BILINGUAL PUBLISHING GROUP

Journal of Environmental & Earth Sciences

https://journals.bilpubgroup.com/index.php/jees

ARTICLE

Migration Perspectives of Water Sector Cybersecurity

Attila Mate Kovacs*

Doctoral School on Safety and Security Sciences, Óbuda University, 1034 Budapest, Hungary

ABSTRACT

The use of digital technologies in the water sector has proved revolutionary in water management but also opens up critical infrastructure to cyber threats, with extreme risks to public health, economic instability, and even forced migration. Therefore, this paper will address how cybersecurity vulnerabilities intersect with migration through case studies from various regions like Norway, Israel, and the United States. By looking into the above incidents, the research speaks of the cascading effects of cyber-attacks on water systems and the urgency for all-encompassing policy frameworks addressing cyber and migration. On a similar note, it points out that the intensification of cyber threats is partly due to the technological innovation era and, on the other hand, the weaknesses in cybersecurity postures. It further highlights how these emerging technologies—specifically artificial intelligence and blockchain—can improve resiliency and provide practical recommendations for implementation even in resource-constrained settings. Through this multidisciplinary approach, the research contributes to a better understanding of protecting communities and critical infrastructure from the growing threat of cyber-induced displacement.

Keywords: Cybersecurity; Water sector; Forced migration; Critical infrastructure; Digital resilience; SCADA systems; Migration policy; Technological solutions; Ransomware attacks; Public health

*CORRESPONDING AUTHOR:

Attila Mate Kovacs, Doctoral School on Safety and Security Sciences, Óbuda University, 1034 Budapest, Hungary; Email: attilamate.kovacs@gmail.com

ARTICLE INFO

Received: 9 August 2024 | Revised: 6 September 2024 | Accepted: 13 September 2024 | Published Online: 8 October 2024
DOI: https://doi.org/10.30564/jees.v6i3.7020

CITATION

Kovacs, A.M., 2024. Migration Perspectives of Water Sector Cybersecurity. Journal of Environmental & Earth Sciences. 6(3): 217-232. DOI: https://doi.org/10.30564/jees.v6i3.7020

1. Introduction

1.1 Background

Integrating digital technologies into the water sector allows for better management and provision of water resources. Driven by innovation in information technology, this change completely revolutionizes how daily operations within water utilities are carried out, making the process more effective, reliable, and scalable. Until recently, water management was a manual process, making it time-consuming and labor-intensive. But a lot of necessary progress has been made with digitalization, which has incorporated new automation technologies such as SCADA, GIS, and metering systems.

For instance, SCADA systems enable operators to control and oversee water treatment and distribution in real time[1]. Such systems can be helpful to operators in preventing problems from arising or having the problems solved or solutions implemented before a disruption occurs. GIS technology helps in the geographical mapping of water networks and aids in effective planning and responses. This development of smart meters has gone a long way to change the affected water usage monitoring by offering specific data used to an area as used in demand management and leakage detection.

Adoption levels are unique, with higher adoption in developed countries due to better infrastructure and investment capacities. Advanced developed countries such as the United States, Germany, and Japan adopt intelligent water management systems to improve performance and reduce water losses. On the other hand, financial constraints, poor infrastructure, and a lack of technical acumen are some factors that put a leash on the digitization of the water sector in developing countries[2].

This paper builds upon the state of knowledge at the intersection of cybersecurity and migration by comprehensively examining how cyber incidents in the water sector can force migration. Unlike previous research, which has focused mainly on single cases, this work integrates several case studies across various regions, thus offering a more general perspective. Moreover, the study bridges the literature gap concerning practical considerations in melding cybersecurity and migration policies, specifically for resource-constrained regions.

1.2 Statement of the problem

Although it is perceived that digitizing the water sector has several benefits, this ushering in digital implementation spirals up the level of cyber threats. Intrusion into water facilities might lead to the unavailability of potable water and contamination, ultimately posing a risk to life and health. This impacts the short term by immediately halting water system operations and, in the long term, by disrupting communities[3].

For example, in 2021, a ransomware attack targeted Florida's Oldsmar water treatment facility. An unauthorized user accessed the plant's control system remotely and attempted to raise the levels of sodium hydroxide significantly. Although the attack stopped in time and no harm was done, it raised concerns about safety and cyber resilience for essential water infrastructures.

Public health crises contaminating the water supply can force mass migrations of communities to safer environments... Industries and agriculture depend on these services, which disrupts their operations and leads to instability in the economy. This follow-up cascading effect indicates the need for urgent comprehensive prevention regarding cybersecurity vulnerabilities to avoid forced migration and assure community resilience.

1.3 Scope

The study will involve geographically different parts, and it is only in this way that it will be possible to better understand cybersecurity incidents in the water sector. Specific case studies will be drawn from regions such as North America, Europe, the Middle East, and Africa, offering a broad perspective on the impacts and responses to cyber threats in different contexts.

In North America, concerns will be directed toward incidents like the Oldsmar water treatment plant attack and the Lansing Board of Water & Light phishing attack. These cases emphasized the vulnerabilities of advanced water systems and the need for solid cybersecurity implementation. While in Europe, the focus will be shifted to the Ryuk ransomware attack on Volue in Norway and how such incidents can disrupt water services within developed countries.

The most interesting region is the Middle East, where highly complex geopolitical attributes and water scarcity issues make it peculiarly attractive. This paper will attempt to analyze how insecurity may result from a series of cyber incidents that hit the water system in Israel over the year 2020. Regarding Africa, an analysis is presented regarding the vulnerabilities of water infrastructure in cases of chronic scarcity, followed by consequences for migration patterns.

1.4 Objectives

General objective

- To explore the relationship between cybersecurity vulnerabilities in the water sector and their implications for human migration.

Specific objectives

1. To review and document notable cybersecurity incidents in the water sector.
2. To analyze the impact of these incidents on public health, economic stability, and quality of life.
3. To investigate how these impacts drive migration.
4. To propose policy recommendations for enhancing cybersecurity measures in the water sector and addressing migration issues related to cyber disruptions.

1.5 Study questions

1. What has the water sector faced the most significant cyber incidents in recent years?
2. How did these cyber incidences affect this region's public health, economic well-being, and quality of life?
3. How have the water services disruptions by cyberattacks affected human migration patterns?
4. What policy measures can be taken to improve cybersecurity in the water sector and prevent migration due to cyber disruptions?
5. How can cross-disciplinary collaboration among experts in cybersecurity and migration, along with policymakers, support enhancing the level of resilience in water infrastructures to manage migration effectively?

2. Literature review

2.1 Migration perspective

The growing reliance of the water sector on digital technologies has introduced severe weaknesses to cybersecurity in a manner that can permit interruptions of such an essential service. This will, in turn, have cascading impacts on public health, economic stability, and quality of life. For this reason, as living conditions deteriorate for communities with malfunctioning water systems, migration becomes a norm for many affected populations. This section now highlights some significant cybersecurity incidents within the water subsector and their effects on migration using specific case studies[4].

2.2 Notable cybersecurity incidents and their impact on migration

Ryuk ransomware attack on Volue, Norway, 2021

The Ryuk ransomware targeted the technology company serving public water systems in 2021. An attack that seriously affected approximately 200 public water systems and hindered them from their normal functioning weakened their service capacity to produce sound, potable water[5]. The ransomware encrypted critical data, brought the system down to a stop, and even terminated the treatment processes. The immediate effect of this act was an essential public health risk since the water quality could not be adequately handled. Given this, an incident like that demonstrated the vulnerabilities to cyberattacks that digital systems within the water sector show and highlighted the imperative need for vigorous cybersecurity measures.

The implications of the Ryuk ransomware attack went further than just the challenges experienced in restoring normal operations. Local people associated with this water relied on these systems and were exposed to potential health hazards, which heightened the sense of insecurity. Forced migration became probable as access to clean and safe water was unpredictable. Residents needed to factor in moving into the region with more reliable water infrastructure that will support both their daily lives and health and safety. This is a clear example of how cyber vulnerabilities in critical infrastructures can drive migrations, and it focuses on the urgency of combining cybersecurity with migration policies.

Credential misuse and outdated systems in San Francisco and Florida, USA, 2021

In 2021, cybersecurity incidents in the USA exposed glaring vulnerabilities in the water sector of San Francisco and Florida. Hackers used login information from former employees to gain unauthorized access to these water treatment plants[6]. These outdated, unsecured systems could provide an easy target for cybercriminals. These incidents revealed that updating security protocols for system access needed to be continuous and consistent—otherwise, there existed the potential for unauthorized access that could sabotage water infrastructure.

The implications of these breaches were much broader than the technical failures suffered. Public confidence in the safety and reliability of water services was severely undermined, creating an environment of uncertainty and fear. In such communities, the slightest possibility of contamination or break in service can drive the people to look for greener pastures elsewhere. These vulnerabilities were what was being exploited and showed the interplay between cybersecurity and migration – people moving to areas where they think the infrastructure is better or where cybersecurity measures are likely to be stronger. This, therefore, emphasizes the need for proactive cybersecurity strategies to prevent forced migration due to a breakdown in critical services.

Phishing attack on Lansing Board of Water & Light, Michigan, USA, 2016

In 2016, ransomware hit Lansing Board of Water & Light in Michigan. Taking critical systems offline and bringing the delivery of vital services to a standstill, in totality, paralyzes all utility functions[7]. The employees were duped into clicking malicious links that opened the network for cyber thugs, who encrypted vital data. The event has laid at the forefront the vulnerability factor as a human factor in cybersecurity and spoke of continuous training and awareness programs to minimize such risks.

The ransomware attack paralyzed the entire community, and the residents were exposed to probable contamination and supply disruption from the water service disruption. This public health and safety threat can affect how families will resettle in an area with better infrastructures that are much safer and more resilient. As demonstrated by the Lansing case, one critical indirect implication of cyber-attacks on critical infrastructures is their potential to strike at immigration. Therefore, full-proof cybersecurity for life-sustaining services in every community is required.

Ransomware attacks on Onslow Water and Sewer Authority, North Carolina, USA, 2018

In 2018, ransomware attacked the authority of Onslow Water and Sewer of North Carolina, USA, completely disrupting service delivery. Critical data of importance for water and sewer operations were encrypted, which meant these vital operations underperformed, with the authority failing to deliver the essential services as expected[8]. This high level of immediate response, toward which the operational difficulties were also relatively significant, included restoring affected systems and implementing contingency measures to ensure continued water supply.

These ransomware attacks had broader implications for community stability and security. Uncertainties and probable health risks associated with using an impaired water supply might drive the residents to shift their reliance on comparatively safer and dependable alternatives. With the community facing extended service outages, it became evident that quality of life must have been sorely impacted, and families possibly shifted to other places where the infrastructure is more robustly kept. The Onslow incident illustrates that strong cyber defenses for public utilities are needed to prevent forced migration in the water sector.

There was a series of cyber-attacks on the Israeli water systems. The cybersecurity incident happened in 2020 when the scope of the attack threatened to adjust the water quality, posing an immense risk to public health[9]. That was an attributed state-sponsored attempt to fiddle with chemicals in the water supply in a way that would have exposed tens of thousands to grave danger. These attacks brought to the fore the notion that cyberattacks were not supposed to be just an inconvenience but that they could deliberately introduce threats to public health by contaminating water supplies.

Immediate public health and safety threats have ripple effects that generate fear and panic. A group grappling with the issues of contaminated water supplies may also opt to move to another settlement, where such vulnerability risks in their infrastructure are secure and less prone to effects. The facts arising out of Israel make it very clear how serious migration is interwoven with cybersecurity in modern times: the unavailability of essential services forces people to migrate into other environments wherein they can protect themselves. This situation only confirms that critical infrastructure security must be enhanced to protect human life from being forcefully migrated.

Insider attack on sewage treatment plant (Maroochy, Australia, 2000)

In this case, the attacker released 265,000 gallons of raw sewage into those parks and rivers, which had severe environmental and public health repercussions. The access to the system they achieved was unauthorized, using vulnerable login information about a flaw in the software[10]. This is a pure insight into governmental levels of critical extreme measures that can prevent insider threats, including access controls, qualified staff, and monitoring critical systems.

The Maroochy incident had environmental implications because the contaminated water sources were opened into that area, threatening people's health. Long-term low living standards and accompanying health impacts would drive them to settle into other less dangerous habitats. This scenario highlights how insider threats pose critical service disruption and further build-up situations that eventually arouse migration pressure. This further insinuates that strict cybersecurity setups should be laid upon critical infrastructures to prevent such instances.

Cyberattack on an American Water Treatment Plant (Oldsmar, Florida, 2021)

The Oldsmar Water Treatment Plant in Florida experienced a remote breach in 2021 when an intruder attempted to poison the city's drinking water supply by raising the levels of sodium hydroxide to alarming heights. According to Greenberg[11], the attackers used remote access tools to manipulate how lye and other chemicals are added to the water supply. As such, the incident revealed just how vital critical infrastructure was in the face of such vulnerabilities, so strict cybersecurity protocols, periodic security audits, and elaborate training programs for all staff must be ensured to prevent unauthorized access or manipulations of the most critical water infrastructure.

The potential that the Oldsmar attack resulted in widespread harm set the stage for a weighty magnitude public health threat birthed into a local crisis of water supply safety. The residents may consider living in a city where this kind of event can happen again, risking people's lives, and these cities can shift from places with more reliable water infrastructures. This gives a perfect example of why good cybersecurity is paramount: to secure the services that come with the vital infrastructure and go ahead without fear of compromise since it can spiral into mass migrations. It further alludes to the need for lessons learned from various incidents along the path of progressive strengthening of resilience in water utilities against threats from inside and outside.

The case studies, as presented in **Table 1** below, clearly prove the devastating effects of cybersecurity incidents within the water sector on migration patterns and point out an urgent need for integrated policies on cybersecurity vulnerabilities and how the latter can drive migration.

3. Methodology

3.1 Exploring the link between migration patterns and cybersecurity

This chapter examines the links between cybersecurity vulnerabilities in the water sector and human migration. In other words, it focuses on cyber incidences as a migration force from risks to public health, economic instability, and decreased quality of life. To do this analytically and powerfully, this research uses case study methodology, selecting diverse regions and incidents so that the study will provide substantial insights into the interplay between cybersecurity and migration.

3.2 Selection of case studies

Case studies were chosen by applying a criterion-based approach; hence, the case study has to give some unique insight into the broader research questions. The criteria are derived from:

1. Geographical Diversity: Regions covered in the research study are from Africa, Asia, and the Middle East, an approach brought out to infer that cybersecurity threats are global and affect migration. This geographical diversity will set the ground for a comparative analysis of how different regions in the world, with various levels of infrastructure development and political stability, respond to water sector cybersecurity incidents.
2. Cyber Incident Severe Impact: Incidents that have impacted public health and the economic stability of countries or have caused significant migration. One such incident is the Ryuk ransomware incident in Nor-

Table 1. Table summary of the incidents and impact on migration.

Incident	Location	Year	Description	Impact on Migration
Ryuk Ransomware Attack on Volue	Norway	2021	Ryuk ransomware attack impacted nearly 200 public water systems, disrupting operations and compromising water quality.	Potential health hazards and uncertainty increased the risk of forced migration to areas with more reliable water infrastructure.
Credential Misuse and Outdated Systems	San Francisco and Florida, USA	2021	Hackers leveraged former employees' login information to target outdated systems, compromising water treatment facilities.	Public trust in water safety is compromised, potentially driving residents to relocate to areas with better cybersecurity measures.
Phishing Attack on Lansing Board of Water & Light	Michigan, USA	2016	Phishing attacks led to ransomware deployment, disrupting utility functions and halting essential services.	Public health and safety threats could prompt families to relocate to regions with more secure water infrastructure.
Ransomware Attacks on Onslow Water and Sewer Authority	North Carolina, USA	2018	Ransomware interfered with water and sewer operations, impeding the authority's ability to deliver critical services.	Prolonged service disruptions impacted quality of life, potentially leading to migration to areas with better-protected infrastructure.
Series of Attacks on Water Systems	Israel	2020	Cyberattacks aimed at altering water quality pose a significant public health risk.	Fear of contaminated water supplies could drive populations to seek safer environments with secure and resilient infrastructure.
Insider Attack on Sewage Treatment Plant	Maroochy, Australia	2000	Insiders leaked 265,000 gallons of raw sewage into area parks and rivers, causing significant environmental and public health consequences.	Environmental and health impacts led to deteriorated living conditions, compelling residents to seek safer environments.
Remote Access Attack on Water Treatment Plant	Oldsmar, Florida, USA	2021	Hacker attempted to poison the city's water supply by increasing sodium hydroxide levels to hazardous amounts.	Public health threats created a crisis of confidence in water safety, potentially driving residents to relocate to areas with secure water systems.

way, and another is the set of incidents targeting water systems in Israel.

3. Relevance to Migration: The chosen cases had to evidence a clear and unambiguously established link between cyber incidents and migration, either as direct forced migration due to public health crises or through indirect economic and social factors. This ensures that each case adds meaning to understanding the research questions.
4. Data Availability: Cases for which comprehensive reports were available were chosen. This ensured that the analysis would be based on something tangible, making the study more reproducible and credible. This criterion is fundamental to allowing for detailed incident analysis.

3.3 Methodological framework

The research is based on a multi-case study approach that allows a comprehensive study in different contexts. The methodological framework for this study encompasses the following:

1. Data Collection: The data were collected from diverse sources, including government reports, incident logs, and media reports, as well as secondary sources such as academic papers and expert analyses. This aspect of multisource data collection ensures that there is a holistic understanding of each of the cases.
2. Cybersecurity Incident Analysis: Elaborate on the cybersecurity incident in the two cases to explain the nature of the attack, the technologies involved, and the immediate impact on the water sector. Consider

the implications beyond the water sector for public health, economic stability, and migration.

3. Impact Assessment on Migration: The paper then assesses cybersecurity incidences' direct and indirect impacts on migration patterns. An assessment would further consider forced migration because of immediate public health threats, economic migration due to job loss, and social migration due to deteriorating living conditions.
4. Comparative Analysis: The selected case studies are compared to draw common themes and identify unique challenges in the different regions. This should allow for generalizable conclusions regarding the relationship between cybersecurity and migration.
5. Policy Implications and Recommendations: Finally, the step involves synthesizing the findings to develop policy recommendations that would alleviate the cybersecurity vulnerabilities in the water sector. The recommendations respond to the specific needs and challenges in the regions studied.

3.4 Case studies overview

Case study: Africa

In Africa, the intersection of cybersecurity vulnerabilities and migration is prominently observed. Kariuki et al.[12] explicate how serious cybersecurity threats on small-scale African migrant traders make them vulnerable. Usually, water infrastructure in several African countries is underdeveloped and protected insubstantially: cyberattacks result in strong disturbances of services to provide water. These attackers are not only health hazards but also leave local economies vulnerable. Hence, most people will be forced to move to cities and neighboring countries with better water provisions.

The level of weak cybersecurity in these areas makes them more prone to attacks. The minute the water systems are attacked, migration from the rural areas to the urban sector results immediately. Migration is a ripple effect of a cybersecurity attack in rural and urban settings. This will be especially devastating in rural communities with little or no option for water supply or recovery facilities. It also fuels the migration to urban areas, which are already stressed further by poor urban water infrastructure since cyber vulnerabilities exist in this sector.

Case study: Asia

An ever-increasing rate of urbanization and climate change in Asia has escalated the impact on the vulnerability of the water sector. These warnings have been taken up by Bhandari et al.[13], who further observe that increased reliance on digital technologies in water management is not without its demerits. Cyber incidents could devastate water supplies to urban areas with high population densities and cause health and economic disruption. The instability that results breeds migration as those affected seek safer zones in the countryside or elsewhere where it is perceived that such threats are at a minimal level.

This is an addition to the complexity of managing water security in Asia due to the resultant layering of the urban-rural migration, with the compounded effect being the rise of the cyber threat. This means that these so-called urbanized areas turn distressing when their water services are tampered with by cyber threats, consequently triggering reverse migration back to rural areas even when there are no possible amenities and economic opportunities. This makes it very critical that the robustness of urban water services is supported by robust cybersecurity to avoid such migrations and ensure that the urban growth experienced is sustainable and robust against cyber threats.

Integrated policy and mitigation

The impacts of migration due to cyber security vulnerabilities in the water sector require a policy that integrates responses in dealing with such challenges. Petersen and Wieltschnig[14] further argue that sound Cybersecurity measures should balance with technological innovation. In this regard, the policies have to firmly establish cyber-security concerns in policies on water management and migration at large so that weaknesses are fully taken care of. Building within such a policy provides an opportunity to reduce the risks of forced migration due to the enhanced resilience of essential water infrastructure.

Indeed, such policies would be welcomed if the proposed solutions are viable and would bridge this gap between cyber and migration. For that to happen, integrating forces by policymakers, cybersecurity specialists, migration scholars, and water management authorities in developing full-fledged strategies on these two fundamental aspects would be essential: securing water infrastructure from cyber threats and dealing with migration root causes. By so doing, this work will ensure comprehensiveness in policy measures toward service delivery in both technological and social dimensions concerning water security and migration.

Better security arrangements

Enhanced cooperation between cybersecurity researchers, migration experts, and policymakers emerges clearly. Mishra et al.[15] expound on interdisciplinary strategies when landscapes change associated with water security. Stakeholders would target integrated solutions to protect water services from cyber threats and reduce migration pressure from compromised infrastructures.

It involves interdisciplinary collaboration to harness several diverse views and competencies to solve a problem. Cybersecurity experts could explain the technical aspects of protecting water systems, and migration scholars could illuminate the social and economic imperatives driving migration. Such policymakers can incorporate such insights into their operational strategies to secure and make water sources resilient, reducing forced migration needs presented by cyber-induced water crises.

Technological solutions

In the water sector, advanced technological solutions are essential; otherwise, any cybersecurity vulnerability could have dire consequences. Technologies incorporating artificial intelligence and machine learning can analyze behaviors and patterns. Simultaneously, real-time detection of anomalies will enable immediate action on detected threats. Blockchain technology offers a decentralized and secure method for managing data transactions, ensuring that critical data remains tamper-proof and reducing the risk of unauthorized access[16]. Additionally, Internet of Things (IoT) devices continuously monitor water infrastructure components, allowing for automatic adjustments and responses to emerging threats, which helps maintain the integrity of essential services.

However, the cost of implementing these technological solutions is high, specialized technical expertise is required, and integrating such technologies with the existing systems is complex. Besides, with the evolution of tactics by cyber attackers, improvements and upgrades in security measures need to be made at regular intervals. Despite these challenges, investment and deployment of these technologies are critical to making water infrastructure more resilient, protecting communities, and reducing the risk of cybersecurity incidents that may otherwise force people to migrate.

Resilience through technological advancements

Investments in state-of-the-art cybersecurity technologies toward a resilient water infrastructure. Bhandari et al.[13] confirm that innovations must run every time in their cyber-physical-human systems to fill present gaps and take security to another level. Assurance for using current cybersecurity mechanisms could prevent the attack, maintain water service delivery, and keep any forced migration at a minimum. These advances will, of course, have to be supplemented with regular in-service capacity building and training programs so that local bodies and communities are armed with the right skills that would make them capable of delivering on cyber defense.

However, such advanced technologies will thus safeguard water systems from present and future threats. The resilient infrastructure that can withstand cyberattacks will ensure communities have water access and lower migration probabilities. Equally important is regular training and capacity building for the local authorities to keep these systems updated and to ensure they can deal with potential cyber incidents. It is a proactive approach since it creates stable, secure environments and mitigating factors causing migrations.

Future research and policy development

Future research must consider the relationship between cybersecurity vulnerabilities in water services and migration. Intensive policy creation and well-developed case studies most effectively incorporate water security's technical and human dimensions. Petersen and Wieltschnig[14] argue that there exists a need to realize a balanced scenario between innovation and vulnerability management. Beyond that, future research may link such approaches at the nexus between critical infrastructure protection strategies and cybersecurity-human protection measures for mitigating cyber-attack incidents that impact human migration. This can improve resilience in infrastructures and how communities concerned are to inform policy development toward mitigated issues that might re-emerge from cyber incidents.

Subsequent findings suggest designing best practices combining migration management strategies with cybersecurity measures. Effective and sustainable solutions should be designed according to local needs by first carrying out baseline studies to fully comprehend the vulnerabilities that characterize a particular region. Through collaborative efforts with policymakers and researchers, the outputs should yield actionable policy matters for enhancing water security, protecting public health, and preventing forced migration from cyber threats. The two work toward making it hard for their communities to alter cybersecurity threats to their water systems.

4. Discussion

Implications for Policy and Practice:

The synergy between the cybersecurity and migration policy is vital to ensure that infrastructure vulnerabilities, among the causes of forced migration, are effectively addressed. Since cyber threats tend to worsen over time, their implications for delivering essential services and infrastructures have rendered urgent, among other things, an integrated policy framework that can regulate and reveal the associated risks effectively and prevent their possible consequences on population groups while increasing resilience to these risks.

4.1 The interconnectedness of cybersecurity and migration policies

The underlying causes of migration, especially cyber-attacks targeting critical infrastructures [4] like water systems, call for better coherence between cybersecurity and migration policies. Cyber-attacks could cause catastrophic failures in service delivery, induce public health emergencies, and most likely cause economic dislocation that catalyzes migration. Thus, integrating cybersecurity with migration policies can help develop more resilient infrastructures and aid in community protection from cascading incidents within the cyber domain.

4.2 Integration in practice

Even though cybersecurity is a relatively new concept, it has already been integrated with migration policy within the frameworks of some past initiatives. For instance, after cyber-attacks on Israeli water systems in 2020, the government sought to harden critical infrastructure by integrating cybersecurity with already integrated migration policies [17]. This involved close collaboration between cybersecurity experts, migration scholars, and policymakers to develop sustainable frameworks that prevent service disruptions and reduce the need for forced migration.

For instance, Estonia is one of the governments that has been very proactive in digital resilience and cybersecurity. The measures the Estonian government has adopted have been critical for safeguarding fundamental infrastructure, including water systems, through applying advanced cybersecurity measures [18]. The government of Estonia has also aimed at synchronizing these efforts with policies that would not allow migration due to the instability of the economic sector, as happened when computers attacked Estonia's key services.

4.3 Challenges in integration:

Thus, the attempts to link cybersecurity and migration policies seem pretty straightforward, though this has yet to happen. The lack of strategic policy guidelines also makes it challenging to nurture the integration of these two domains. For instance, while cybersecurity strategies involve guarding infrastructure, migration policies concern themselves with antecedents that spur migration. Merging those two points of view into one position has been an impossible endeavor seen more often as the Sisyphean task and usually calls for teamwork and interdisciplinary.

Equally, resources are under-allocated. This is limited, particularly in most regions within the developing world, by inadequate capital to invest in security infrastructure and sound migration policies [19]. This may result in what is referred to as overarching priorities, which effectively mean neglecting one area in favor of the other, which can be very damaging and bring into question the entire concept of integration.

Implementation is always challenging, especially if politically sensitive areas are involved. The practical form of real integration can stem from the agreement made by different concerned groups formed by government agencies, private sectors, and international organizations. There is always a challenge when it comes to getting a consensus on how the integration has to be undertaken in situations where there are divergent interests or where there is little trust between two parties or more.

Hence, it is important that policies focus on issues of coordination, resource allocation, and stakeholder engagement in developing this exhaustive and integrated policy on protecting critical infrastructure and managing forced migration. With examples like the Israeli and Estonian cases, other countries can find ways to strengthen infrastructures and communities to decrease migration dangers.

4.4 Integrated policy frameworks

Mitigating the impact occasioned by migration due to cybersecurity vulnerabilities will also require policy coherence. These are required to cover preventive and proactive activities to build up necessary cybersecurity and immediate response mechanisms to respond to cyber events in addition to systems for affected populations. In this manner, the policymakers will then be able to confront the risks provided by cyberattacks and the future impacts on migration and community cohesiveness.

For instance, the value of systematic reviews on the availability of data about the understanding of cyber risks and the formulation of strategies toward cybersecurity was underlined by Cremer et al.[20]. This will indicate, in an inclusive manner, the development of integrated policy frameworks that build up cybersecurity and consider the socio-economic drivers for migration. For instance, policies need to be set so that security protocols are updated routinely, investments are made in the cybersecurity infrastructure, and personnel are trained to handle cyber threats.

4.5 Addressing root causes of migration

There is no single solution to address the root causes of infrastructure-related vulnerabilities. For example, critical infrastructure vulnerabilities such as water systems cause untold suffering in communities and, ultimately, force migration. Addressing these vulnerabilities by policymakers will reduce the likelihood of migration being triggered by a cyber incident.

Gilodi et al.[21] critically examine how vulnerability and economic stability can be considered. Their work presents a new conceptual model for understanding and addressing migration-driving factors. More comprehensive strategies in this model would address the physical vulnerabilities to infrastructure and the socio-economic factors influencing migration. The union of these perspectives would provide policymakers with effective response mechanisms for cyber threats affecting migration.

4.6 Building resilience through collaboration of stakeholders

There is a need for collaboration between cybersecurity professionals, migration scholars, and policymakers to develop comprehensive strategies for protecting critical infrastructures and managing migration. This could lead to crafting robust policy frameworks in cybersecurity and the human dimensions of migration.

A case in point is that McLeman & Hunter[22] advanced the need to understand migration in vulnerability and adaptation in the view of climate change, calling for similar approaches in understanding cybersecurity. These are strategies that policymakers can acquire through climate change adaptation insights and the development of resilient communities to cyber threats.

5. Recommendations

As societies depend increasingly on interdependent technologies, the resilience of critical infrastructures, such as water systems, to cyber threats becomes a public need. This goes hand in hand with the global migration challenges because infrastructure vulnerabilities[23] often force populations to relocate. These recommendations aim to foster a robust cybersecurity framework, integrate cybersecurity within the policy framework on migration, and enhance cooperation among stakeholders. This is crucial to ensure that critical services continue stably and securely against any mass disorder due to migration.

5.1 Enhance cybersecurity measures

Recommendation: Enhance the digitized protections for water systems to deter cyberattacks, ensuring business continuity of essential services.

Rationale: Water systems are part of critical national infrastructure; their disruption would thus automatically result in dire public health and safety ramifications. Strengthening cybersecurity will lower the risks of service interruptions and later require emergency migrations. This is done using up-to-date state-of-the-art security technologies and regular software updating and patching to address system vulnerabilities.

Practical Implementation:

Cost-Effective Solutions: Cybersecurity solutions in low-resource settings can be executed at minimal costs. For instance, constant staff training in cybersecurity, basic intrusion detection systems, and strong passwords and access controls can be implemented at minimal cost.

International Collaborations: Countries with less capacity can tap into international collaboration or collaboration with developed countries to access advanced cybersecurity technologies and skills. For example, Kenya has worked with international donors to enhance water security using modest cybersecurity measures.

Action Steps:

1. Perform periodic security audits and vulnerability assessments to uncover and fix possible security gaps.
2. Advanced encryption techniques and intrusion detection systems should be in place to prevent unauthorized access.
3. Very tight access controls and authentication protocols must be in place to ensure that only authorized personnel get access to the critical systems.

5.2 Policy integration

Recommendation: Cyberspace issues should be integrated into migration policies to prevent situations where infrastructure weaknesses continue to precipitate migration.

Rationale: Incorporating cybersecurity into migration policy frameworks will help governments prepare for managing the severe consequences of infrastructure breakdowns on migration, as expected. This integration assists in developing proactive policies that contain the challenges as they emerge.

Practical Implementation:

Resource Allocation: One can establish priorities for important areas and gradually increase cybersecurity coverage in regions with limited resources. Depending on the availability of resources, governments can expand their activities in the most vulnerable infrastructures.

Community Involvement: Policies may be much more effective if the local communities are involved in their formulation and implementation. This can lead to more accessible approaches and enhanced sustainability due to the people's localized understanding of their needs.

Example of success: Estonia's integration of cybersecurity into public safety and broader migration policies offers a beneficial model. Though a small state with few resources, Estonia has succeeded in establishing a vital, robust digital infrastructure because it has placed cybersecurity at the top of public policy.

Action Steps:

1. Policies with direct links to migration should be drawn to incorporate cybersecurity measures into routine planning and infrastructure maintenance as a standard practice.
2. Policy dialogue by the cybersecurity agencies with the migration departments to strategize and share intelligence.
3. To ensure that these aspects are addressed, funds for cybersecurity will be appropriated in the different budgets for migration and infrastructure development.

5.3 A call for collaborative

Collaboration between cybersecurity experts, migration scholars, and policymakers is needed to develop an inclusive approach to protecting critical infrastructure and managing migration.

Justification: Collaboration between various disciplines and sectors may bring about more innovative and effective responses to complex problems at the intersection between cybersecurity and migration. Partnerships are needed to combine interdisciplinary knowledge with both fields' unique yet complementary strengths to devise comprehensive security and human mobility approaches.

Practical Implementation:

Multidisciplinary Task Forces: Cybersecurity and migration are multidimensional, so task forces are most apt for developing technically reasoned and socially informed strategies.

Capacity Building: An investment in capacity building, such as workshops and training, would develop cybersecurity measures' implementation and management skills locally. That can be important in resource-poor environments, where minimal experts are outside the ranks.

Example of success: Estonia's joint efforts in resilience in the digital domain have shown that multidisciplinary approaches can work even in resource-constrained environments. For instance, Estonia has developed a model that has mainstreamed cyber resilience in the public sector through continuous collaboration between government agencies, academia, and the private sector.

Action Steps:

1. It convened multidisciplinary task forces to devise strategies that address challenges arising from both cybersecurity and migration.
2. It can organize regular workshops and conferences to facilitate sharing of information and best practices among cybersecurity, migration, and policy experts.
3. Encourage joint research projects and pilot programs to test the effectiveness of an integrated approach to manage cyber threats and migration issues.

6. Conclusion and future research

The interplay of cybersecurity vulnerabilities in the water sector regarding human migration is another critical area of the holistic perspective. This study identified several critical findings, and further research is being conducted to develop the most effective measures and policies.

6.1 Key findings

Cybersecurity vulnerabilities and migration

Cyber-attacks on water systems disrupt critical services that are upheld with public health crises and economic instability, degrading living standards. It would, therefore, usually call for the migration of populations into areas they feel safer and assured about living in [12, 13]. The cascading effects of such disruptions underscore the critical need for a robust cybersecurity system to protect water infrastructures and significantly prevent forced migration. The incidents analyzed in this study manifest the weaknesses of digital water systems and how these have immense impacts on human migration patterns.

However, such cyber-attacks on the water system cause a loss of trust in utilities. Moreover, such erosion might lead to a decision to migrate in search of more reliable and secure climes. These dynamics further explain how the understanding gained from this level would allow policymakers to target strategies to improve cybersecurity in the Water sector, mitigate risks of forced migration, and build resilience among communities against various cyber threats.

Implication on public health and safety

The potential for cyber incidents to cause a compromise in water services is enormous due to the risk levels exposed to public health. Poor-quality water poses an immediate health threat to the community. Similarly, supply disruption exposes the communities to immediate risks; hence, relocation is possible to a region with better security features or more secure and functional water infrastructure [14]. Most relocations are usually super urgent and imminently necessary for survival away from such health threats. The interface between public health and cybersecurity is at a critical junction, underlined by massive, urgent movements in this sector.

Cyberattacks on the water infrastructure could result in a public health crisis, which adds to the pattern of long-term migration as the affected population seeks to avoid such events in their locality. Thus, this calls for including the public health dimension in a cyber security strategy targeting water infrastructure. Ensuring that cyber threats do not affect a water system ensures good health among the public, hence eliminating forced migration that may destabilize or diminish a community's resilience.

Economic and social implications

The economic manifestations of water service disruptions are enormous and undermine industries and agriculture with substantial job losses and financial instability, stalling growth and fuelling migration. According to Mishra et al. [15], when water services become compromised, such an economic shock in the form of community livelihoods can become disturbed by financial strain, which often compels people to migrate elsewhere for better opportunities where the situation regarding water infrastructure and economy appear promising.

The social implications of cyber-attacks on water systems include daily challenges in access to and quality of water that lessen the quality of life and community stability. Continuous stress and uncertainty can scrape away social cohesion or community resilience, cause constant outmigration, and add more burden to the receiving areas accommodating such populations. These economic and social impacts call for a comprehensive approach to wind cybersecurity with other broad social and economic policies to foster community resilience.

Need for integrated policies

Cybersecurity issues must be integrated into migration policies to address the root causes of infrastructure vulnerabilities. As Petersen and Wieltschnig[14] put forth in 2020, integrated policies can also reduce the impact of cyber incidents on vulnerable populations. Tying cybersecurity with the migration framework will only develop links with proactive measures protecting critical infrastructure against forced migration risks.

Integration makes the infrastructure and communities more resilient, able to sustain better and recover from cyber threats. Such policies must be formulated in sectoral and disciplinary collaboration among cybersecurity, migration, and water. This cooperation can offer fertile ground for innovation in responding to the technical and human sides of cybersecurity and migration. To this end, partnerships can be established, and knowledge can be shared to execute strategies to protect infrastructure for supplying water, support vulnerable populations, and guarantee stability and security for communities affected by cyber threats.

6.2 Future research directions

Detailed case analyses

Future research should be based on the case analysis of frontline cybersecurity incidents in the water sector. Profound studies of specific incidents occurring in Norway, the USA, and Israel can provide prolific information about diverse direct and indirect impacts on further migration patterns[22, 24]. The in-depth investigation of these cases has the potential to reveal how best practices might be identified and deleterious effects mitigated regarding cyber incidents upon water infrastructure and human migration.

These case studies should be based on diverse geographical regions and time frames. In understanding various contexts and responses, nuance will be given to discern the factors that drive post-cyber incident migration. That knowledge can, in turn, be used to develop targeted strategies and policies that look toward resilience building in water systems—systems that will undeniably help cut the risk of forced migration.

Research should prioritize questions such as: What specific factors in different regions most strongly influence migration after a cybersecurity incident in the water sector? How do varying levels of infrastructure development impact the severity of migration outcomes following such incidents? These inquiries will enable a comprehensive understanding of the complex dynamics at play.

Integrated policy frameworks

To this extent, it is essential to set up integrated policy frameworks that consider cybersecurity and migration factors. Such frameworks should consider proactive measures to strengthen such aspects as cyber security, rapid response strategies about a cyber incident, and assistance mechanisms for the affected population[20]. In this way, policymakers, through such an endeavor, would develop comprehensive strategies addressing the issues of technology and social aspects of Cybersecurity and Migration.

Policymakers should also evaluate the effectiveness of these integrated policy frameworks in mitigating the impacts of cyber incidents. This evaluation can provide valuable feedback to refocus and tabulate such policies to protect critical infrastructure effectively and sustain vulnerable populations. Governments can continuously assess and update policy frameworks to enhance resiliency in water systems and deter forced migration due to cyber threats.

Key research questions include: What are the most effective components of an integrated policy framework that addresses cybersecurity and migration? How can policymakers balance the immediate need for cyber defense with long-term strategies for community resilience? These questions will guide the creation of robust policies protecting infrastructure and populations.

Collaborative research

Encouraging collaborative research between cybersecurity experts, migration scholars, and policymakers can lead to the development of innovative solutions applicable to technical and human dimensions. In such respects of collaborative efforts, the resilience of their critical infrastructure and management of migrating flows become enhanced due to cyber threats[12]. can strengthen the resilience of critical infrastructure and improve the management of the flows of migration driven by cyber threats. In this respect, collaborative research through joint efforts can be helped by using scholars who represent divergent views and expertise toward holistic approaches in cybersecurity and migration.

Future studies should also address the potential of new technologies in improving cybersecurity and reducing vulnerabilities within critical infrastructures. What role technologies such as Artificial Intelligence, Blockchain, and IoT can assume will be investigated here to realize new insights on how such innovations exist or can be retrofitted to protect water systems from cyber incidents. If researchers and policymakers are to remain at the forefront of technological development, it will help come up with strategies that enable better security and resilience for water infrastructure.

Roadmap for future studies

1. Cross-disciplinary Approaches: Future research should focus on interdisciplinary methods to explore the multifaceted impacts of cyber incidents on migration. Collaboration among cybersecurity experts, social scientists, and policymakers is essential for developing comprehensive and holistic solutions.
2. Longitudinal Studies: Longitudinal studies that monitor the effects of cyber incidents on migration over time will provide deeper insights into its long-term impacts and sustainability in solutions applied.
3. Evaluation of Policies: Further research should see how effective an integrated policy framework would be in mitigating the impacts of cyber incidents and managing migration. Researchers will help build more solid and pragmatic frameworks by pointing out the successes and limitations of the existing policies.
4. Technological Innovations: The role of new technologies in cybersecurity research must be addressed, as these also help to minimize the vulnerabilities associated with critical infrastructure. The research agenda should address the practical application of such technologies and their potential to prevent forced migration.

Research Questions:

- In what ways do emerging technologies perform, especially in resource-constrained environments?
- What are the possible unintended consequences of using leading-edge cybersecurity technologies within critical infrastructures?
- How could policy frameworks be revised to include technological innovations and ensure protection from all cyber threats?

In conclusion, the interaction between the cybersecurity vulnerabilities of the water sector and migration provides numerous challenges and opportunities. Future research areas should focus on detailed case analyses, creating integrated policy frameworks, collaborative research initiatives, and exploring various technological innovations. Addressing these critical areas will enable researchers to develop a deeper understanding of the complex dynamics that obtain and, thus, propose actionable solutions to protect vulnerable populations by making the critical infrastructure resilient. Comprehensive research, well-integrated policy, and collaborative efforts will create a stable and secure environment for everyone.

Conflicts of Interest

The authors declare no conflict of interest.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The below two referenced sources and underlying links may provide relevant and available data: Ernst & Young. (2019). Welcome to e-Estonia: A digital pioneer stakes a claim in AI's landscape. Global Tax News. https://globaltaxnews.ey.com/news/2019-5574-welcome-to-e-stonia-a-digital-pioneer-stakes-a-claim-in-ais-landscape[18]. UNHCR - The UN Refugee Agency. (n.d.2024). Global Trends | 2023. UNHCR. UNHCR. https://www.unhcr.org/global-trends[24].

Funding

This work received no external funding.

Acknowledgments

Attila Mate Kovacs is a Ph.D student at Obuda University Doctoral School on Safety and Security Sciences.

Special thanks to his PhD supervisor, Professors Zoltán Rajnai and also to Professor János Besenyő, for their inspiring guidance, which has been instrumental in developing papers such as "Migration Perspectives of Water Sector Cybersecurity." Attila Mate Kovacs would also like to acknowledge the Neurology Department of the Uzsoki Street Hospital, a teaching hospital affiliated with the Semmelweis University Faculty of Medicine, for their continuous medical and professional support. Attila Máté Kovács works at ExxonMobil, where, despite the demands of his role, he has received support and an encouraging environment. Outside of his working hours, he has been able to continue pursuing his PhD research, contributing valuable insights to his academic work.

References

[1] Altaleb, H., Rajnai, Z., 2024. A comprehensive analysis and solutions for enhancing SCADA systems security in critical infrastructures. Proceedings of The IEEE 11th International Conference on Computational Cybernetics and Cyber-Medical Systems. p. 1. Available from: https://www.researchgate.net/publication/381759077_A_Comprehensive_Analysis_and_Solutions_for_Enhancing_SCADA_Systems_Security_in_Critical_Infrastructures

[2] Besenyő, J., Gulyás, A., 2021. The effect of the dark web on security. Journal of Security and Sustainability Issues, 11(1), 103–121. DOI: https://doi.org/10.47459/jssi.2021.11.7

[3] Bederna, Z., Rajnai, Z., Szadeczky, T., 2020. Attacks against energy, water and other critical infrastructure in the EU. Proceedings of The 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE); Budapest, Hungary. 000125–000130. DOI: 10.1109/CANDO-EPE51100.2020.9337751

[4] Besenyő, J., Kovács, A.M., 2024. Cybersecurity Vulnerabilities in the Water Sector. Springer.

[5] Kovacs, E., 2023. Ransomware hit SCADA systems at 3 water facilities in U.S. SecurityWeek. Available from: https://www.securityweek.com/ransomware-hit-scada-systems-3-water-facilities-us/

[6] Boubaker, K.B., 2021. Water industry: a look back at twenty years of cyber attacks. Stormshield. Available from: https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/

[7] Townsend, K., 2016. Michigan Power and Water Utility Hit by Ransomware Attack. SecurityWeek. Available from: https://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack/

[8] Olenick, D., 2018. North Carolina water utility ONWASA taken down by ransomware. SC Media. Available from: https://www.scmagazine.com/news/north-carolina-water-utility-onwasa-taken-down-by-ransomware

[9] Wall, T., 2022. Throwback Attack: Hackers attempt to flood Israeli water supply with chlorine. Industrial Cybersecurity Pulse. Available from: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-hackers-attempt-to-flood-israeli-water-supply-with-chlorine/

[10] Cohen, G., 2021. Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire. Industrial Cybersecurity Pulse. Available from: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/#:∼:text=Then%2D49%2Dyear%2Dold

[11] Greenberg, A., 2021. A Hacker Tried to Poison a Florida City's Water Supply. Wired. Available from: https://www.wired.com/story/oldsmar-florida-water-utility-hack/

[12] Kariuki, P., Ofusori, L.O., Subramaniam, P.R., 2023. Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. Security Journal. DOI: https://doi.org/10.1057/s41284-023-00378-1

[13] Bhandari, P., Creighton, D., Gong, J., et al., 2023. Evolution of cyber-physical-human water systems: Challenges and gaps. Technological Forecasting and Social Change. 191, 122540. DOI: https://doi.org/10.1016/j.techfore.2023.122540

[14] Petersen, K., Wieltschnig, P., 2020. BALANCING INNOVATION AND VULNERABILITY: WATER SECURITY IN AN AGE OF CYBER-WARFARE. WIT Transactions on Ecology and the Environment. DOI: https://doi.org/10.2495/wp200071

[15] Mishra, B.K., Kumar, P., Saraswat, C., et al., 2021. Water security in a changing environment: concept, challenges, and solutions. Water. 13(4), 490. DOI: https://doi.org/10.3390/w13040490

[16] Hassanzadeh, A., Rasekh, A., Galelli, S., et al., 2020. A Review of Cybersecurity Incidents in the Water Sector' Journal of Environmental Engineering. 146(5), 03120003. DOI: https://doi.org/10.1061/(asce)ee.1943-7870.0001686

[17] Welle, D., 2020. Israel stops cyberattack on water system. DW.com, 28 May. Available from: https://www.dw.com/en/israel-thwarted-attack-on-water-systems-cyber-chief/a-53596796

[18] Ernst & Young, 2019. Welcome to e-Estonia: A digital pioneer stakes a claim in AI's landscape. Global Tax News. Available from: https://globaltaxnews.ey.com/news/2019-5574-welcome-to-e-stonia-a-digital-pioneer-stakes-a-claim-in-ais-

landscape

[19] Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., et al., 2021. Cybersecurity in ICT supply chains: key challenges and a relevant architecture. Sensors. 21(18), 6057. DOI: https://doi.org/10.3390/s21186057

[20] Cremer, F., Sheehan, B., Fortmann, M., et al., 2022. Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance—Issues and Practice. 47(3). Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

[21] Gilodi, A., Richard, C., Albert, I., et al., 2023. The Vulnerability of Young Refugees Living in Reception Centres in Luxembourg: An Overview of Conditions and Experiences across Subjective Temporal Imaginaries. Social Sciences. 12(2), 102. DOI: https://doi.org/10.3390/socsci12020102

[22] McLeman, R.A., Hunter, L.M., 2010. Migration in the context of vulnerability and adaptation to climate change: insights from analogues. Wiley Interdisciplinary Reviews: Climate Change. 1(3), 450–461. DOI: https://doi.org/10.1002/wcc.51

[23] Besenyő, J., Fehér, A., 2020. Critical Infrastructure Protection (CIP) as New Soft Targets: Private Security vs. Common Security. Journal of Security and Sustainability Issues. 10(3), 14. DOI: https://doi.org/10.9770/jssi.2020.10.1(1)

[24] UNHCR—The UN Refugee Agency, 2024. Global Trends | 2023. UNHCR. Available from: https://www.unhcr.org/global-trends