INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

MIGRATION PERSPECTIVES OF WATER SECTOR CYBERSECURITY

Attila Mate Kovacs
CISA|CISM|OSCP|CEHv11|CCISO|ISO27kCLA
Óbuda University Doctoral School on Safety and Security Sciences
Senior Industrial IT Cyber Security Expert, ExxonMobil Industrial Cyber Security
ORCiD: https://orcid.org/0000-0001-5088-5749
https://www.linkedin.com/in/attilamatekovacs/

Abstract
Integrating digital technologies into the water sector has revolutionized the management and provision of water resources, driven by advances in information technology. This shift enhances the efficiency, reliability, and scalability of daily operations within water utilities, transitioning from labor-intensive manual processes to sophisticated automated systems. Key technologies include SCADA, GIS, and advanced metering infrastructure.
Adoption rates vary, with developed countries like the United States, Germany, and Japan leading due to superior infrastructure and investment capabilities. These nations leverage intelligent water management systems to enhance performance and minimize water losses. Conversely, developing countries face challenges such as financial constraints, inadequate infrastructure, and limited technical expertise, hindering the widespread adoption of digital technologies in their water sectors. Despite these obstacles, the global trend towards digitalization in water management continues to grow, promising significant improvements in water resource management worldwide.

Introduction

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 mainly manual, leading to a labor-intensive process. However, the sector has advanced much with digitalization, introducing automation technologies such as SCADA, GIS, and metering infrastructure.
For instance, SCADA systems allow operators to monitor and control water treatment and distribution systems in real-time. Operators can use such systems to identify and solve problems or implement solutions on time before potential disruption. GIS technology enables mapping and management of water networks, thus assisting in better planning and response strategies. The development of smart meters has revolutionized affected water usage monitoring by providing specific data on use to the extent that it can be used for 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.

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.

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.

Scope

The study will involve geographically different parts, and it is only in this way that it will be possible to understand cybersecurity incidents in the water sector better. 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.

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.

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 cyber attacks 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?

Cybersecurity Incidents in the Water Sector:
A 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.

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 (Kovacs, 2023). 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 (Boubaker, 2021). 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. By taking critical systems offline and bringing the delivery of vital services to a standstill, in totality, it paralyzes all utility functions (Townsend, 2016). 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 that these vital operations underperformed, with the authority failing to deliver the essential services as expected (Olenick, 2018). 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 (Wall, 2022). 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. All this situation testifies is 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(Cohen, 2021). 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 in that the contaminated water sources were opened into that area, therefore threatening the 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 (2021), 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, clearly prove the devastating effects of cybersecurity incidences within the water sector in driving migration patterns and point out an urgent need for integrated policies on cybersecurity vulnerabilities and how the latter can drive migration.

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	**San Francisco**	**2021**	**Hackers leveraged former employees'**	**Public trust in water safety is compromised,**

Outdated Systems	**and Florida, USA**		**login information to target outdated systems, compromising water treatment facilities.**	**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	**Oldsmar, Florida, USA**	**2021**	**Hacker attempted to poison the city's water supply by increasing sodium**	**Public health threats created a crisis of confidence in water safety, potentially**

Treatment Plant			**hydroxide levels to hazardous amounts.**	**driving residents to relocate to areas with secure water systems.**

Migration and Cybersecurity Vulnerabilities

Exploring the Link between Migration Patterns and Cybersecurity

Forced Migration and Public Health

In one extreme example, a cyber-attack of this nature might result in a catastrophic public health disaster, with consequent forced migration. This is evident, for instance, in the case of contamination or the disruption of water supplies, which immediately poses a severe threat to community health. In this regard, Kariuki et al. (2023) argue that it is the small-scale African migrant traders in Southern Africa who are at a disproportional risk from such threats, compounding their plight. Outbreaks of waterborne diseases will likely become severe public health risks and force populations from such affected areas to migrate to places with safer water supplies.

Public health emergencies that occur from cyber incidents can easily translate to mass migrations taking place very quickly. People can be forced out of their homes if they live in an area where a cyber attack has contaminated water to save them from related health hazards. This indicates a strong interaction between cybersecurity in water infrastructure and migration, as these households move into areas where security about water quality and the public health system is better. All these movements result in resource strain on the new destination regions and make the need for heightened cybersecurity more acute to avoid those crises and uphold public health.

Economic Impact and Migration Drivers

Economic instability due to cybersecurity incidents in the water sector is among the leading driving factors for migration. Water service interruptions lead to industrial and agricultural process stoppages. This, in turn, leads to the loss of jobs and economic downturns. Bhandari et al. (2023) further elaborate on these issues, which have been brought by the latest development of the cyber-physical-human water systems, and hence insist on close linkage of economic activities with reliable water services. In financially less stable areas, cyber-related water service outages can create an economic emergency in their own right, driving masses and families to move in search of financial well-being.

Those local economies lacking employment and other financial resources will encourage the population to move when they become destabilized. Among the particularly vulnerable groups are communities that depend on agriculture and industry since a disruption can stop both production and income generation at the same time. As people struggle to make a living amid this economic pressure, they often migrate to urban centers or across national borders. Cybersecurity in the water sector may maintain financial stability and prevent forced migration dictated by financial imperatives.

Quality of Life and Migration Decisions

The general quality of life in those areas affected by cyberattacks on water systems can deteriorate quickly, influencing migration decisions. Residents exposed to unreliable water supplies or possible contamination are, by and large, falling in their living conditions. Mishra et al. (2021) observe that water security is critical in maintaining human health and economic development. With decreasing life quality, migration happens where the infrastructure is perceived as more secure and resilient for good living standards and open access to clean water.

However, such unabated daily trials make life unliveable concerning water services in such areas. Problems of cooking, cleaning, and ensuring personal hygiene beset families and are only possible with reliable water availability. The psychological burden of living under the threat of constant contamination further diminishes life quality and makes them migrate to safer habitats. One of the most important factors supporting maintaining quality of life and preventing migration from dramatically degraded living conditions, therefore, must ensure adequate water infrastructure protection against cybersecurity threats.

Cyber Vulnerabilities

Regions whose environments and structures have already been exposed to stress are, unsurprisingly, often most immediately sensitive to the fallout of any cybersecurity incident in the water sector. Petersen and Wieltschnig (2020) emphasize the dangers of balancing innovation with vulnerability in water security, arguing that regions of rapid technological development without an equal cybersecurity investment rate are more exposed. In Asian and African areas, where water security is already on a thin line, the risks rise, and these areas become hotspots for forced migration caused by the distortion of water service.

At this level, the added layer of cyber vulnerability may complicate things. For example, cyber-risks to water infrastructure further worsen the situation for countries in the Middle East that already face either water scarcity or political instability. These dual risks further increase the migration option for residents seeking a more stable and secure existence. This requires knowledge of such vulnerabilities based on the geography and infrastructure types in question so that targeted improvements may be made in water security to mitigate migration.

Case Study: Africa

In Africa, the intersection of cybersecurity vulnerabilities and migration is prominently observed. Kariuki et al., 2023 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. (2023), 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 (2020) 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 is a factor that emerges very clearly. Mishra et al. (2021) 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 resulting 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.

Resilience through Technological Advancements

Investments in state-of-the-art cybersecurity technologies toward a resilient water infrastructure. Bhandari et al. (2023) 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 (2020) 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 comprehend the vulnerabilities that characterize a particular region fully. The outputs should, through collaborative efforts with policymakers and researchers, yield actionable policy matters for enhancing water security, protecting public health, and preventing forced migration resulting from cyber threats. The two work toward making it hard for their communities to alter cybersecurity threats to their water systems.

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.

The Interconnectedness of Cybersecurity and Migration Policies:

The solution to the root cause of migration might lie in the interconnectedness between cybersecurity and migration policies due to infrastructural vulnerabilities. Suppose cyber-attacks against critical infrastructures, like the water system, are flourishing. In that case, they might lead to dramatic failures in delivering essential services that create public health emergencies and economic dislocation pressures, both of which catalyze migration. Therefore, cybersecurity in migration policies builds more resilient infrastructures and protects the community from the cascading effects of cyber incidents.

The UNHCR Report on Global Trends emphasizes the urgent need to solve the displacement crises fueled by conflict, violence, and disasters. The critical infrastructure vulnerabilities in cybersecurity will add another layer of risk that such development poses; thus, policy changes covering cybersecurity and migration become necessary. An integrated approach can protect infrastructure from cyber threats, reducing the likelihood of service disruptions that would force people to migrate.

Integrated Policy Frameworks:

Effective mitigation of the impacts of migration due to cybersecurity vulnerabilities will also call for integrated policy frameworks. These are needed to encompass proactive measures to enhance cybersecurity defenses and rapid response strategies to deal with cyber incidents, on top of systems supporting the populations affected. By such means, policymakers will then be able to address the immediate dangers posed by cyberattacks and the long-term consequences for migration and community stability.

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. (2022). 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.

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. (2022) critically examine how to consider vulnerability in the case of migration. Their work presents a new conceptual model applied to 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.

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 (2010) 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.

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 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.

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.

Action Steps:

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

Policy Integration

Recommendation: Cyberspace concerns should be integrated into migration policies to ensure that infrastructure vulnerabilities no longer remain the underlying causes of migration.

Rationale: Making cybersecurity a critical factor in migration policy frameworks will enable governments to proactively deal with the expected severe impacts of infrastructure failures on population movements. Such integration helps formulate policies that should be reactive and preventive, hence nipping the challenges at their roots.

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.

A Call for Collaborative

Efforts There is a need for collaboration between cybersecurity experts, migration scholars, and policymakers to develop an all-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.

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 the 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.

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 placed on developing the most effective measures and policies.

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 (Kariuki et al., 2023; Bhandari et al., 2023). 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 (Petersen & Wieltschnig, 2020). 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 extents of 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. (2021), 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 need to be integrated into migration policies to address the root causes of infrastructure vulnerabilities. As Petersen and Wieltschnig 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.

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 (UNHCR; McLeman & Hunter, 2010). 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.

Integrated Policy Frameworks:

To this extent, it is essential to set up integrated policy frameworks considering 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 (Gilodi et al., 2022). 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.

Collaborative Research:

Encouraging collaborative research between cybersecurity experts, migration scholars, and policymakers can lead to developing 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 (Petersen & Wieltschnig, 2020). 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.

Future Research

Directions Future research, for example, would help to fill these gaps and further provide explanations based on the following:

- Cross-disciplinary Approaches: Investigation on Multiple Impacts of Cyber Incidents on Migration- interdisciplinary methods are needed.
- Longitudinal Studies: Research over a long period to trace the impacts of cyber incidents on migration over time.
- Policy Evaluation: Assessing the effectiveness of integrated policy frameworks in mitigating the impacts of cyber incidents and managing migration.
- Technological Innovations: Exploring the role of emerging technologies in enhancing cybersecurity and reducing vulnerabilities in critical infrastructure.

Therefore, the interplay between cybersecurity vulnerabilities in the water sector and migration presents significant challenges and opportunities. Comprehensive research, integrated policies, and concerted actions will help make critical infrastructure resilient, protect vulnerable populations, and give everyone a stable and secure environment.

References

Bhandari, P., Creighton, D., Gong, J., Boyle, C., & Law, K. M. Y. (2023). Evolution of cyber-physical-human water systems: Challenges and gaps. Technological Forecasting and Social Change, 191, 122540. https://doi.org/10.1016/j.techfore.2023.122540

Boubaker, K. B. (2021, August 30). Water industry: a look back at twenty years of cyber attacks. Stormshield. https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/

Cohen, G. (2021, November 4). Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire. Industrial Cybersecurity Pulse. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/#:~:text=Then%2D49%2Dyear%2Dold

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

Gilodi, A., Richard, C., Albert, I., & Nienaber, B. (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. https://doi.org/10.3390/socsci12020102

Greenberg, A. (2021, February 8). A Hacker Tried to Poison a Florida City's Water Supply. Wired. https://www.wired.com/story/oldsmar-florida-water-utility-hack/

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. https://doi.org/10.1057/s41284-023-00378-1

Kovacs, E. (2023, January 24). Ransomware hit SCADA systems at 3 water facilities in U.S. SecurityWeek. https://www.securityweek.com/ransomware-hit-scada-systems-3-water-facilities-us/

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. https://doi.org/10.1002/wcc.51

Mishra, B. K., Kumar, P., Saraswat, C., Chakraborty, S., & Gautam, A. (2021). Water security in a changing environment: concept, challenges, and solutions. Water, 13(4), 490. https://doi.org/10.3390/w13040490

Olenick, D. (2018, October 16). North Carolina water utility ONWASA taken down by ransomware. SC Media. https://www.scmagazine.com/news/north-carolina-water-utility-onwasa-taken-down-by-ransomware

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

Townsend, K. (2016, May 3). Michigan Power and Water Utility Hit by Ransomware Attack. SecurityWeek. https://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack/

UNHCR - The UN Refugee Agency. (n.d.). Global Trends | UNHCR. UNHCR. https://www.unhcr.org/global-trends

Wall, T. (2022, May 26). Throwback Attack: Hackers attempt to flood Israeli water supply with chlorine. Industrial Cybersecurity Pulse. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-hackers-attempt-to-flood-israeli-water-supply-with-chlorine/