCLUSION

The integration of AI and machine learning into water cybersecurity strategies presents a promising pathway toward safeguarding critical water infrastructure against increasingly sophisticated cyber threats. Despite the technical, socio-economic, and data-related challenges, the potential of these technologies to transform cybersecurity practices in the water sector is significant. In both Africa and the U.S., embracing AI and ML can enhance the detection,

prediction, and mitigation of cyber threats, ensuring the reliability and safety of water services. Future directions in research and technology development, alongside strategies to overcome existing barriers, will be crucial in realizing the full potential of AI and ML in water cybersecurity. The journey toward secure, AI-enhanced water systems requires concerted effort, innovation, and collaboration, underpinned by a commitment to ethical principles and the equitable distribution of benefits across all communities.

References

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics, 11*(2), 198.

Adedeji, K. B., Ponnle, A. A., Abu-Mahfouz, A. M., & Kurien, A. M. (2022). Towards digitalization of water supply systems for sustainable smart city development—Water 4.0. *Applied Sciences, 12*(18), 9174.

Aivazidou, E., Banias, G., Lampridi, M., Vasileiadis, G., Anagnostis, A., Papageorgiou, E., & Bochtis, D. (2021). Smart technologies for sustainable water management: An urban analysis. *Sustainability, 13*(24), 13940.

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks, 165*, 106946.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review, 54*(5), 3849-3886.

Carter, D. (2020). Regulation and ethics in artificial intelligence and machine learning technologies: Where are we now? Who is responsible? Can the information professional play a role? *Business Information Review, 37*(2), 60-68.

Cosgrove, W. J., & Loucks, D. P. (2015). Water management: Current and future challenges and research directions. *Water Resources Research, 51*(6), 4823-4839.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580.

ElBaih, M. (2023). The role of privacy regulations in ai development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI). *Available at SSRN 4589207*.

Fagnan, K., Nashed, Y., Perdue, G., Ratner, D., Shankar, A., & Yoo, S. (2019). *Data and models: a framework for advancing ai in science*. Retrieved from

George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. *Partners Universal International Innovation Journal, 1*(4), 155-172.

Gorment, N. Z., Selamat, A., Cheng, L. K., & Krejcar, O. (2023). Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges and Future Directions. *IEEE Access*.

Harshadeep, N. R., & Young, W. (2020). Disruptive technologies for improving water security in large river basins. *Water, 12*(10), 2783.

Hartmann, K., & Steup, C. (2020). *Hacking the AI-the next generation of hijacked systems.* Paper presented at the 2020 12th International Conference on Cyber Conflict (CyCon).

Hassani, H., Silva, E. S., Unger, S., TajMazinani, M., & Mac Feely, S. (2020). Artificial intelligence (AI) or intelligence augmentation (IA): what is the future? *AI, 1*(2), 8.

Kabanda, G. (2022). The ODL African Continental Education Strategy: Anchoring AI/Machine Learning on the African Technological Innovation and Investment Table. *West African Journal of Open and Flexible Learning, 10*(2), 33-96.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR), 53*(1), 1-34.

Leflaive, X., Witmer, M., Martin-Hurtado, R., Bakker, M., Kram, T., Bouwman, L., . . . Kim, K. (2012). Water.

Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*: John Wiley & Sons.

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy.

Niemczynowicz, J. (1999). Urban hydrology and water management–present and future challenges. *Urban water, 1*(1), 1-14.

Packin, N. G., & Lev-Aretz, Y. (2018). Learning algorithms and discrimination. In *Research handbook on the law of artificial intelligence* (pp. 88-113): Edward Elgar Publishing.

Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. *ACM Computing Surveys (CSUR), 54*(5), 1-36.

Sambasivan, N., Kapania, S., Highfill, H., Akrong, D., Paritosh, P., & Aroyo, L. M. (2021). *"Everyone wants to do the model work, not the data work": Data Cascades in High-Stakes AI.* Paper presented at the proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.

Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science, 10*(6), 1473-1498.

Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentacion Cientifica, 15*(4), 42-66.

Shapira, N., Ayalon, O., Ostfeld, A., Farber, Y., & Housh, M. (2021). Cybersecurity in water sector: Stakeholders perspective. *Journal of Water Resources Planning and Management, 147*(8), 05021008.

Sommer, P., & Brown, I. (2011). Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011), 3*.

Tagert, A. C. (2010). *Cybersecurity challenges in developing nations.* Carnegie Mellon University,

Tschider, C. A. (2018). Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age.

Vähäkainu, P., & Lehto, M. (2022). Use of Artificial Intelligence in a Cybersecurity Environment. In *Artificial Intelligence and Cybersecurity: Theory and Applications* (pp. 3-27): Springer.

Wong, A. (2021). *Ethics and regulation of artificial intelligence.* Paper presented at the Artificial Intelligence for Knowledge Management: 8th IFIP WG 12.6 International Workshop,

AI4KM 2021, Held at IJCAI 2020, Yokohama, Japan, January 7–8, 2021, Revised Selected Papers 8.

Zehnder, A. J., Yang, H., & Schertenleib, R. (2003). Water issues: the need for action at different levels. *Aquatic Sciences, 65*, 1-20.