Reconfiguring governance: How cyber security regulations are reconfiguring water governance

Ola Michalec
Faculty of Engineering, Bristol Cyber Security Research Group, Bristol, UK

Sveta Milyaeva
School of Sociology, Politics and International Studies, The University of Bristol, Bristol, UK

Awais Rashid
Faculty of Engineering, Bristol Cyber Security Research Group, Bristol, UK

Abstract

Developments in improved monitoring, asset management, and resource efficiencies led to the water industry promising a step-change in the design and operation of these facilities: the “blending” of traditional engineering equipment with digital technologies. These apparent benefits inevitably produce new challenges of regulating an emerging techno-political landscape. One of the regulations is Europe’s Network and Information Systems Security Directive, which aims to improve cyber security across critical infrastructure providers. This paper focuses on the implementation of Network and Information Systems in the context of the water sector in England. At the national and supranational levels, Network and Information Systems acts as a boundary object that gathers diverse communities of practice without the need to establish common goals. Further, in the process of transposing the Directive into the sectoral context, Network and Information Systems requires interpretation by expert communities. We show how translating the regulatory scope to the sectoral landscape involves prioritizing some water governance goals over others. As diverse expert communities converge in their collaboration practices, their priorities align or stand in tension with public interests. We argue that cyber security regulations have potential to reconfigure water governance by refocusing strategic priorities away from traditional concerns of environmental governance. We suggest ways to maintain diverse collaborations across engineering, computing, and water expertise that Network and Information Systems implementation remains aligned with the goals of water governance.

Keywords: critical infrastructure, cyber security, expertise, regulation, science and technology studies.

1. Introduction

In their foundational work, Bowker and Star (1999), p. 35, characterize infrastructure as “visible upon breakdown.” To this day, this remains the most concise and apt observation of pipes, power lines, and sensors. The possibility of breakdown – whether through safety accidents, cyber security attacks or the repercussions of climate change – has put infrastructure and its studies in the spotlight (Rowland & Passoth 2015; Musiani et al. 2016; O’Grady 2020). Adding to that, infrastructure breakdowns make dramatic headlines in the news: a recent example of Florida water facilities incident illustrated that a remotely executed cyber security attack could disrupt public safety and poison thousands of people by barely changing the decimal points in the concentration of water treatment chemicals (BBC 2021). But how do we see what infrastructures are made of without waiting for them to break down? How do we know what goes into making infrastructures, what regulates therefore shapes them?

Of a particular importance are so-called critical infrastructures: services, resources, people, and equipment deemed essential for the society to function (Aradau 2010). Defining criticality and prioritizing certain assets over
others is a matter of contestation; however, critical infrastructures are usually found in sectors like water, energy, transport, health, etc. (Engels 2018). Critical infrastructures are typically operated by a combination of Information Technologies (IT) and Operational Technologies. While IT are concerned with data and information, OT are concerned with engineering assets. To further help with the distinction, we can think of OT as an umbrella term for computer systems controlling pumps, valves, sensors, MRI scanners, train tracks, to name a few (Cherdantseva et al. 2016). Traditionally OT systems were built for reliability and endurance; by design, they are less complex compared to computers at offices or homes. However, developments in improved asset management and operational efficiencies are promising a step-change in the design of these infrastructures. In other words, OT and IT are dubbed to be “blending” (Cisco 2018). With all facilities connected to the public Internet and monitored in real-time, infrastructure operations will enter a new era – at least that is the IT sector’s vision (International Water Association 2019).

Not only the technologies are blending, so are the expert communities and regulatory domains. The proposed intersection of IT, OT, and water expertise is the focus of this paper. Indeed, this anticipated modernization creates a unique regulatory gap, where there is a requirement for multiple communities and policy areas to converge (van Veelen et al. 2021). Policymakers are drawing expertise from the IT, OT, and sector-specific practitioners to ensure that the modernization of OT systems is undertaken in the public interest. And so, calls for the regulation of emerging digital technologies encompass novel considerations and domain applications. From security and privacy (Carr & Tanczer 2018), through financialization (Loftus et al. 2019) to sovereignty and justice (Noble 2018), emerging digital technologies and their regulation have the potential to significantly reconfigure human relationships and institutional powers. These technologies create regulatory challenges, not only through unforeseen consequences, but through uncertainty over who can regulate and what expertise is needed (Lewallen 2020). As a result, with the emergence of digital regulations, traditional areas of governance (like water, energy, transport) face the possibility of new actors, relationships, and strategic priorities.

One example of such a regulatory effort is the EU Network and Information Systems (NIS) Security Directive aiming to raise the baseline level of cyber security across critical infrastructure sectors (European Commission 2016). NIS is already creating converging pressures on critical infrastructures; it requires rapid recruitment of large numbers of OT security experts against the backdrop of insufficient standardization (Michalec et al. 2020). Since 2018, NIS Directive has been transposed to the EU Member States and the UK as NIS Regulations (DCMS 2018). This move meant that while high-level objectives and international cooperation mechanisms were set by the EU, the scope of what’s regulated as well as implementation mechanisms are decided by each state individually. Transposing the directive into the national context, combined with rendering NIS’ scope relevant to the sectoral issues makes a decisive moment for the future of digitization. After all, the interpretations of NIS will ultimately shape what gets digitized, protected and whom this transformation will serve. As the regulatory implementation is currently underway, paying attention to the converging expert communities can potentially shed a light on what goes into the black box of NIS and how OT and IT expertise aligns with public interests.

The aim of this paper is to shine the light on the emergence of the technical expertise and collaborative practices as key to the regulatory implementation. The novelty of this paper lies in analyzing technological (cybersecurity) regulations jointly with environmental regulations, acknowledging their co-production (Jasanoff 2004). To do so, we followed the OT security professionals in their efforts to implement the NIS Directive as illustrated with the case of water governance in England. Despite being regarded as a common good, water has been a subject to privatization since the 1980s, which claimed to protect the public interest (Loftus et al. 2019). The regulatory oversight of the digitization of this infrastructure leads to question how NIS is re-configuring the notion of water infrastructure itself. More specifically, if provision of water is a matter of public interest, what about the protection of industrial facilities, algorithms and data surrounding it? In analyzing the notion of governance, we take on board its conceptual fluidity and multiple meanings across disciplines (Rothstein et al. 2013; Slayton 2020). For our analysis, we understand governance and its outcomes (i.e., regulations) as actions and actors aiming to achieve specific goals pertaining to the protection of public interest. Theoretically, the paper brings scholarship from Science and Technology Studies (STS) to address the challenges of regulation at the intersection of digital technologies and environment.

Following the studies of internet infrastructure governance (e.g. DeNardis 2014; Musiani 2015; Musiani et al. 2016; Brass & Sowell 2020), we argue that the scope of NIS reaches far beyond the technical protection of...
engineering equipment from cyber security incidents. The governance of digital technologies occurs at “infrastructural control points, around which are entangled matters of technical and economic efficiency, as well as mediations over human and societal values” (Musiani 2015, p. 275; DeNardis 2014). As such, NIS has important political ramifications by shaping the direction of digitization in the water sector. Using the concept of boundary objects (Bowker & Star 1999), we examine how NIS enables cooperation across divergent expert communities: OT workers, IT practitioners, water experts. The ways they negotiate their priorities constitute the core practice of NIS implementation. How NIS will reconfigure the meaning of water depends on the opportunities to align technical expertise with the goals of water governance. We, therefore, analyze digital infrastructure regulations in conjunction with its sectoral context. If water is a common good, what are the implications of cyber security regulations for the future of water itself?

2. The goals of water governance

Water in England\(^1\) is regulated by two authorities: the economic regulator Ofwat and the water quality assessor, Drinking Water Inspectorate (DWI). Ofwat determines the spending and the profit operators can make by, for example, overseeing the level of investment in equipment upgrades. DWI audits the quality and sufficiency of drinking water supplies and deals with incidents potentially affecting water provision. This seemingly sanitized arrangement does not reveal much about the contested and value-laden character of water provision. To shed a light on this, we reviewed strategic policy documents (Table A1) to locate the goals of contemporary water governance. We identified that the following six priorities influence the provision of drinking water in England: safety (i); continuity of supply (ii); affordability (iii); sustainability (iv); economic efficiency (v); and broad participation (vi). However, there is an ongoing debate about the “correct” ways to embed such high-level priorities in the regulatory practices. The presence of these debates confirms that despite the attempts to turn water governance “post-political” (Swyngedouw 2010), the field is riddled with negotiations and tensions. Water governance scholars have extensively studied policy transitions, highlighting the need to protect the public interest and embed the values of justice, resilience, or sustainability in an increasingly corporatized setting present across multiple Global North countries (Lankford et al. 2013; Sultana & Loftus 2013). For example, Linton (2010) highlights the relational and coproductionist aspects of water, technology, and society. Water is not a fixed entity, rather “water becomes what it is in relation to other things and processes, it is what we make of it” (Linton 2010, p. xv). Other scholars argue that although there is a consensus that water is both a human right and a scarce resource to protect, the ongoing regulatory changes within the sector could transform critical infrastructures into primarily wealth generating businesses (Loftus et al. 2019). Indeed, the reviews of water governance mechanisms present in England (public-private partnerships, economic regulation) have not found the evidence that they are sufficient to protect the public interest and achieve the goals of water governance (Seppälä et al. 2001; Bayliss 2017). Instead, the water sector observed a rising trend of financialization – the transformation of material assets (pipes, plants, sewers) into “liquid assets,” enabling opportunities for short-term wealth extraction at the expense of public interest (Loftus et al. 2019).

3. Promises and consequences of digital water

The intricacy of water governance becomes even more complex when we look at water infrastructure. These facilities are often outdated (Mansfield-Devine 2019), and in comparison with other critical infrastructures (e.g., energy or aviation), “digital water” does not equate with “smart water”: datasets and equipment are yet to reach interoperability while behavioral insights on water consumption are far from comprehensive (Lloyd Owen 2018). As a result, about 20% of drinking water is leaking through pipes (EurEau 2017), water sensors yield poor quality data, and slow adoption of household metering in the UK means that water companies are not aware of the consumer usage figures (Michalec et al. 2019).

The potential applications of novel digital technologies and the promises they carry are burgeoning. For example, the Industrial Internet of Things (IIoT) could optimize the performance of pumping systems, machine learning algorithms could detect leaks, digital twins would be used for improved imaging of the underground pipe network, and smart metering, for household demand management (International Water Association 2019).
With this level of ambition, it is not surprising that practitioners are enthusiastic about the so-called “IT-OT blending” (Cisco 2018).

The pressure to digitize water infrastructure means that water governance is subject to legislation which falls outside traditional environmental governance. The novel governance challenges tackle the questions of privacy, security, datafication, the increased carbon footprint from ICT, surveillance, monopolization, just to name a few (Moy De Vitry et al. 2019). They complicate and reconfigure known water regulations. The “unintended consequences of policy” (Merton 1967) – the idea that particular regulations might unwittingly impact policy areas beyond the original scope – has been challenged by the science and technology (STS) scholars who showed that they can be anticipated and mitigated against by the analysis of expertise and regulations “in making” (Garfield 2004; de Zwart 2015). What we argue here is that cyber security regulations might affect not only cognate issues of privacy and surveillance, but also have impacts on sustainability, democracy, and the economy. From solidifying new commercial partnerships, through diverting funding from other policy areas, to accelerating the adoption of emerging technologies, cyber security regulations re-shape how water is governed.

4. Regulating digital water: A case of NIS directive

So, what is the cybersecurity governance that oversees (and we argue makes) digital water? As the number of components connected to the Internet (and each other) is rising in the quest for ever increasing data collection, so is the so-called attack surface (Rashid et al. 2019). To mitigate this, the EU introduced a new cyber security directive in 2016 (European Commission 2016). The Network and Information Systems Security Directive (NIS) aims to improve a baseline level of cyber security across the essential services, such as energy, water, transport, health etc. In the UK, four objectives of NIS are: to manage cyber security risks, to protect against cyber security attacks, to detect cyber security events, and to minimize the impacts of cyber security incidents (NCSC 2019).

The EU member state as well as the UK after leaving the EU are currently implementing the NIS Directive, after transposition to national legislations in 2018 (European Commission 2016). At the EU level, NIS Directive (European Commission 2016) is written in a sector agnostic, top-down way but the implementation is devolved to sector-specific authorities publishing their own NIS regulations and implementation guidelines (i.e., DWI 2019). This situates NIS at this convergence of IT, OT, and sectoral expertise, as these professional communities are required to collaborate effectively despite potential differences in jargon and agenda. Indeed, risk management at an organizational level by necessity involves difficult tradeoffs and a degree of legal flexibility with regards to assessing “appropriate and proportionate” measures (Michels & Walden 2018).

NIS is work-in-progress. At the time of writing (April 2021), NIS is being implemented in sectors and organizations the UK government deemed “essential,” and regulatory bodies called “Competent Authorities” oversee the process. In the water sector, it is the Drinking Water Inspectorate, and their current responsibility is to provide guidance and ensure the appropriateness and proportionality of security measures (Michels & Walden 2018). Throughout 2020, Water companies submitted their self-assessment forms (known as “Cyber Assessment Framework” – CAF; an example for the water sector can be found here: DWI 2020a) and agreed on improvements and investment plans to upgrade their digital assets in a secure way (Shukla et al. 2019). These documents are “principles-based regulation tools,” meaning that companies work toward meeting the governmental objectives rather than being told which steps to take to meet these objectives. (Michels & Walden 2018) Over the next few years, Competent Authorities will conduct external audits and provide OT security training to the critical infrastructure (Wallis & Johnson 2020).

To render more complexity, the implementation of NIS occurs against the backdrop of the evolving UK cyber security policy landscape as well as the UK’s exit from the EU. the UK cyber security strategy is currently driven by domestic security, ambition to grow the cyber security sector and the UK playing the role of the global cyber security leader (Carr & Tanczer 2018). Despite common associations of cyber security with intelligence and defense agencies, this policy area has profound effects on the whole spectrum of the society from transport, public health, through finance, and innovation (O’Grady & Dwyer 2020). What’s more, each time cyber security is prioritized in the government budget, it leads to the creation of new partnerships between the state and private businesses (Wallis & Johnson 2020; Carr 2016; O’Grady and Dwyer, 2020). This means that public-private partnership is a leading mode of governance in critical infrastructure cyber security (Carr 2016; Topping 2019).
et al. 2021), with apparently successful public–private partnerships characterized by the alignment of interests and clear responsibilities of various experts involved in the governance activities (Carr 2016). The alignment between water and digital governance as well as the collaboration between the experts are the main matters of concern of this paper.

5. Who are cyber security experts?

Traditional approaches view cyber security expertise as either a matter of “exogenous” technical knowledge and solutions, or an expression of international diplomacy (Dunn Cavelty 2018). In contrast, following the STS and Computer-Supported Cooperative Work (CSCW) scholarship, we insist on the relational, dynamic and value-laden nature of cyber security expertise (Ashenden & Sasse 2013; Shires 2018; Slayton & Clark-Ginsberg 2018). Shifting from organizations and states to the practitioners and their practices (Kocksch et al. 2018; Matthew & Cheshire 2018; Jenkins et al. 2020), these studies of expertise are focused on the relationships between the technologies, the people, and their environment. Callon’s (1998, 2007) concept of a sociotechnical assemblage is helpful here as it refers to a heterogenous agency and its capacity to enact a particular reality, in this case “digital water.” In the context of NIS implementation, the assemblage of legal, cybersecurity, and water sector experts; their tools (including conceptual tools their expertise); technological devices; and documents highlights the interdependences between the need for cyber security, emerging technologies, and competencies required from the community of practitioners (Michalec et al. 2020). In our understanding, the instances of collaboration on NIS are sociotechnical assemblages, as they highlight the inseparability of actors and technologies.

6. Objects of collaboration

The making of cyber security expertise in critical infrastructures has not received sufficient attention, with notable exceptions of Slayton and Clark-Ginsberg (2018), who pointed out the tension between Operational Technology (OT) and Information Technology (IT) experts in the context of the US history of critical infrastructure protection. Experts in OT emphasized the importance of reliability, safety and 24/7 availability of critical infrastructures. This stood in tension with the IT experts interviewed: those practitioners favored privacy, security, accuracy, and recovery of data over other priorities.

Nevertheless, critical cyber security scholars highlighted the impressive variety of practitioners working in critical infrastructures and its regulatory environment – lawyers, engineers, civil servants, salesmen, consultants, and senior managers to name a few (Haines 2011; Slayton & Clark-Ginsberg 2018; Stevens 2020). But, when it comes to regulation of technologies, the phenomenon of “expertise asymmetry” is often encountered, where the specialized knowledge lies within the infrastructure operators, which leads the delegation of regulation away from the public sector administration (Downer 2010; Spinardi 2019). For technical practitioners to communicate successfully outside their narrow domains, there need to be ways of mobilizing security knowledge through shared standards and governance goals (Barry 2006). Such collaboration, we argue, is enabled through cyber security regulations acting as boundary objects – information, documents, and concepts assembling the community of practice around a focal point (Star & Griesemer 1989). Boundary objects are information structures enabling collaboration; they are used in different ways by different communities; yet maintain some sort of constant identity (Star & Griesemer 1989). Practitioners gather around boundary objects and hold debates about high-level strategies, enabling cooperation across multiple social worlds without necessarily achieving consensus on the fine detail (Star 2010). Conceptually, the scholarship on “boundary objects” draws from symbolic interactionism seeking to understand communication practices surrounding the perspectives of actors belonging to multiple and heterogeneous social worlds (Trompette & Vinck 2009). In the context of NIS implementation, it is crucial to account for the worlds of IT, OT, water experts, and policy makers. By analyzing collaboration practices of multiple experts, we show that the digital water governance is a heterogenous assemblage enabled, among other things, by NIS as a boundary object in its capacity to be a space that accommodates collaboration through translation. As Star (2010) insightfully points out, with time, communities and meanings within boundary objects solidify, translating selected priorities into formal standards. Indeed, these successful translations across various expertises
are the evolution of NIS from a boundary object to an early version of what could be considered a formal standard: sector-specific Cyber Assessment Frameworks (CAF).

The vagueness of boundary objects has a pragmatic advantage in communication as it allows for fruitful disagreements across disciplines and communities of practice; it serves as a common reference point. Furthermore, boundary objects help to form professional identities by acting as gatekeepers that selectively filter information between the organizations (Bharosa et al. 2012). We treat NIS as a boundary object following the multiple ways our interviewees justify it, highlighting that multiplicity is crucial as people simultaneously belong to multiple communities of practice and they do so at different rates of commitment and competency (Bowker & Star 1999). There is an implicit egalitarianism involved in this conceptualization (Bowker & Star 1999). However, this alone does not guarantee a successful or long-standing collaboration.

Star (2010) argues that collaboration takes places in a cyclical fashion: with time, existing boundary objects become translated into formalized standards (Fig. 1). Once actors gather around a boundary object, they need to move between the flexibility of interpretation and translation of their expertise into standards to advance their goals. However, once established, each standard leaves out unaccounted “residual categories” around which new boundary objects form. Translation of expertise occurs across communities of practice as well as between the epistemic communities of researchers.

We understood translation as a *passage of something to another place where previously it was not* (Stritzel 2011, p. 344). Translation focuses on far more than merely “transporting” meaning; it is a creative co-construction of new meanings and new contexts. Translation opens analysis on to the travel, localization and evolution of security concerns; it highlights that what it means to be secure changes over time, place and depending on who is argues it (Stritzel 2011). In our case study, translation of cyber security expertise is central to our thinking as we are concerned with diverse communities of practice: lawyers, engineers, software engineers, OT

![Figure 1](image_url)
security specialist, IT security professionals, and water engineers. Multiple understandings of the “best practices” and “top risks” travel between technical experts, senior executives, and regulators, each time shifting the conversation to new concerns present locally.

7. Conceptualizing research at the boundary

Focusing on security experts’ practices of positioning cyber security regulations within their sector-specific knowledge, we investigate how NIS practitioners perform tensions and alignment between the goals of water governance and goals of cyber security. We also conceptualize NIS directive as a boundary object: an arena for diverse practitioners to cooperate and negotiate implementation of the cyber security regulations. To operationalize this concept in further analysis, we suggest the following: first identifying water governance goals at stake (Table A1). Second, analyzing how practitioners cooperate on the implementation of regulations. Finally, investigating instances of collaboration which hinder or help with alignment between water governance goals and cyber security goals.

Using NIS as a focal point of analysis, we interviewed 30 cyber security experts, namely industry regulators, consultants, lawyers, site engineers, hardware manufacturers, software vendors, and project managers. We used a snowball recruitment technique (Sadler et al. 2010), starting from our professional networks and attendance at cybersecurity events. All our informants were based in England and our interviews were conducted in person. We wanted to collect the accounts of cyber security practices - cyber security improvements, equipment upgrades and the introduction of emerging technologies. In order to investigate how NIS enabled collaboration, we followed Star’s (2010, p. 605) advice and paid attention to interviewees’ discourses, for example, “the special language used in the location, metaphors, mots justes, turns of phrase, private codes used by one group and not another things that strike them [the researcher] as strange, weird, and anomalous.” This enabled us to trace which communities perceived themselves as aligned and which ones – in conflict. Table 1 summarizes the interview topic guide. We conducted the interviews between October 2019 and January 2020; conversations lasted between 40 and 90 minutes. We complemented our data with an observation of the following industry events: a manufacturer-led workshop on opportunities IIoT could bring to the water sector (November 2019) and an invitation-only working group on safety and security standard for water SCADA equipment, led by the UK water suppliers (January 2020).

Interview transcripts and event memos were coded using qualitative data analysis software. Our approach to integrating the insights from different types of qualitative data was informed by thematic analysis (Guest et al. 2011). Open and inductive coding allowed focusing on the trajectories of digital transformation in the water industry as well as the instances of interpretation practitioners are required to do (e.g., translation between IT and OT worlds, sector-specific vs. generic guidance). In our analysis, we pay attention to the divergence between

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Topic guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Story of OT security in your sector/organization: How did OT security look like before NIS, what has NIS changed in comparison?</td>
<td></td>
</tr>
<tr>
<td>2. Story of your career: How did you get into security? How did your previous roles influence your current job?</td>
<td></td>
</tr>
<tr>
<td>3. Situating security in a sector-specific context: What are the typical security concerns, regulations, technologies and procedures in your sector/organization?</td>
<td></td>
</tr>
<tr>
<td>4. Standards and regulations: How do you apply industry standards and security policies in your organization? How to ensure they are applied successfully?</td>
<td></td>
</tr>
<tr>
<td>5. Experiences from NIS: How do you understand NIS guidelines? What are your opinions on it? How have you been implementing NIS so far?</td>
<td></td>
</tr>
<tr>
<td>6. Investments and innovations in your organization/sector: What are your plans for the next few months/years with regards to improving security? How will NIS influence your future investments?</td>
<td></td>
</tr>
<tr>
<td>7. Communicating OT security in your organization/sector: How should we communicate across IT-OT divide? How should we communicate between the board members and the technical experts?</td>
<td></td>
</tr>
</tbody>
</table>

© 2021 The Authors. Regulation & Governance published by John Wiley & Sons Australia, Ltd.
the goals of strategic documents and the actual “nitty-gritty of cyber security policy-making” (Möllers 2020, p.7). While senior political officials make broad normative decisions about what should matter, experts and organizations implementing regulations might hold other (sometimes conflicting) understandings.

8. Water governance as cyber security governance

There are multiple strategic priorities that, in one way or another, influence the governance of the water sector. Here we suggest looking at how the strategic priorities were enacted by the cyber security practitioners in their day-to-day work. One of the most common goals shared by the water and cyber security experts is “safety of supply,” with safety being a part of “the OT engineers’ DNA” (IoT Manufacturer) or “engineering philosophy” (OT Security Manager at a Water Company). Although health and safety regulations pertain to the whole sector, it’s the engineers’ responsibility to understand, interpret, and implement them. What becomes clear is that the notion of safety is contingent on the OT practitioners’ expectations formed by their daily experiences of managing and maintaining the operational infrastructure. For example, “continuity of supply” in participants’ view is linked to safety as cuts in supply are detrimental to human health. However, unlike power supply cuts, the impact of water supply cuts unfolds in slower timescales:

Anything that happens in rail or transport or energy will hit the media faster than it will in the water sector. (...) If you lose energy, the impact on people is instant, isn’t it? In the water industry, the problem is never immediately because I have thousands, millions of gallons of water already pre-treated and held in reservoirs. (Security Consultant)

Water affordability is another priority guiding the sector. However, the presumed “IT-OT blending” is explicitly acknowledged as being in conflict with the goal of affordability. The maximum prices of water and, therefore, the spending and the profits operators can make, are controlled by the Water Services Regulation Authority (Ofwat) that is in charge of the economic regulation of the water sector. However, another regulatory body, the Drinking Water Inspectorate (DWI), in its overseeing the quality of drinking water and NIS implementation, expects costly upgrades to digital systems as a part of NIS (DCMS 2020). This conflict was particularly visible in the early stage of NIS implementation: water suppliers were required to provide proposals of cyber security investments in early 2020, which was too late to align it with the five-year price review timescales.6 One reason for this misalignment would seem to be a lack of an established collaboration between Ofwat and the cyber security division of DWI, and in the words of one of the DWI’s employees, acknowledged as an obstacle: “We will have to get very friendly with Ofwat” (Regulator 1).

The “economic efficiency” goal is another moot point. While OT cloud computing or the Industrial IoT promise improved efficiency and optimization, currently the water sector practitioners do not consider them secure.7 Furthermore, there is not enough clarity whether these technologies would fall under the scope of NIS or seen as a responsibility of supply chains8 (Wallis & Johnson 2020). There is a risk that the development of digital technologies will be outsourced away from the water sector and in the direction of digital service providers, whose priorities differ from those of water governance.

There are also water governance goals that would not seem to be at the forefront of cyber security professionals’ minds: sustainability and broadening participation. For example, the Drinking Water Inspectorate (DWI), traditionally regulated the quality of water, has recently become responsible for compliance with NIS Regulations. When prompted about how often they think about environmental issues, a DWI water regulator replied: “Probably not at all – probably later in the role. At the moment you’re just so buried in the weeds, aren’t you?” (Regulator 1). Meanwhile, the goal of broadening participation, traditionally understood as the involvement of citizens in water planning, was not considered this way by cyber security professionals in the water sector. The calls for broadening participation in cyber security usually refer to diversifying recruitment and improving communication across technical staff and members of the board. Yet, cyber security is not seen as a matter of concern for a water consumer. While the lay users are not yet included in the conversations about data privacy and security, this topic is expected to gain more attention with the advent of IoT smart home gadgets and smart water meters. As one water supplier remarked:
Water sector data fall in various places on the spectrum between physical to social, for example metering is clearly seen as a social dataset, but what about sewage? If you are flushing illegal drugs, this could be used as evidence in court if linked to your address. But what about privacy? (IT Security Manager at Water Company 2).

9. NIS as a boundary object

The complexity of the operationalization of the water sector’s strategic goals and priorities becomes even more contingent when we turn to the implementation of NIS. According to the UK Government, NIS is aiming to improve the baseline level of cyber security of networks and information systems for the provision of essential services (DCMS, 2018). How does this pertain to the water sector or, to put simply, what does NIS protect?

As a boundary object, NIS can be understood in plural ways, as there are multiple motivations and potential beneficiaries, all bound by the need to implement the policy of protection (Table 2). Our data show that when it comes to cyber security of “digital water” there are five potential beneficiaries of NIS: the public, the nature, the water industry, the IT industry and the state. During the early stages of NIS implementation (designation of the operators of essential services and formation of working groups), NIS “opened up” to the diversity of actors and interpretations. Accessing the diversity of experiences and opinions was crucial at this stage, so that the NIS could overcome the “expertise asymmetry” (Downer 2010) and allow non-technical experts to contribute towards agenda setting. As a result, number of narratives co-existed, albeit not without tensions.

The dominant narrative suggests that the protection of cyber-physical facilities is crucial for the public values of safety and continuity of supply. However, as one of our interviewees, an OT security manager with engineering backgrounds at one of the water companies, highlighted IT security does not easily translate into water plant safety:

You’ve got to be very careful when you put in a countermeasure against a potential cyber security incident that it doesn’t actually wreck the safety case. When you design a plant safely, there’s a thing called probability of failure of demand. You work out what the risk is of failure of demand because we’re talking here about random failures (...) If you put a component in which has got an unknown probability failure demand, it obviously wrecks your statistical analysis. So, if I put a firewall in, which is a critical bit of communications equipment, we don’t know what the probability failure of demand to that firewall is and we wreck the safety case.

(OT Security Manager at a Water Company 1)

<table>
<thead>
<tr>
<th>Table 2</th>
<th>NIS as a boundary object: multiple understandings and beneficiaries</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Beneficiaries</strong></td>
<td><strong>Understanding</strong></td>
</tr>
<tr>
<td>Cyber security for the public</td>
<td>Protection of residents (personal data privacy, continuity of supply, safety, affordability)</td>
</tr>
<tr>
<td>Cyber security for nature</td>
<td>Protection of the natural environment (conservation, preventing pollution, lower CO₂ footprint from wasteful operations)</td>
</tr>
<tr>
<td>Cyber security for the water industry</td>
<td>Protection of the company (reputation, assets, avoidance of penalties, cost saving)</td>
</tr>
<tr>
<td>Cyber security for the IT industry</td>
<td>Generation of market demand for IT products and consultancy advice</td>
</tr>
<tr>
<td>Cyber security for the state</td>
<td>Protection of the state interests (competitive digital market, creation of jobs, diplomatic powers)</td>
</tr>
</tbody>
</table>
Conventional thinking would be that constitutes a win-win situation when it comes to the relationship between the NIS Directive and the natural environment – after all, if cyber security incidents are avoided, pollution is prevented. Yet, our data show that the current regulatory framework disconnects cyber security and environmental governance. Take, for example, the Ofwat’s economic regulation of the water industry, which sets the maximum prices of water bills in five-year “Asset Management Plans,” effectively capping the spending and the profit operators can make (Ofwat 2020). The spending cap affects ultimately affects the cyber security budget, hence it is viewed as a hurdle that puts sustainability in conflict with cyber security: “Climate change is going to be an issue, because if companies can’t put the bills up, and they’re having to spend more money on getting water out the ground and treating it, that’s less money to spend on cyber” (Regulator 1).

The water industry itself is in a process of being re-shaped by the NIS Directive and its implementation. Cyber security improvements are motivated by preserving reputation: “There are, you know, reputation concerns, particularly in customer-facing industries. Yes, that is always what most people are worried about: how they look in their brand” (Lawyer). However, what also emerges from the practitioners’ accounts is the understanding that cyber security improvements form the pragmatic communication strategy: “If you look at the water industry, implementing NIS, water suppliers need to do asset management. So, if you can do all of that, that’s a really good business benefit because you now understand your assets. You understand their lifetime and their connectivity. So, that’s nothing to do with cyber security, that’s management” (Security Consultant 2). What’s more, the ability to communicate business benefits is seen as a skill reserved for consultants and IT staff, as the OT engineers “don’t have the culture or the mindset to go out and campaign for resources” (Engineering Consultant 1).

One way to grab the attention of company boards is utilizing cyber security investments as an enabler of further digital innovations. In particular, centralization and IIoT were flagged up as the most talked about among the water suppliers in England. Centralized control rooms are a commonplace across critical infrastructures, although less so in the water industry. Their benefits, challenges and everyday practices have been a topic of research for the last few decades (Luff & Heath 2000; Wózniak et al. 2017). Meanwhile, the ultimate value of IIoT is less clear to our interviewees, even though water practitioners often frame it as “inevitable” (Security Consultant 1) or “something we have to embrace” (Regulator 2). At an event focusing on the IIoT in water industry we attended (November 2019, London), its participants, many of them water operators, argued that the business case for IIoT is not strong enough. Without a clear connection to public interests, digital innovation and regulations will not be able to serve the public.

We’re seeing more and more what [we] call shiny boxes coming out in the market. All of this is changing the market because people see opportunities to deliver a new shiny box, a new system, a new bit of software, a new service. So, that’s really, really driving and almost pushing along cyber security innovation in the market. (Security Consultant 3)

Last, but not least, our interviewees suggest that the successful implementation of NIS feeds into what Jasanoff and Kim (2015) call the government’s “sociotechnical imaginary,” presenting the UK as a leader in digital innovation. Not only is NIS expected to create new jobs, it is poised to establish the country as the key player in the international cyber diplomacy. NIS is anticipated to improve incident reporting across EU member states. It is also an opportunity to establish the UK’s own cyber security expertise. Interviewees treated NIS as a matter of good domestic governance, a matter of minimizing negative impacts and adapting to the increasingly complex world, all together “not necessarily a cyber thing” (Incident Response Expert).

10. Towards standardization of NIS

Nevertheless, this diversity of meanings and actors proves to be unstable in the long run as NIS requires precise decisions about what to include in scope and how to improve cyber security resilience. Going further, we observed that with time, NIS practitioners assemble in smaller groups, with the intention to work on specific topical issues. If successful, such instances of collaboration would transform a boundary object into a formalized standard – that is, a consensus on the requirements and scope of Cyber Assessment Framework forms. We argue that the initial non-translation and incommensurability of NIS as a boundary object has to give way to translation and standardization between the IT, OT, and sectoral communities of practice in order to align the governance...
goals of water and security. Translating typical security measures and concerns to water-specific context was a first step towards standardization of NIS (Table 3).

While the pressures of NIS expectations and the current threat landscape necessitate a rapid recruitment of large numbers of cybersecurity experts in OT, the appropriate pace and scale of recruitment is not yet possible due to this skills gap and the gap in understanding between IT and OT identified in Table 3. However, the collaborations formed in response to the NIS Regulations are enabling the required skills to grow as critical infrastructures undergo further modernization and IT and OT understandings are brought together. The novel expertise of OT cybersecurity needs to stay joined to the original goal of the water sector to deliver an essential service of clean, sustainable and affordable drinking water.

Below, we list and analyze five instances of collaboration pertaining to NIS (for further description, see Table A2). We identified the first two as successful in mobilizing NIS actors to align their expertise with water governance goals, whereas the remaining three as ambivalent or unsuccessful. These successful collaborations are: (i) the water OT engineers’ working group and (ii) the informal working group consulting on the early draft of NIS set up by the Drinking Water Inspectorate (DWI). In these collaborations, semi-formal arrangements were established to convert IT security terminology present in early versions of NIS Directive into the OT and sector-specific context (Table 3). This ensured that NIS works toward the values of safety and continuity of supply. What’s interesting about these cases is that the experts influencing NIS are water regulators and engineers organizing from the bottom-up, rather than trade bodies or water suppliers’ senior management. Technical OT expertise becomes key to the political direction of NIS implementation.

We were able to identify the next collaborations as ambivalent in mobilizing NIS implementation: (iii) relationships between the regulators (DWI, Ofwat) and the government (National Cyber Security Centre, Department for Environment, Food and Rural Affairs, Department for Digital, Culture, Media and Sport). On the one hand, building a team of cyber security regulators within DWI was beneficial as it embedded concerns with safety and continuity of supply. On the other, the lack of a relationship between Ofwat and DWI led to a

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Translation of cyber security practices and concerns across IT and OT, as reported by the interviewees</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT</strong></td>
<td><strong>OT</strong></td>
</tr>
<tr>
<td>Machines can be switched off for upgrades</td>
<td>Machines have to be always on; cannot reboot or do patch management</td>
</tr>
<tr>
<td>Concerned with information (data)</td>
<td>Concerned with critical assets (pipes, valves, sensors, data)</td>
</tr>
<tr>
<td>Back up of data is essential</td>
<td>Back up of data unfeasible if an organization owns 1000s of remote assets</td>
</tr>
<tr>
<td>Blocking access to prevent brute force password attacks is common</td>
<td>It is not feasible to block access to OT equipment if you type your password incorrectly</td>
</tr>
<tr>
<td>IT do not commonly deal with time critical data; firewalls are a basic element of security</td>
<td>OT engineers work in milliseconds to facilitate synchronization or chemical reactions. Precision of equipment is essential: firewalls and IIoT could slow down critical processes</td>
</tr>
<tr>
<td>IT security staff are trying to stop the OT engineers having domain administrator privileges</td>
<td>OT engineers need domain administrator privileges to do some of the work that they needed to do which was forced on them by the software vendors</td>
</tr>
</tbody>
</table>

© 2021 The Authors. *Regulation & Governance* published by John Wiley & Sons Australia, Ltd.
misalignment between Ofwat price review timescales and DWI’s NIS improvement plans. Missing concern for the cost of NIS implementation and associated investments could bring about a risk that the goals of “economic efficiency” and “affordability” will not be realized. Similarly, the fourth collaboration, (iv) internal NIS “Steering groups” set up within water operators mobilized expertise for NIS in ambivalent ways. Many of the operators set up such groups made of diverse experts representing various areas of their organizations. They claimed that this move allowed to take into account multiple motivations and goals, while facilitating translation of the IT expertise to the OT context. However, power struggles existing inside some organizations combined with low retention of staff across the sector are seen as a barrier to the success of these Steering Groups.

The final point identified is characterized by an unsuccessful attempt to collaborate, and, therefore, an absence of alignment with public interest: (iv) Water industry trade body. The group has failed to generate expertise and, as a result, lacked the power to influence the NIS implementation so far. Participants admitted that the official “NIS working group” led by the water industry trade body has not brought about any developments so far due to the lack of agreement on terms of reference which did not create a trustworthy environment to share experiences and data. Practitioners navigate between translation and incommensurability, between inclusion and specialization, allowing NIS to oscillate between a boundary object (the Directive) and a standard (the consensus on the scope of water industry CAF). This does not end, however, the process of interpreting and implementing complex technological regulations. As Star (2010) argues, established standards leave out “residual categories” around which new boundary objects form. Given that the implementation of improvement plans and the procurement of security measures is undergoing but far from complete (DCMS 2020), we suggest that going forward, NIS practitioners will collaborate to establish what constitutes the “appropriate and proportionate” level of investment. Above all, such improvements should also align with water governance and environmental goals rather than be solely proportionate to the cybersecurity risks. In order to achieve this, OT, IT, and sectoral practitioners ought to engage in the cycle of translation and standardization to maintain collaborations grounded in respect for public goals. Further research ought to observe how these collaborations form and whether they align with the public interest.

11. Conclusions

How do we regulate water? What role does the NIS Directive play in this process and to what extent does the advent of NIS affect what it regulates? In this paper, we investigate how digital regulations are aligned with the goals of water sector governance, drawing from a case study of cyber security regulations and the water sector in England. Having identified a set of specific priorities guiding water governance – safety of supply, continuity of supply, affordability, economic efficiency, sustainability, and broadening participation – we mapped these goals onto the experiences of NIS implementation. By viewing NIS as a boundary object, we demonstrate plural understandings and beneficiaries of the regulations. We then show how NIS Directive evolves: observing early stages of a standardization process in which the water sector makes itself accountable as a subject of cyber security governance. Through the translation of expertise across the OT and IT worlds, water practitioners were able to reach a consensus on the scope of NIS in the sector-specific CAF document.

Furthermore, we identify five instances of collaboration to suggest the mechanisms enabling or hindering NIS’ alignment with water governance priorities. Only two collaborations were successful in translating expertise and aligning NIS goals with water governance. This alignment, we argue, is what allows the emerging governance configuration to define what water is, how its supply is established and maintained. We argue that NIS implementation is only partially aligned with the public interest. In the appraisal of cyber security improvement plans, regulatory bodies like DWI and Ofwat ought to keep the water governance goals at the forefront. In co-producing environmental and digital regulations, diverse practitioners should actively negotiate their priorities so that further standardization processes are grounded in sector-specific contexts.

As we are in the early stage of NIS implementation, the pathway to digital and cyber secure water provision is not fixed yet, and it is indeed related to the industry-specific understandings of the relationships between digital technologies, security, and water infrastructure. The accommodating nature of NIS as a boundary object facilitates unfolding of multiple narratives around security of digital water systems. It is, therefore, vital to reflect what and whom we are securing, be it water, residents, state interests or business models. Cyber security could be, and
often is, treated as a technical issue of equipment maintenance, left for the IT professionals to be dealt with. Yet, the IT security solutions cannot be successfully appropriated to the water infrastructure context, where OT equipment and engineering informs professional priorities and procedures. The bottom-up involvement of experts in OT and Safety and Water is key to ensure a NIS implementation is grounded in sector specifics and inclusive of water governance issues.

The need for cyber security reconfigures the water sector itself, for instance, by forming new relationships between the regulators, manufacturers and water suppliers, creating new types of jobs or leveraging new funding mechanisms. Furthermore, cyber security could be viewed in the context of the government’s vision to become the key player in the international cyber diplomacy and develop domestic cyber security market. Without paying attention to collaborations visible through the analysis of “the making of” digital regulations, we cannot see the possible trajectories of cyber security and digitization across critical infrastructures. But we also call for shifting the debate from understanding cyber security as an issue solely requiring “solutions” rather than a matter of negotiation (Morozov 2013). The process of negotiation between diverse experts will be essential to enable the necessary translation and integration towards the goals of water. As cyber security regulations are intimately intertwined with the future of digitization, we risk that they will leave the adoption of emerging digital technologies unquestioned just because they are deemed “secure.” In the era of “OT and IT blending”, it is important to investigate how the experts themselves “blend” into other areas of expertise: what is translated and what is left open to interpretation. Ultimately, the introduction of emerging digital technologies will reconfigure our relationship with water itself.

Acknowledgments

The authors thank their participants for sharing the insights and inviting them to their professional events. The authors disclosed receipt of the following financial support for the research and/or authorship of this article: This research is supported by the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS); project title: “How many shades of NIS? Understanding Organizational Cybersecurity Cultures and Sectoral Differences”. RITICS is funded by the National Cyber Security Centre.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Endnotes

1 Note that water governance is multi-scalar and occurs at several administrative levels: river basin, coast, EU, the UK, England and Wales, England, water company. For the avoidance of confusion, the empirical material in this paper draws from English governance only, where water suppliers are private companies regulated by the government.

2 This is also known as “The Internet of Things” or “smart tech.”

3 Their self-assessment follows the government guidance, see Cyber Assessment Framework (NCSC, 2019).

4 Following Brexit, the designated Operators of Essential Services and Digital Service Provides still have to comply with NIS. Organizations offering services in the UK based in the EU have to a UK-based representative (DCMS, 2020) https://www.gov.uk/guidance/nis-regulations-non-uk-digital-service-providers-operating-in-the-uk.

5 We draw from Stritzel (2011) understanding of “cyber security translation” rather than the definition of translation used in actor-network theory.

6 Water Industry operates in five-year price review cycles, for example, setting the budget in 2019 ahead of the 2020–2025 period. In contrast, NIS proposals were required in early 2020 (DWI 2020b).

7 Opinions voiced by water sector practitioners during IIoT&water industry event, November 2019, London.

8 Opinions voiced by water sector practitioners during IIoT&water industry event, November 2019, London.

Reconfiguring water

11 Interviews with water regulators and OT manager working for water supply company, November 2019.

References


NIS Directive. Improving Cybersecurity in Europe


**Appendix A**

### Table A1 Goals of water governance in England

<table>
<thead>
<tr>
<th>Goal</th>
<th>Quote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety of supply</td>
<td>“it is vital to recognize first the basic right of all human beings to have access to clean water and sanitation at an affordable price” (Dublin Principles – DP 1992)</td>
</tr>
<tr>
<td></td>
<td>“Reduces health risks in particular through the management of water quality” (Integrated Water Resources Management – IWRM; UNESCO 2009)</td>
</tr>
<tr>
<td></td>
<td>“What we all need: resilient, reliable, safe and good quality water services” (Ofwat 2019)</td>
</tr>
<tr>
<td></td>
<td>“To protect public health and maintain public confidence by securing sufficient, safe and clean drinking water, now and for future generations” (DWI 2020c)</td>
</tr>
<tr>
<td></td>
<td>“Water protection is therefore one of the priorities of the Commission. European Water Policy should get polluted waters clean again, and ensure clean waters are kept clean” (WFD)</td>
</tr>
<tr>
<td>Continuity of supply</td>
<td>“What we all need: resilient, reliable, safe and good quality water services” (Ofwat 2019)</td>
</tr>
<tr>
<td></td>
<td>“To improve and protect the quality and sufficiency of drinking water supplies in England and Wales.” (DWI 2020c)</td>
</tr>
</tbody>
</table>

(Continues)
Table A1  Continued

<table>
<thead>
<tr>
<th>Goal</th>
<th>Quote</th>
</tr>
</thead>
</table>
| Affordability | “it is vital to recognize first the basic right of all human beings to have access to clean water and sanitation at an affordable price” (DP 1992)  
“Balance between ‘water for livelihood’ and ‘water as a resource’” (IWRM, 2009)  
“For water companies to provide greater public value, delivering more for customers, society and the environment (...) What we all need is: affordable water for everyone” (Ofwat 2019) |
| Sustainability| “Past failure to recognize the economic value of water has led to wasteful and environmentally damaging uses of the resource” (DP 1992)  
“Assists appropriate planning of water use, conservation, and the protection of surface-water and groundwater with better resilience and/or larger safety margins” (IWRM, 2009)  
“For water companies to provide greater public value, delivering more for customers, society and the environment (...) Companies will need to improve the environment as a core part of their business” (Ofwat 2019)  
“To promote strategic planning for water quality and sufficiency now, and for future generations”. (DW, 2020c)  
“There are a number of objectives in respect of which the quality of water is protected. The key ones at European level are general protection of the aquatic ecology, specific protection of unique and valuable habitats, protection of drinking water resources, and protection of bathing water” (WFD) |
| Economic efficiency | “Water has an economic value in all its competing uses and should be recognized as an economic good. Managing water as an economic good is an important way of achieving efficient and equitable use, and of encouraging conservation and protection of water resources” (DP 1992)  
“Balance between ‘water for livelihood’ and ‘water as a resource’” (IWRM, 2009)  
“A laser focus on driving up performance and efficiency now will put companies in a better place to face the challenges ahead. As companies prepare for the future, they will need to innovate and make investment in assets and people, which should deliver near-term as well as long-term benefits” (Ofwat 2019)  
“The need to conserve adequate supplies of a resource for which demand is continuously increasing is also one of the drivers behind what is arguably one of the Directive’s most important innovations - the introduction of pricing. Adequate water pricing acts as an incentive for the sustainable use of water resources and thus helps to achieve the environmental objectives under the Directive” (WFD) |
| Broad participation | “Water development and management should be based on a participatory approach, involving users, planners and policy-makers at all levels. The participatory approach involves raising awareness of the importance of water among policymakers and the general public. It means that decisions are taken at the lowest appropriate level, with full public consultation and involvement of users in the planning and implementation of water projects.” (DP 1992)  
“To drive water companies to meet long-term challenges through increased collaboration and partnerships” (Ofwat 2019)  
“With following key aims: getting the citizen involved more closely (...)” (WFD) |
Table A2  Five instances of collaboration in the water industry cyber security landscape. We analyzed whether they help or hinder with the alignment of NIS and public interest

<table>
<thead>
<tr>
<th>Collaboration</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Semi-formal water engineers’ working group [Helps with alignment]</td>
<td>Semi-formal working group, organized bottom-up by engineers and security managers working for the UK water suppliers. Aims to create an ‘aspirational gold standard’ for telemetry. Meets to share experiences on NIS and establish a benchmark. According to water operators, since companies are regional monopolies, they can collaborate on security and trust each other: “So, that’s a big part of the work we are doing, and this is what we do which I believe the other sectors aren’t doing” (OT Security Manager at a Water Company)</td>
</tr>
<tr>
<td>2. The informal working group consulting on the early draft of NIS set up by the Drinking Water Inspectorate [Helps with alignment]</td>
<td>On top of statutory consultations, DWI requested that two water suppliers review the first draft of the NIS Guidelines and provide comments on language and policy scope. This allowed an effective translation of generic and IT-oriented policy into water-specific and OT-appropriate context</td>
</tr>
<tr>
<td>3. Relationships between regulators and government agencies [Ambivalent]</td>
<td>Situating NIS implementation team inside Drinking Water Inspectorate enabled NIS stakeholders to establish relationships between the regulator and water suppliers, even if the rest of DWI does not conduct “cyber” work There is a need for further communication between DWI and NCSC (for help with capability building across the operators) as well as DWI and Ofwat (for aligning timescales of price control and NIS implementation; for aligning NIS implementation with the goals of water governance)</td>
</tr>
<tr>
<td>4. Internal NIS “Steering groups” [Ambivalent]</td>
<td>Successful communication goes beyond exchanging technical details. Therefore, raising a case for cyber security requires a degree of pragmatism, where a security expert is able to communicate the benefits to diverse stakeholders. Water companies commonly set up in-house steering committees to implement NIS; they are made of engineers, business continuity experts and senior management: “The only way address the old IT-OT division is to bring in senior management and to create what I call an A team. So, the A team is a group of people from different walks of life, so you might have IT, OT, health and safety and general security, like physical security. You might have finance, operations, maintenance and senior management. So, with all of those people in there, there should be nothing stopping your project going forward,” (Security Consultant 4) However, internal organizational politics can hinder successful implementation, for example, high turnover of management boards reported in the water industry. Some participants argued that appointing a fixed-term external CISO could be in a better position to advice on bold actions as they would not be involved in day-to-day office politics</td>
</tr>
<tr>
<td>5. Official water sector trade body [Hinders alignment]</td>
<td>A top-down working group on resilience and continuity did not manage to establish trust due to a lack of agreements on the terms of reference and expectation that operators will share confidential details of policy implementation</td>
</tr>
</tbody>
</table>