International Journal of Frontiers in
Engineering and Technology Research
Journal homepage: https://frontiersrj.com/journals/ijfetr/
ISSN: 2783-0497 (Online)

(REVIEW ARTICLE)

Check for updates

Theoretical perspectives on cybersecurity challenges in critical water infrastructure: Insights from Africa and the United States

Fatai Adeshina Adelani [1,*], Tosin Michael Olatunde [2] and Johnson Sunday Oliha [3]

[1] *Lagos Water Corporation, Lagos, Nigeria.*
[2] *Department of Electrical Power and Energy Systems (with Advanced Practice), Nigeria.*
[3] *Independent Researcher, Lagos, Nigeria.*

International Journal of Frontiers in Engineering and Technology Research, 2024, 06(02), 001–007

Publication history: Received on 18 February 2024; revised on 28 March 2024; accepted on 30 March 2024

Article DOI: https://doi.org/10.53294/ijfetr.2024.6.2.0029

Abstract

This review paper examines the theoretical perspectives on cybersecurity challenges facing critical water infrastructure, with a focus on comparative insights from Africa and the United States. By exploring foundational theories of risk management, resilience, and deterrence, the paper delineates how these concepts are applied and adapted to address the cybersecurity needs of critical water systems within the distinct contexts of the two regions. The analysis identifies common challenges such as malware attacks, system vulnerabilities, human factors, and how regional differences influence technological infrastructure, regulatory environments, and cyber threat landscapes. Through a comparative analysis, the paper highlights lessons learned and best practices from both regions, emphasizing the importance of capacity building, comprehensive risk management, and the role of public-private partnerships. The paper concludes with a call for future research to develop adaptable theoretical models that address different regions' unique cybersecurity challenges, underlining theoretical understanding's critical role in enhancing the global resilience of critical water infrastructure against cyber threats.

Keywords: Cybersecurity Challenges; Critical Water Infrastructure; Theoretical Perspectives; Risk Management; Resilience Theory

1. Introduction

The importance of cybersecurity in safeguarding critical water infrastructure cannot be overstated in today's interconnected and digitally dependent world. Water systems, essential for life, economic development, and public health, are increasingly reliant on digital technologies for their operation and management (Boyle et al., 2022; Mondejar et al., 2021). This reliance, however, exposes them to cyber threats that could compromise their functionality, safety, and reliability. The global landscape of these threats varies significantly, with each region facing unique challenges and vulnerabilities. In Africa, the combination of rapidly advancing technology adoption, alongside often underdeveloped cybersecurity frameworks, presents a distinct set of challenges (Tagert, 2010). Conversely, while there is a more mature cybersecurity infrastructure in the United States, the complexity and scale of water systems, alongside sophisticated and highly motivated threat actors, create a different set of vulnerabilities (Glenn, Sterbentz, & Wright, 2016; Panguluri, Nelson, & Wyman, 2017). The juxtaposition of these two contexts provides a rich backdrop for exploring theoretical perspectives on cybersecurity challenges in critical water infrastructure, offering insights into universal and locale-specific issues.

Critical water infrastructure systems are a foundational pillar for societies, ensuring the delivery of clean water and the safe treatment of wastewater. However, these systems are increasingly targeted by cyber threats, ranging from

* Corresponding author: Fatai Adeshina Adelani

ransomware attacks that lockout operational control to sophisticated espionage that seeks to steal sensitive data or manipulate water treatment processes (Delanka-Pedige, Munasinghe-Arachchige, Abeysiriwardana-Arachchige, & Nirmalakhandan, 2021; Pokhrel, Chhipi-Shrestha, Hewage, & Sadiq, 2022). The repercussions of such attacks can be catastrophic, leading to potential water shortages, health crises, or even environmental disasters. The cybersecurity challenges faced by critical water infrastructure are multifaceted, involving technological, organizational, and policy-related dimensions. Addressing these challenges is not merely a technical endeavour but requires a comprehensive understanding that integrates theoretical insights from cybersecurity, critical infrastructure protection, and public policy. This review paper aims to contribute to this understanding by exploring the theoretical underpinnings of cybersecurity challenges in critical water infrastructure, with a specific focus on the contexts of Africa and the United States (Givens, Busch, & Bersin, 2018; Vaseashta, Susmann, & Braman, 2014).

This review paper aims to synthesize theoretical perspectives on the cybersecurity challenges faced by critical water infrastructure, providing insights that are relevant both globally and within the specific contexts of Africa and the United States. This paper intends to bridge the gap between theory and practice by elucidating the conceptual frameworks that underpin the cybersecurity challenges and the strategies to address them. By doing so, it seeks to contribute to a deeper understanding of the complexities and nuances involved in protecting critical water infrastructure from cyber threats.

2. Theoretical Frameworks

2.1. Overview of Cybersecurity Theories

The domain of cybersecurity encompasses a broad range of theories that inform the understanding, management, and mitigation of cyber threats. Risk management, resilience, and deterrence theories are three foundational theories relevant to cybersecurity. Each offers unique insights into how cyber threats can be approached and managed.

Risk Management Theory: This theory focuses on identifying, assessing, and prioritizing risks, followed by the coordinated application of resources to minimize, control, or otherwise cope with the impact of undesirable events. In the context of cybersecurity, it emphasizes the importance of continuous risk assessment processes, the development of risk mitigation strategies, and the allocation of resources to protect against cyber threats effectively (Aven & Renn, 2010; Fan & Stevenson, 2018).

Resilience Theory: Resilience theory, rooted in systems theory, emphasizes the ability of a system to withstand disruptions and to recover quickly from them. In cybersecurity, resilience goes beyond mere prevention, incorporating the capacity to detect threats, respond efficiently to incidents, and recover systems to their normal operational status. This theory underscores the importance of adaptability and learning in the face of evolving cyber threats (Pisano, 2012; Ukpoju et al. 2023).

Deterrence Theory: Originally derived from military strategy, deterrence theory in cybersecurity focuses on preventing attacks through the threat of retaliation or the imposition of costs on the attacker. It involves creating a perceived level of risk and consequence for attackers, aiming to make the cost of an attack outweigh the benefits. While its application in cyberspace is complex due to issues like attribution and the asymmetry of cyber conflict, deterrence remains a strategic consideration in national cybersecurity policies (Linkov & Trump, 2019; Pisano, 2012).

2.2. Application to Critical Infrastructure

The application of these theories to critical water infrastructure requires a nuanced understanding of the sector's unique vulnerabilities and threat landscape.

Risk Management in Water Infrastructure: Applying risk management theory to water infrastructure involves conducting vulnerability assessments to identify potential cybersecurity gaps, threat modelling to understand and anticipate types of cyber attacks, and developing mitigation strategies tailored to the protection of water systems. This includes safeguarding control systems, ensuring data integrity for water quality monitoring, and protecting communication networks (Kure & Islam, 2019; Kure, Islam, & Razzaque, 2018; Ukpoju et al. 2024).

Building Resilience in Water Systems: Resilience theory emphasizes the need for water systems to maintain operational capabilities even when under cyber attack. This involves implementing robust detection systems for early warning, developing incident response plans that can be rapidly enacted, and having recovery strategies in place to restore services. Resilience in water infrastructure also means fostering a culture of continuous improvement and learning from past incidents to better prepare for future threats (Carlson et al., 2012; Adegbite et al. 2023).

Deterrence and Water Infrastructure: While deterrence theory may be more challenging to apply directly to the protection of water infrastructure, it highlights the importance of legal and regulatory frameworks that can penalize cybercriminals and state actors. In the context of national security, it also underscores the role of international cooperation and norms in cyberspace to deter attacks on critical infrastructure.

2.3. Comparative Analysis

The application and relevance of these theoretical frameworks can vary significantly between Africa and the United States, reflecting differences in technological infrastructure, regulatory environments, and threat landscapes.

In Africa, where cybersecurity frameworks and critical infrastructure protection may still be developing, the focus might be more on risk management and resilience building. This includes efforts to enhance the capacity for threat detection, incident response, and system recovery, often within limited resources and technical capabilities (Dalton, van Vuuren, & Westcott, 2017; Malatji, Marnewick, & Von Solms, 2022).

With the more mature cybersecurity infrastructure in the United States, all three theories are actively applied but significantly emphasize deterrence, especially at the national and international levels. The U.S. also invests heavily in resilience and advanced risk management practices, leveraging sophisticated technologies and frameworks to protect its water systems (Adekanmbi et al., 2024; Oladipo, Okoye, Elufioye, Falaiye, & Nwankwo, 2024).

These differences underscore the importance of context in applying theoretical frameworks to cybersecurity challenges in critical water infrastructure. While the core principles of risk management, resilience, and deterrence are universally relevant, their specific applications and effectiveness can vary widely depending on local conditions, resources, and capabilities.

3. Cybersecurity Challenges in Critical Water Infrastructure

3.1. Common Challenges

Critical water infrastructure globally faces many cybersecurity challenges that threaten their operational integrity, safety, and reliability. These challenges can be broadly categorized into issues related to malware attacks, system vulnerabilities, and human factors, each presenting unique difficulties in safeguarding water systems.

Malware, including ransomware, spyware, and viruses, poses a significant threat to critical water infrastructure. These malicious software programs can be designed to infiltrate, disrupt, or damage computer systems that control water treatment and distribution processes. For instance, ransomware attacks can lock out operational controls, demanding payment to restore access, thereby jeopardizing water safety and availability (Ibarra, Butt, Do, Jahankhani, & Jamal, 2019; Riggs et al., 2023).

Water infrastructure relies on complex information and operational technology systems, which inherently come with vulnerabilities. These can include outdated software, unpatched systems, or poorly configured networks, making them susceptible to cyber intrusions. Attackers can exploit these weaknesses to gain unauthorized access, steal sensitive information, or manipulate system operations. Human error remains one of the most significant cybersecurity vulnerabilities (Omar, 2016; Adefemi et al. 2023). This can include anything from the use of weak passwords, falling prey to phishing attacks, or improper handling of sensitive information. Insufficient training and awareness among staff about cybersecurity best practices can exacerbate these issues, increasing the risk of successful cyber attacks (Adewusi et al., 2024; Dada et al., 2024; Di Pietro et al., 2021).

3.2. Regional Differences

The impact and nature of these cybersecurity challenges can vary markedly between regions such as Africa and the United States, influenced by differences in technological infrastructure, regulatory environments, and the cyber threat landscape.

In many parts of Africa, the technological infrastructure for water systems may not be as advanced or interconnected as in the United States. This can limit the scope and complexity of cyber attacks but also means that systems may lack sophisticated cybersecurity protections. Conversely, the U.S.'s highly digitized and interconnected infrastructure offers more points of entry for cyber attackers, necessitating a more robust and complex cybersecurity framework (Johnson, 2012).

The regulatory landscape for cybersecurity in critical infrastructure also differs significantly. In the United States, there are stringent regulations and standards (such as those set by the Environmental Protection Agency and the Department of Homeland Security) that mandate cybersecurity measures for water systems. In contrast, African countries may have varying levels of cybersecurity regulation for critical infrastructure, with some regions still in the process of developing and implementing comprehensive cybersecurity policies. This variation can affect the prioritization of cybersecurity measures and the allocation of resources for their implementation (Cole et al., 2008; Ellefsen, 2014).

The types of cyber threats and the actors behind them can also differ. In the U.S., critical infrastructure may be targeted by sophisticated state-sponsored actors or highly skilled cybercriminals, motivated by espionage, political objectives, or financial gain. In Africa, while similar threats exist, there may also be a higher prevalence of opportunistic attacks exploiting basic vulnerabilities due to some areas' nascent stage of cybersecurity defenses (Geers, 2009; Lewis, 2019; Odunaiya, Nwankwo, Okoye, & Scholastica, 2024).

These regional differences highlight the need for tailored approaches to cybersecurity in critical water infrastructure. In Africa, efforts might focus on building cybersecurity capacity, improving regulatory frameworks, and raising awareness. In the United States, the emphasis may be on enhancing resilience against sophisticated attacks, ensuring compliance with regulatory standards, and fostering innovation in cybersecurity technologies and practices. Understanding these nuances is crucial for developing effective strategies to mitigate cyber risks and protect water systems (Dupont, 2019; Safitra, Lubis, & Fakhrurroja, 2023).

3.3. Comparative Analysis

3.3.1. Theoretical Perspectives Comparison

The application and adaptation of theoretical perspectives on cybersecurity challenges in critical water infrastructure exhibit notable differences between Africa and the United States, reflecting their unique technological, regulatory, and threat landscapes.

In Africa, the application of risk management theory often focuses on establishing foundational cybersecurity practices and identifying the most pressing vulnerabilities within limited resource settings. In contrast, the United States applies risk management more nuanced and sophisticatedly, leveraging advanced technologies and analytics to assess and mitigate risks. The U.S. approach includes a comprehensive assessment of cyber threats and the implementation of layered security strategies.

The emphasis in Africa is on developing resilience through capacity building and infrastructure hardening, often with the support of international partners. The goal is to enhance the ability of water systems to maintain operations despite limited cybersecurity capabilities. In the U.S., resilience theory is applied through advanced cyber incident response exercises, investment in redundant systems, and fostering a robust cybersecurity culture within organizations.

The concept of deterrence is more prominently featured in the U.S. context, where national and international policies and actions, including cyber offense capabilities, are utilized to deter cyber threats against critical infrastructure. In Africa, the focus is more on developing legal and regulatory frameworks that can serve as a basis for deterrence, with an emphasis on collaboration and information sharing to strengthen collective security posture.

3.4. Lessons Learned and Best Practices

3.4.1. Lessons Learned

Capacity Building is Crucial: Africa's focus on capacity building highlights the importance of developing internal expertise and infrastructure resilience as foundational elements of cybersecurity.

Comprehensive Risk Management: The U.S. demonstrates the effectiveness of a comprehensive and proactive risk management approach, utilizing advanced technologies and methodologies to anticipate and mitigate cyber threats.

Best Practices

Developing and Implementing Standards: The adoption of cybersecurity standards and frameworks, as seen in the U.S., can guide critical water infrastructure protection efforts and should be adapted and implemented according to regional contexts.

Public-Private Partnerships: Both regions benefit from collaboration between the government and the private sector, sharing knowledge, resources, and intelligence to enhance cybersecurity.

Continuous Awareness and Training: Addressing human factors through continuous awareness and training programs is universally recognized as a critical component of a cybersecurity strategy.

4. Conclusion

The comparative analysis of theoretical perspectives on cybersecurity challenges in critical water infrastructure between Africa and the United States reveals divergent approaches and priorities. While Africa focuses on capacity building and foundational cybersecurity practices within a context of rapid technological adoption and varied regulatory environments, the United States leverages advanced technologies and sophisticated risk management strategies to protect its more complex and interconnected water systems against sophisticated threats.

Future research should focus on developing theoretical models that are adaptable to the unique challenges and contexts of different regions. This includes models that can guide the integration of cybersecurity practices into the early stages of infrastructure development, strategies for resource optimization in settings with limited cybersecurity capabilities, and frameworks for international cooperation and support.

A theoretical understanding of cybersecurity challenges is crucial for enhancing the resilience of critical water infrastructure globally. By learning from the experiences of different regions, adopting best practices, and continuously adapting to the evolving cyber threat landscape, nations can better protect their water systems against cyber threats. The insights gained from such analyses underscore the importance of a coordinated, informed, and proactive approach to cybersecurity in critical infrastructure sectors.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adefemi, A., Ukpoju, E.A., Adekoya, O., Abatan, O., Adegbite, A.O. 2023. Artificial intelligence in environmental health and public safety: A comprehensive review of USA strategies. World Journal of Advanced Research and Reviews 20 (3), 1420-1434

[2] Adegbite, AO., Adefemi, A., Ukpoju, EA. Abatan, A., Adekoya, O., Obaedo. BO. 2023. Innovations In Project Management: Trends And Best Practices. Engineering Science & Technology Journal 4 (6), 509-532

[3] Adekanmbi, A. O., Ani, E. C., Abatan, A., Izuka, U., Ninduwezuor-Ehiobu, N., & Obaigbena, A. (2024). Assessing the environmental and health impacts of plastic production and recycling.

[4] 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.

[5] Aven, T., & Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications* (Vol. 16): Springer Science & Business Media.

[6] Boyle, C., Ryan, G., Bhandari, P., Law, K. M., Gong, J., & Creighton, D. (2022). Digital transformation in water organizations. *Journal of Water Resources Planning and Management, 148*(7), 03122001.

[7] Carlson, J., Haffenden, R., Bassett, G., Buehring, W., Collins III, M., Folga, S., . . . Whitfield, R. (2012). *Resilience: Theory and Application*. Retrieved from

[8] Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. (2008). Cybersecurity in africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

[9] Dada, M. A., Majemite, M. T., Obaigbena, A., Daraojimba, O. H., Oliha, J. S., & Nwokediegwu, Z. Q. S. (2024). Review of smart water management: IoT and AI in water and wastewater treatment. *World Journal of Advanced Research and Reviews, 21*(1), 1373-1382.

[10] Dalton, W., van Vuuren, J. J., & Westcott, J. (2017). *Building cybersecurity resilience in Africa.* Paper presented at the 12th International Conference on Cyber Warfare and Security.

[11] Delanka-Pedige, H., Munasinghe-Arachchige, S., Abeysiriwardana-Arachchige, I., & Nirmalakhandan, N. (2021). Wastewater infrastructure for sustainable cities: assessment based on UN sustainable development goals (SDGs). *International Journal of Sustainable Development & World Ecology, 28*(3), 203-209.

[12] Di Pietro, R., Raponi, S., Caprolu, M., Cresci, S., Di Pietro, R., Raponi, S., . . . Cresci, S. (2021). Critical infrastructure. *New Dimensions of Information Warfare*, 157-196.

[13] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity, 5*(1), tyz013.

[14] Ellefsen, I. (2014). *The development of a cyber security policy in developing regions and the impact on stakeholders.* Paper presented at the 2014 IST-Africa Conference Proceedings.

[15] Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International journal of physical distribution & logistics management, 48*(3), 205-230.

[16] Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective, 18*(1), 1-7.

[17] Givens, A. D., Busch, N. E., & Bersin, A. D. (2018). Going global: The international dimensions of US homeland security policy. *Journal of Strategic Security, 11*(3), 1-34.

[18] Glenn, C., Sterbentz, D., & Wright, A. (2016). *Cyber threat and vulnerability analysis of the US electric sector*. Retrieved from

[19] Ibarra, J., Butt, U. J., Do, A., Jahankhani, H., & Jamal, A. (2019). *Ransomware impact to SCADA systems and its scope to critical infrastructure.* Paper presented at the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3).

[20] Johnson, R. L. (2012). *An analysis of IT governance practices in the federal government: Protecting US critical infrastructure from cyber terrorist attacks.* Walden University,

[21] Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications, 4*(4), 332-340.

[22] Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 898.

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

[24] Linkov, I., & Trump, B. D. (2019). *The science and practice of resilience*: Springer.

[25] Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security, 30*(2), 255-279.

[26] Mondejar, M. E., Avtar, R., Diaz, H. L. B., Dubey, R. K., Esteban, J., Gómez-Morales, A., . . . Prasad, K. A. (2021). Digitalization to achieve sustainable development goals: Steps towards a Smart Green Planet. *Science of The Total Environment, 794*, 148539.

[27] Odunaiya, O. G., Nwankwo, E. E., Okoye, C. C., & Scholastica, U. C. (2024). Behavioral economics and consumer protection in the US: A review: Understanding how psychological factors shape consumer policies and regulations. *International Journal of Science and Research Archive, 11*(1), 2048-2062.

[28] Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape.

[29] Ukpoju, E.A. Abatan, A. Adekoya, O. Obaedo, BO., Balogun. OD. 2023. Recycling And Upcycling In The Electro-Mechanical Domain: A Review Of Current Practices. Engineering Science & Technology Journal 4 (6), 489-508

[30] Ukpoju, EA., A Adefemi, AO Adegbite, OD Balogun, BO Obaedo, A Abatan. 2024. A review of sustainable environmental practices and their impact on US economic sustainability. World Journal of Advanced Research and Reviews, 2024, 21(01), 384–392

[31] Omar, S. (2016). *Information system security threats and vulnerabilities: evaluating the human factor in data protection.*

[32] Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Creating a cyber security culture for your water/waste water utility. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, 133-159.

[33] Pisano, U. (2012). Resilience and Sustainable Development: Theory of resilience, systems thinking. *European Sustainable Development Network (ESDN), 26*, 50.

[34] Pokhrel, S. R., Chhipi-Shrestha, G., Hewage, K., & Sadiq, R. (2022). Sustainable, resilient, and reliable urban water systems: making the case for a "one water" approach. *Environmental Reviews, 30*(1), 10-29.

[35] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., . . . Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors, 23*(8), 4060.

[36] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369.

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

[38] Vaseashta, A., Susmann, P., & Braman, E. (2014). *Cyber security and resiliency policy framework*: IOS press.