BALANCING INNOVATION AND VULNERABILITY: WATER SECURITY IN AN AGE OF CYBER-WARFARE

KATRINA PETERSEN & PETER WIELTSCHNIG
Applied Innovation & Research Team, Trilateral Research, Ireland

ABSTRACT

Through technological and organisational innovations, water services are increasingly finding new pathways to reduce water insecurity. For instance, the real-time detection of water pollution through the deployment of novel sensors can mitigate contamination problems before they become widespread. While these tools open up new forms of water security, they simultaneously create new forms of vulnerability as the connectivity and digitalisation of these infrastructures create remote pathways to control water system behaviours. The cyber-warfare capabilities of state and non-state actors are becoming increasingly sophisticated, and attacks have successfully infiltrated water systems with worrying potential. Indeed, in 2018, the US Department of Homeland Security and Federal Bureau of Investigations highlighted the threat of cyber-attacks from hostile countries on water systems, demonstrating the very real nature of these threats. This paper assesses the vulnerabilities arising from increasing interconnectivity and digitalisation in water infrastructures, paying particular attention to demographics at risk of insecurity. The paper starts by reviewing cyber-warfare practices relating to infrastructure, including their increasing frequency and sophistication. This is overlaid with a current demographic understanding of water insecurity and potential vulnerabilities to cyber-attack to identify what intersectionalities appear as new threats emerge. The paper then explores the necessary structure and value of ethical impact assessments in the design of innovative technology and practices in the water sector. In order to foster sensitivity to vulnerabilities and create avenues for incorporating scalable preventative and mitigating measures into design, a practical framework (in the form of a list of questions) is outlined. This paper finds that our understanding of water insecurity must adapt to the challenges posed by cyber-attacks. Sensitivity to the existence of these threats must be fostered and a practical framework developed to attune stakeholders to cyber-threats and assist those engaged with new technologies in the water sector.

Keywords: water security, cyber-attacks, cyber-security, intersectionality, ethics, environmental justice, vulnerability, internet of things, impact assessments, water pollution.

1 INTRODUCTION

Water security is commonly framed in terms of securing quality and quantity, and whether water is accessible, sustainable, and drinkable. For example, in 2013, the UN defined water security as "the capacity of a population to safeguard sustainable access to adequate quantities of acceptable quality water for sustaining livelihoods, human well-being, and socio-economic development" [1]. A lack of fresh water can affect the affordability of drinking water, and have a detrimental effect regarding public health, food security, human security, and political unrest [2]. But what is at stake with water insecurity and what actions need to be taken to ensure these water security goals are met can vary greatly depending on the region of focus. Wealthy nations, like those in Europe, face different forms of water insecurity than developing countries. As a result, the European Water Framework Directive, the Drinking Water Directive have re-articulated water security in contexts where access to running water is plentiful. They shift the focus from getting water to people in the first place, to maintaining the ecological and chemical quality of water and the work necessary ensure this public good. They establish definitions for sustainable use of that water, including the potential for water scarcity from shrinking water tables, increased demand from growing populations and agricultural needs (expected to be a problem across 30% of EU Member

WIT Transactions on Ecology and the Environment, Vol 242, © 2020 WIT Press
www.witpress.com, ISSN 1743-3541 (on-line)
doi:10.2495/WP200071

States by 2030), the adaptation to climate change events (such as drought or flooding), and the likely increasing need to work with water from outside of EU borders [3]. The directives also aim to define what it means to have healthy water quality. Despite the established water infrastructures, sewage, industrial, and agricultural waste discharged into the waterways (diffuse pollution affects 90% of river basin districts, 50% of surface water bodies and 33% of groundwater bodies across the EU) continue to harm the environment or human health [4]. As a whole, they make the case that services need to provide for this good by protecting the transit of the water as well as the aquatic ecosystems and river basins the water comes from.

In this context, the risks to water security are framed strategically, e.g. what if the water gets cut off? In particular, vulnerabilities are framed not in humanitarian need or developmental progress, but as coming from external sources, such as extreme weather events or terrorist attacks, where standards and technology innovation are often looked to as mitigation measures [5], [6]. Similarly, solutions to these risks are framed in strategic technologies, like the use of remote sensors, smart technologies, and IoT systems. Within our work in the European Union Horizon 2020 funded project, aqua3S (grant agreement number 832876), we are currently addressing these challenges. The aqua3S project addresses seeks to create a water sensor system that utilises sensor technologies to support water safety. In doing so, IoT connected sensors, unmanned aerial vehicles (UAVs), satellite images and community generated social media observations on water quality will be used to identify anomalies in water networks. The collected information will then be presented to water network operators through an interactive user-face. Ultimately, these systems will only be used to assist decision making. In developing this system, robust physical and cyber-security measures are being developed, including encryption, privacy by design processes and access restrictions among others.

However, the relationship between water security, vulnerability, and human rights need to be fully appreciated in this context [2]. Movements like the Citizens' Initiative "Right2Water", reveal that even within these generally water secure regions, concerns still exist about how these definitions and solutions take into account differential access, equality, and uneven vulnerabilities. Exploring where interconnectivity and digitalisation in water infrastructures and strategic state solutions intersect with human rights and vulnerability offers an opportunity to explore the ethical dilemmas raised within water security. This article examines these water and cyber security frames to explore how to balance scales between innovation, inequal vulnerabilities and cyber-security threats. To approach the answer, it pays particular attention to demographics at risk of insecurity. Doing so, it sets the stage to create a reflexive framework for assessing the ethical implications of water security practices that help decision-makers see beyond normative and global assessments. We argue that to meaningfully understand the implications it is necessary to focus not only on where things can break but also on what is at stake, and for whom. The article bring into discourses about which bodies of water, pipelines, or ecologies could be affected (and by what) questions about how we know that the security provided is fair, just, and beneficial to all. It also highlights the important differences and overlaps between human security versus state security. The risk, at its core, is whether failing to develop a nuanced understanding of these relationships ultimately risks puncturing entry points for malign cyber infiltration into services that are essential for populations with the brunt of the potential resultant harms falling disproportionately on vulnerable and marginalised communities.

2 WATER SECURITY IN EUROPE

Within Europe, water security issues are defined through acceptable thresholds of threats and risks, including uncertainty, trade-offs, and social-economic and environmental externalities.

Running through these definitions around water security in legal frameworks across Europe are assumptions that the original water supply is relatively safe, protected against disease, is adequate and reliably availability for the needs, be they community, agriculture, or state [7]. This is reflected in European nations' massive investments of resources in decreasing water scarcity and similar high stressors. However, ethics and human rights – including how these definitions of security supports the necessities of a good life, human health, and ecosystem sustainability – are less well articulated in these definitions [8]. The underlying causes of water insecurity which have demonstrated discriminatory affects that are both less visible in the structure of these regulations and in water security practices themselves [9]. To help make these vulnerabilities more visible, questions like "is the water clean?" and "is the water reaching its destination?" need to be paired with "whose water is clean?" and "who is accountable for that protection?"

2.1 Unknowns and uncertainties as vulnerabilities

Such an approach requires understanding the vulnerabilities that need securing. Vulnerability is tied to a person's or community's ability to cope with a risk [10]. Coping abilities, however, are difficult to measure with data, numbers, or sensors. Moreover, quality of the data is only possible to ensure with knowns, yet vulnerabilities, often by definition, are the result of unknowns. This is exacerbated by intersecting practices of water security with state security where the daily acts of living (a child turning on the tap to wash hands in a kitchen sink pulling water from leaking lead pipes) become side-lined for equally important discussions around national water supplies, international relations necessary for such supplies, and trade-offs in different water usages (e.g. agricultural for food versus washing laundry at home) [11].

Indeed, measurements technologies are often weakest in areas with the highest uncertainties or variabilities [10]. Both new and legacy chemicals add to the chemical burden on Europe's populations and ecosystems, affecting public health in uncharted ways. Moreover, scientific uncertainty around what levels of some chemical substances are harmful has resulted in varying definitions of contamination. For example, the effects of the mobility, widespread use, and persistence of per-fluoroalkyl and polyfluoroalkyl substances (PFAS), which have been used for years in products from stain resistant textiles, Teflon, to pizza boxes are just now being made visible, resulting in contaminated drinking water and ubiquitous exposure throughout the Global North. Yet, despite government acknowledgement of long-term negative health effects of these and other micropollutants, there are no EU standards for drinking water on PFAS enabling use of such chemicals to go without restrictions, often without oversight [12], [13]. Further, for chemicals for which there exists guidance in the EU Drinking Water Directive, in some highly polluted areas concentrations of perfluorooctanoic acid (PFOA) and perfluorosulfonic acid (PFOS) in drinking water were well above the proposed limits [13]. Similar data gaps and asymmetries fall around diffuse water pollution from agriculture (DWPA), which can consist of pollutants from fertilizers and manure, sediment, and pesticides from farms, golf courses, private gardens and other rural domestic activities [14]. These pollutants have dispersed and less readily visible sources, making knowing where to put a sensor, when to sense, and what to sense for elusive. These uncertainties can be seen in the challenges in managing these chemicals in drinking water that emerge simply from their large numbers and variety, unconsolidated information, and limited studies on health impacts, particularly around persistence and regional sources that risk different types of exposure [15].

All too often guidelines are designed and applied only after contamination is discovered by other mechanisms, frequently through public outcry or new disease bubbles. While these mechanisms for monitoring keep increasing, validated methods are still lacking for some sources, like groundwater. Moreover, the policy and guidelines for making decisions around these issues lag, making it difficult for those facing insecurity from these arenas to know how to ask for change [12].

2.2 Differential and unequal vulnerabilities

Overall, low-income and minority communities disproportionately suffer from water pollution, are less able to afford treatment systems in home, lack technical and financial support, are more likely to live in areas with failing infrastructures and legacy chemicals like lead and have less resources for oversight [16]. However, water security discourse focuses on water infrastructure (e.g. water to buildings), and less about water within buildings or all populations. These differentials affect most those forgotten in society in general. For example, water security statistics miss the homeless who deal with a different type of complexity to water security, such as access to public toilets and water fountains [17]. More generally, such vulnerabilities are increasingly documented in many regions in a similarly wealthy nation, the U.S., as exemplified by the ongoing water crisis in Flint, Michigan and the water health crisis Hurricane Katrina and Hurricane Harvey.

Flint has demonstrated that many vulnerabilities are infrastructure based, both in home and in transit. The vulnerabilities faced were not results of the water source, per se, but result of the pipes themselves the water travelled through: in the lead leached from the pipes that travel to the kitchen faucets. It does not help that the particulate release from the pipes into the water was often sporadic and thus only sometimes registered toxicity when tested [16]. The families living in the houses fed by these pipes were most likely near or below the poverty level without the financial means to fix their pipes or the time to campaign for structural changes, reducing their visibly to decision-makers. These vulnerabilities are further masked by the young bodies that experienced the greatest harms, as they do not as readily have a political voice to push for change.

Climate stresses on water security are already a prominent discussion in policymaking. Nonetheless, even here, socio-economic disparities have the potential to influence the intensity of vulnerabilities. After Hurricanes Katrina and Harvey, the excess water from flooding meant facing toxicity residues in soils from activities that ended decades prior, leaking into groundwater and water sources undetected. In some cases, these previous activities were no longer recorded in land management or public housing planning. The lack of understanding around how these chemicals from the past affect water quality and health over the long term aggravates unknows and uncertainties for all. But, just as much, considering the trend to poorer, marginalised communities (often based in racial and class divides) living on former industrial and farm sites, such gaps in data and can have disproportionate effects. This cascading toxicity, moving from forgotten chemical legacies contaminating the ground to pollutants in drinking water had direct effect on the socio-economically disadvantaged populations that often live in or near former industrial sites [18]. By not collecting this data, structural water insecurity is built in for those already less powerful in society, trends that in the US have already instigated discourses around racial violence [11]. In the EU, these challenges are emerging in the discourses around toxic soils.

From the other direction, these kinds of power differentials also play out into who gets policed in relation to water security violations. Several studies have identified that a small subset of polluters cause the majority of the pollution, and that these polluters create

disproportionate exposures to these chemicals through water for low income, non-white, and otherwise disadvantaged populations that don't have equal resources for making such activity visible to government decision-makers or for holding the companies accountable [19].

Much of the literature around the second phase of environmental justice has pushed this last point: justice requires mechanisms through which to make change, the procedures for participating in decisions and opportunities to build equality [20]. Security, from this perspective, is not just about the ability to obtain a good (e.g. clean drinking water) generally in society, but about how the risks to such a good are produced and distributed across society. This requires identifying positional inequalities that affect how vulnerabilities are spread in ways that disadvantage some while giving advantages to others, so that the basis for social and political change that support sustainable water security can emerge [20].

3 THE RELATIONSHIP BETWEEN CYBER SECURITY AND WATER SECURITY

The push towards the minimisation of operational costs and expenses has also led the charge towards technical innovation to better manage these increasingly evident forms of water insecurity. Amongst these is a drive to create increasingly extensive sensor networks across water systems to identify leaks and bursts, locate contaminants, and better manage disruptions, thereby creating new ways to see and eliminate uncertainties that lead to vulnerabilities [21]. In doing so, water service providers have looked towards the Internet of Things (IoT), utilising cloud computing to extend the reach and interconnectedness of their system [22]. This section maps these innovative potentials onto the vulnerabilities described in the previous section to explore how these efforts to protect water security produce new forms of benefits and vulnerabilities. It considers new risks that arise from cyber-attacks on these water systems in order to identify how cyber-security threats could manifest and influence how vulnerabilities and water security are framed.

Within the context of the water sector, this sensor innovation is most often achieved through connecting Supervisory Control and Data Acquisition (SCADA) systems – used for monitoring and controlling systems – with the IoT-cloud [22]. Beyond minimising costs, such remote sensor systems can capture issues that may otherwise be resource intensive and time consuming, such as the detection of pollutants and weak water pressure. Water service providers can produce a reactive and agile system that is able to detect anomalies and target threats in an efficient manner before actual harms manifest. Within analogue systems these anomalies may only be identifiable once a harm has already materialised or through the resource heavy system of manual testing, presenting concern to water services providers.

However, though these measures safeguard the integrity of the system, water security should not simply be addressed as a problem that can be solved with technical solutions. To begin with, cyber-attacks on smart water infrastructures in recent years demonstrate the vulnerability of critical infrastructure to infiltration. In addition, the ethical dimensions of such approaches to water insecurity need to be considered to inform our responses and provide an insight into how such responses shift our focus within the concept of water security in specific ways.

3.1 Cyber-attacks on water networks

Previous cyber-attacks on water networks offer some insights into key areas of vulnerability, the methods of attackers and the ways in which the effects can manifest. From the outset, it is important to note that the attacks outlined below do not necessarily relate to vulnerabilities arising out of IoT connected infrastructure. Nevertheless, they paint a useful picture of the vulnerability of systems that are able to be accessed remotely.

While these systems increase the nature and effectiveness of monitoring risks, they open these infrastructures to remote access and control. Moreover, they transform new forms of access to the pipelines and the water within into different vulnerabilities. To start, multiple attacks have occurred with worrying potential. Some are considered to have arisen out the offensive capacities of units specialising in cyber-attack that were not targeting water specifically but water as a means to state disruption. For instance, the Iranian Revolutionary Guard are said to have attacked the Bowman Avenue Dam in New York state, gaining control of the command and control system, with the ability to produce kinetic effects on the water system. While the flood gates were offline for maintenance and were therefore not accessible within the attack, this was fortuitous and demonstrates how vulnerable systems may actually be [23]. The 2016 attack on the "Kemuri" water plant (a pseudonym given to the plant), attributed to political hackers affiliated to Syria, gained control the levels of chemicals used within the water system, as well as retrieving large quantities of personal customer data [24]. In 2018, the Ukrainian security service reported that Kremlin-sponsored attackers targeted their water sanitation system with malware. This allowed the attackers to engage in espionage activities as well as kinetic damage to the water system. It was one of a suite of Ukranian systems affected – from transport, to governmental authorities, and even radiation monitoring systems at the Chernobyl Nuclear Power Plant [25]. Through these cyber-security attacks, water insecurity becomes a tool in geo-political conflict.

Outside of the geopolitical context, attacks are used to create disruptions for a range of reasons from financial gain to social activism. A remote attack at the Maroochy Water Services facility in Australia in early 2000, led to a loss of communication and pump control capabilities, altered the pump station configuration, and set off false alarms. In 2006, a cyber-attack on the Pennsylvania Water Filtering Plant in America gave attackers the ability to alter the concentration levels of disinfectants within the potable water. In another example from the Tehama-Colusa Canal in 2007, a former employee with had an intimate understanding of control systems accessed and damaged the computer system and diverted water to the local farms. In yet another, in 2019, governmental services, including water, in Florida were targeted in a ransomware attack. The attack compromised Riviera Beach Water Utility's computer systems, preventing them from using their pumping stations, water quality testing functions and their payment operations [23].

The diversity of motive, nature and scope of attacks demonstrates a need to be attuned to the possibility of attack across the entire cycle of the water system, materialising in an array of harms. Water insecurities emerge not from the lack of water delivery systems or ability to clean water, but from cross-border political dynamics to malicious actor seeking financial gains. A full understanding of system and human vulnerabilities must therefore be understood and built into the decision-making process, planning and response measures.

3.2 Key cyber vulnerabilities in relation to water

So how do the impacts that have manifested in previous attacks translate into real human harm? Cyber-attacks can result in kinetic effects on critical features of water services, such as the manipulation of flood gates, interference with chemical and water levels and even the diversion of irrigated water. Moreover, where customer information is contained in water systems – the type necessary to get the water from plant to house – it can be remotely retrieved, posing a very real concern for the privacy rights of service users. A distinct set of threats may appear in contrast to the usual anticipated harms of lack of water provision.

As technological innovation is frequently built into existing legacy systems, it is necessary to ensure that retrofitting innovation does not ignore the concern that legacy systems may

include outdated systems vulnerable to infiltration. Where unpatched code remains, innovation measures must seek to actively address and overcome these challenges [26]. SCADA systems which integrate old and new technologies, – industrial business systems and the IoT-cloud system – they become more susceptible to infiltration than the traditional, less advanced SCADA systems [22]. Whilst recognising the advantages that IoT connected systems may bring, they may also include a number of vulnerabilities. These include configuration errors from default factory settings, vulnerability in cloud services, memory corruption and weakness in validating input data, and ultimately the vulnerability of system commands and information to interference [22].

The cumulative result of these vulnerabilities are that the combined integrated systems are at risk of advanced persistent threats; the lack of data integrity where data is destroyed; man-in the middle attacks where the attackers gained illegitimate access or monitors the messages and activities within the system; replay attacks which delay messages sent to physical devices and denial of service attacks which prevents the system from performing tasks by overloading the computer resources [22].

In order to chart the levels and nature of cyber-vulnerability, a focus on the underlying structural issues that may lead to such vulnerability is key. Here, a drive to reduce costs appears to be a motivator to enhance remote sensing and control capabilities of water infrastructures. Does this drive results from a profit focus to drive down costs at the expense of the community and result from an underfunding of the water sector? Understanding why such tools are in place can point to what kinds of mitigation measures are needed to reduce these new risks. Some could continue to be technical, like regular system or sensor updates. Some are political or organisational, including staff training to avoid human error, new regulations to manage silent polluters, or increased government funding [27]. Some require resources for the immediate moment, and others require resources throughout a longer water or pollutant lifecycle. Sufficient attention needs to be paid to the continuing costs necessary to upkeep the cyber security framework. The development of such systems is not a one-off event, and the failure to update both the technology and the socio-economic and political systems that support them may mean that they do not keep pace with the advancement and innovation of malicious threats, reopening water networks to potential harm [26].

Moreover, despite the increasing frequency of cyber-attacks on water networks, the concept remains relatively novel, particularly within the European context. As such, where remote sensing is utilised within the system, the potential for cyber-attacks may not receive adequate attention or investment. In this sense, where the resources are scarce in the first instance, water service providers may be hesitant to invest the necessary funds to safeguard against a vague hypothetical and potentially unrealised threat. As a result, the security concerns must be appreciated by senior staff, or those with decision and investment-making positions, in order to ensure that they are aware of the seriousness of these threats [27].

Technical and organisational measures can be developed to better protect connected water systems. But just as importantly, each new measure put in place to reduce water insecurity shifts the focus and aim of water security. Paul Rosenberg, the mayor for the district in which the compromised Brookman Avenue Dam was located, responded to the attack by taking the dam controls offline, holding that “the risks outweigh the benefits” [28]. As sensors bring geopolitics into view, the needs for more resources shift towards cyber security (away, likely from more marginalised social needs), and focuses water security as an infrastructure problem. Yet, invisible toxicities bring into focus how living conditions and structural inequalities in society, even in wealthy nations, still drive less tangible and democratic water insecurities, vulnerabilities only partially addressed through sensors. How, then, can we use

the lens of vulnerability to better understand what benefits and harms are created by the different measures developed to improve water security?

4 IMPACT ASSESSMENTS

This section outlines ways to sensitise water service providers, policy makers, and technology designers to the ethical and human rights challenges of water security, and how to better assess the proportionality of the risks and benefits in their security frames. Drawing on the methodology of an Ethical and Privacy Impact Assessment, it provides a structured and reflexive approach for identifying and assessing risks, as well as developing recommendations to be considered and actioned where possible within system innovation and development. Within the European Union, Privacy Impact Assessments and Data Protection Impact Assessments are often compulsory under the General Data Protection Regulation in order to demonstrate compliance with the legal and regulatory requirements. Such practices are now widely used across the globe [29]. Increasingly, similar processes are being used to capture a broader array of considerations, including ethical impact assessments and societal impact assessments [30], [31].

Building from an E/PIA provides a distinct avenue to include conversations around individual and diverse community insecurity into technology and policy decisions, thereby attuning decision-makers to these considerations so they can recalibrate their ideas to their potential real-world impacts on diverse populations and any disproportionate impacts on individual's rights [32]. To support such a process, we propose a set of questions, based on the themes, overlaps, and disparities between the discourses in western water insecurities and water security solutions we present here.

These questions have no right answers but help make visible and transparently engage with what may otherwise be morally opaque at first glance [33]. They require a reflexive ability to grapple with the particulars of each setting, porous to the dynamic range of issues. By starting with such questions for an E/PIAs framework, they can contribute towards informed decision-making, protection of societal concerns, and overall effective risk management strategy [34]. These questions intend to uncover some of the key vulnerabilities of populations and indeed the water sector as a whole.

1. What are the fundamental vulnerabilities to water insecurity that the innovative system is trying to protect and how does the innovation prevent or reduce these vulnerabilities?
2. To what extent is information on the local population disaggregated to include characteristics such as gender, age, class, disability to appreciate their particular vulnerability and resilience to water insecurity?
3. How do these characteristics influence how individuals/communities interact with the water system?
4. How do water system's response measures seek to protect a particular area, sector, site, or community at the expense of another? If so, how is this prioritisation calculated and what are the potential human impacts of this prioritisation?
5. What are the human impacts if a community or responsible authority have sufficient resources to take advantage of the solution?
6. To what extent do the processes used to identify and evaluate risks to the water network also contain information on the vulnerability and resilience of the population against such risks?

7. What are the human impacts that can arise from cyber-attacks? Does the potential for these impacts out-weight the existing water security threats that the system is trying to mitigate (taking into account the specific harms/burdens per community outlined in Question 2)?
8. To what extent are there sufficient resources for training personnel and updating systems to safeguard against the new vulnerabilities arising through the solution?
9. Have compounding harms that arise for the simultaneously disruption of other critical infrastructures and socio-economic activities been mapped?
10. How does the system adjust to accommodate new knowledge regarding potential threats to communities or individuals (e.g. increased awareness on new forms of pollutants and new forms of cyber-attack)?
11. What are the mechanisms for policy change or accountability to address and change the root causes of water insecurity?

5 CONCLUSION

This paper adopts an anthropocentric view of the impacts of water insecurity. Nevertheless, the proffered impact assessment model can be tailored to other referent objects, such as the environment or agriculture, recognising both these objects' innate worth and need for protection from pollution and the complexity of how to define and articulate risks of water-based harms. Ultimately, such an approach provides for a holistic understanding of water security making it possible to anticipate and prevent harms from occurring in the first place. With such a perspective, mitigation measures for water pollution can be better designed to addresses underlying causes and drivers, and in doing so informs effective and responsive measures and responses.

Putting vulnerabilities into conversation with technological solutions makes visible how water security is a right that looks beyond the flow of water between source to a view that interconnects international, local, human, environmental, economic, and political concerns [4]. Understanding the social, economic, political context of technology adoption, particularly the complexities barriers, can make visible the indirect impacts that have differential effects yet shape both the concept of water security as well as the vulnerabilities that water security addresses [35].

The vulnerabilities that arise with increasing innovation in the water sector have resulted in a recalibration of how we look at the threat of water insecurity in the European context. They show how a new technological solution to one problem (networked sensors to detect chemical threats, a common and diversely experienced water vulnerability at the community and individual scape) can shift the view to a state and political sense of security (facing new threats from geo-political dynamics). As the threat of cyber-attack looms larger, we must be aware of how humans can be affected in their unique contexts, the new drivers of harm (for instance, as geo-political dynamics are introduced into the critical infrastructure ecosystem), and how we should prioritise our resources to address these threats. At its core, increasing innovation in the water sector demands a clear understanding of the proportional risks, based in an appreciation of marginalised people and communities and capable of ensuring that their voices and concerns are factored in responses.

These particular concerns can be better identified and addressing by engaging in a meaningful ethical impact assessment process. Starting from reflexive questions, ones without rights or wrongs but that pose dilemmas or interrogate assumptions, can make visible to all what goes into a water security measure; and as importantly, what and who is left out.

They make it possible to better articulate why decisions get made, understand what kinds of policy pathways are necessary for supporting change, help identify new risks that might emerge, and make visible what might be otherwise further masked.

Fundamentally, when considering how water pollutants should be measured and addressed, we must steep this understanding of the human context. A pollutant detection system will ultimately be human-agnostic, measuring chemical makeup without reference to the fact that the resultant water insecurity risks are not equally distributed across societies. Indeed, new technologies to monitor pollution can even reshape what risks water pollution potentially poses. The adoption of an impact assessment can help to bring in this contextual analysis. Moreover, as highlighted within Section 2, pollutant-based harms occur on an intersection of cross-cutting behaviours, events and structural dynamics that dictate harms' scope and severity. The impact assessment methodology can help to develop an appreciation of how innovations interact with these relationships and other harms that arise from separate areas (such as privacy). Finally, developing this intersectional insight can bring community voices into the equation. In this respect, it is possible to complement current expert-led approaches to water insecurity with bottom-up participatory measures. Consequently, our understanding of water pollution can develop a well-rounded picture of its context, which in turn will help both assess and prioritise innovations and policy, as well as tiers of harms.

REFERENCES

[1] United Nations, UN Analytical Brief: Water Security and the Global Agenda, 2013. https://www.unwater.org/app/uploads/2017/05/analytical_brief_oct2013_web.pdf.

[2] Maganda, C., Water security debates in 'safe' water security frameworks: Moving beyond the limits of scarcity. *Globalizations*, **13**(6), pp. 683–701, 2016.

[3] Security Research Community of Users, Water Security and Safety, CoU Brief, no. 2, Mar. 2018.

[4] Scocca, G., Strengthening international water security: The European Union's proposal. *World Water Policy*, **5**, pp. 192–206, 2019.

[5] Zeitoun, M., *The Web of Sustainable Water Security, in Water Security: Principles, Perspectives and Practices*, Routledge: London, pp. 11–25, 2013.

[6] EurEau, The Need for Greater EU Policy Coordination Realising the Water Framework Directive, 16 May 2017. http://www.eureau.org/resources/position-papers/140-greater-eu-policy-coordination-may2017/file.

[7] Wouters, P., Water Security: Global, regional and local challenges, Institute for Public Policy Research (IPPR), 2010.

[8] Bakker, K. & Morinville, C., The governance dimensions of water security: a review. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, **371**, 2013. http://doi.org/10.1098/rsta.2013.0116.

[9] Vörösmarty, C., et al., Global threats to human water security and river biodiversity. *Nature*, **467**, pp. 555–561, 2010.

[10] Garrick, D., et al., Water Security, Risk and Society – Strategic Report on Research Findings, Gaps and Opportunities, Submitted to the Economic and Social Research Council by Oxford University Water Security Network, 2012. www.water.ox.ac.uk.

[11] Dillon, L. & Sze, J., Police Power and particulate matters: Environmental justice and the spatialities of in/securities in U.S. Cities. *English Language Notes*, **54**(2), 2016.

[12] Cordner, A., et al., Guideline levels for PFOA and PFOS in drinking water: the role of scientific uncertainty, risk assessment decisions, and social factors. *Journal of Exposure Science and Environmental Epidemiology*, **9**, pp. 157–171, 2019.

[13] European Environment Agency, Emerging chemical risks in Europe -PFAS, Briefing no. 12/2019, 2019. https://www.eea.europa.eu/themes/human/chemicals/emerging-chemical-risks-in-europe.
[14] Graversgaard, M., et al., Opportunities and barriers for water co-governance—a critical analysis of seven cases of diffuse water pollution from agriculture in Europe, Australia and North America. *Sustainability MDPI*, **10**(5), pp. 1–39, 2018.
[15] Guelfo, J.L. et al., Evaluation and management strategies for per- and polyfluoroalkyl substances (PFASs) in drinking water aquifers: perspectives from impacted U.S. Northeast communities. *Environmental Health Perspectives*, **126**(6), 2018.
[16] Katner, A., et al., Weaknesses in federal drinking water regulations and public health policies that impede lead poisoning prevention and environmental justice. *Environmental Justice*, **9**(4), pp. 109–117, 2016.
[17] Hale, M., Fountains for environmental justice: Public water, homelessness, and migration in the face of global environmental change. *Environmental Justice*, **12**(2), pp. 33–40, 2019.
[18] Boudia, S. et. al., Residues: Rethinking chemical environments. *Engaging Science, Technology and Society*, **4**, pp. 165–178, 2018.
[19] Collins, M., Munoz, I. & Jaja, J., Linking "toxic outliers" to environmental justice communities. *Environmental Research Letters*, **11**(1), 2016.
[20] Curran, D., Environmental justice meets risk-class: The relational distribution of environmental bads. *Antipode*, **50**, pp. 298–318, 2018.
[21] Sammaneh, H. &. Al-Jabi, M., IoT-enabled adaptive smart water distribution management system. *International Conference on ICPET Promising Electronic Technologies (ICPET)*, pp. 40–44, 2019.
[22] Sajid, A., Abbas, H. & Saleem, K., Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, **4**, pp. 1375–1384, 2016.
[23] Hassanzadeh, A., et al., A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, **146**(5), 2020.
[24] Tsagourias, N., Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, **17**(2), pp. 229–244, 2012.
[25] Martin, A., Russian hackers targeted Ukraine's water supply, security service claims, *Sky News*, 11 Jul. 2018. https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826. Accessed on: 17 Apr. 2020.
[26] Adepu, S., et al., Investigation of Cyber Attacks on a Water Distribution System, ArXiv abs/1906.02279, 2019.
[27] Germano, J. H., Cybersecurity Risk and Responsibility in the Water Sector, American Water Works Association, 2018.
[28] Esposito, F., Westchester village finds clever solution to thwart hacking of critical infrastructure, *Rockland/Westchester Journal News*, 8 Jan. 2020. https://eu.lohud.com/story/news/local/westchester/rye-brook/2020/01/08/iran-hacked-rye-brook-dam-2013/2846127001/. Accessed on: 17 Apr. 2020.
[29] Wright, D. & Friedewald, M., Integrating privacy and ethical impact assessments. *Science and Public Policy*, **40**(6), pp. 755–766, 2013.
[30] Wright, D., Ethical impact assessment. *Ethics, Science, Technology and Engineering: A Global Resource*, eds J. Holbrook & C. Mitcham, 2nd ed., Macmillan Reference: Farmington Hills, 2015.

[31] Kush Wadhwa, K., Barnard-Wills, D. & Wright, D., The state of the art in societal impact assessment for security research. *Science and Public Policy*, **42**(3), pp. 339–354, 2015.
[32] Carroll, J.M., Five reasons for scenario-based design. *Interacting with Computers*, **13**, pp. 43–60, 2000.
[33] Brey, P., Disclosive computer ethics. *Computers and Society*, **30**(4), pp. 10–16, 2000.
[34] Kloza, D et al., Data Protection Impact Assessments in the European Union: Complementing the new legal framework towards a more robust protection of individuals, d.pia.lab Policy Brief No 1/2017, 2017.
[35] McDonnell, R. et al., Water Security, Risk and Society – Knowledge Exchange Opportunities for UK and European Agencies, Briefing note submitted to the Water Security Knowledge Exchange Programme by Oxford University Water Security Network, 2012. www.water.ox.ac.uk and www.wskep.net.