Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P4957-cd

Navigating Complexity and Hybrid Threats: The Relevance of Resilience Perspectives in a Digitalized Water Sector

Jannicke Thinn Fiskvik

NTNU Samfunnsforskning AS, Norway. E-mail: jannicke.fiskvik@samforsk.no

Tor Olav Grøtan

SINTEF Digital, Norway. E-mail: tor.o.grotan@sintef.no

Rita Ugarelli

SINTEF Community, Norway. E-mail: rita.ugarelli@sintef.no

Camillo Bosco

SINTEF Community, Norway. E-mail: camillo.bosco@sintef.no

Managing urban water supply systems is challenged by several factors, including increased pressure on water resources with respect to both quantity and quality. In addition, digitalization of the water sector has increased system complexity, including interdependencies between physical and digital systems. Considering a new geopolitical reality and serious threat landscape, we argue that the water sector, as a critical infrastructure faced with increased complexity and new risks (e.g., cyber and physical hybrid threats), can benefit from a more holistic resilience thinking in security practices. The paper explores the relevance of resilience thinking in a Norwegian water utility, engaging perspectives from Resilience Engineering. The paper builds interviews of employees that work with digital and physical security of water distribution systems, supplemented with a document analysis. The study finds that there is resonance with resilience principles in ongoing work and current ways of thinking. Simultaneously, we suggest that there is value in increased awareness of avoiding becoming 'robust yet fragile' and highlight the importance of adaptive capabilities. In turn, this can contribute to the water sector being better prepared to handle future challenges and growing complexity of the multifaceted socio-technical water supply system.

Keywords: resilience, water sector, digitalization, security, threat landscape.

1. Introduction

Water infrastructure is a complex and composite system that must be managed in a holistic and organized manner (Bosco et al. 2023). Over the past 20 years, a high leakage percentage, aging water supply systems and a significant backlog in pipeline renewal have increased the motivation for digitalization of the water sector (Campisano et al. 2020). Other drivers have been the need for increased efficiency in water production and efficient resource management in the water supply industry as requirement from the revised Water distribution Directives but also a need in response to water security issues due to climate change impacts (Bosco et al. 2022). The digital transition of the sector has led to a significant increase in the use of innovative technologies, requiring the rise of systems that combine information technology (IT) and operational technology (OT) (Bour et al. 2023). IT in the water industry controls data or various types of information, while OT controls equipment and physical processes. This development has increased the challenges of the water industry's cyber security, creating new vulnerabilities that must be addressed to secure the cyber and physical systems in the water infrastructure (Ugarelli 2021); further, even though the infrastructures of the water sector comprise interconnected physical and cyber assets, physical security and cybersecurity remain fragmented. Digitalization could put the sector at higher risk, if the process of digitalization does not integrate security into

solutions, with systematic management of risks covering both cyber and physical threats.

Since 2022, the new geopolitical situation characterized by conflict, great power rivalry and hybrid threats, entails a more serious threat landscape than in the last decades. Vital societal functions, including the water sector, face increased threats of sabotage and cyber threats. For example, there have been several break-ins into Finnish water treatment facilities during July 2024 (Sandström 2024). Cyberattacks against various national water utilities have increased significantly (SWM 2025). And, in the Ukraine war, water systems have been indirectly and directly targeted, signifying the vitalness of water supply (Gleick, Vyshnevskyi, and Shevchuk 2023).

Historically, security work in the water sector has mainly been reactive, resulting in security not being adequately addressed (Bosco et al. 2020). More recently, however, several security requirements have been introduced for securing water supply following its status as a vital societal function. The purpose is partly to stay ahead of unwanted incidents and protect the water supply and its associated systems (Rousso et al. 2024). Nevertheless, national authorities warn against existing vulnerabilities and the need to prioritize security work further in response to the new threat landscape after 2022 (Norwegian Food Safety Authority 2023).

The water supply sector has traditionally focused on system safety and reliability to ensure water supply when assets fail. Little has been done in terms of resilience and even less in terms of integrated cyber-physical approach for risk management linking security and safety, in which the cyber and the physical layers of the water systems are secured as an integrated cyber-physical domain (Ugarelli 2021). Existing research on resilience in the water sector has often focused on the development of indicators (Creaco, Franchini, and Todini 2016) to analyze individual aspects related to the topology of the system. On the other hand, in terms of resilience associated with preparedness against cyber-physical attacks, scenario-based stress-testing technologies have been developed by the STOP-IT project and demonstrated in real environment (e.g., Bosco et al. 2022).

To address new challenges in a constantly evolving society and threat landscape, the water sector must be adaptable to maintain its core function (i.e., being reliable) in a safe and secure manner. Our presumption is that the water sector can benefit from a more holistic resilience thinking related to integrated safety and security practices. Accordingly, the research aims to investigate whether resilience thinking has been spurred throughout the overall digitalization processes in a water supply organization, if such thinking is reflected in current practice, and if potentials of strengthening of resilience are present. The analytical approach is anchored in *cyber resilience*, pointing to the need for resilient organizational and sociotechnical performance to ensure both (1) safety and security in infrastructure domains critically relying on cyber technologies, and (2) resilient countering of incidents and brittleness of those technologies.

The next section outlines a framework for theoretical perspectives including Resilience Engineering (RE), before the following section describes primary methods and empirical data. Then the paper analyzes the case of City of Oslo, Agency for Water and Wastewater Services, followed by a discussion of findings in an RE theoretical framework, and a concluding section.

2. Resilience and Adaptive Capacity

With growing complexity in digitalized infrastructures and critical societal functions, the notion of 'resilience' has gained increasing popularity. The term is, however, polysemic and ambiguous. A prevalent conceptualization is related to the recognized need to ensure controlled recovery and rebound from incidents that elude risk management efforts. Here, resilience as a practice corresponds to practices of risk management, emergency planning and business continuity planning. This is accompanied by the presumption that preparedness aimed at anticipated events projected from a current understanding of how the system works, also will be useful in the event of fundamental surprise (or 'black swans').

In parallel, the RE strand has advocated a very different approach, rooted in complexity theory. From this perspective, fundamental surprise is inherent, and common basic assumptions of order, rational choice and intent in organizational decision-support and strategy are challenged (see e.g., Kurtz and Snowden 2003). RE therefore aims to *engineer*, not a

specific solution in the classical engineering sense, but *an adaptive capacity* that enables organizations constantly to revise their models, anticipations and response repertoire, avoiding becoming stuck and stale when encountering complexity and deviations from normal operations. Arguably, by embracing change and being poised to adapt through pursuing resilience as a distinct practice, organizations will avoid becoming "robust, yet fragile", and instead enable what Woods (2018) denotes as "graceful extensibility"; the system's ability and capacity to stretch beyond set and perceived boundaries. Key issues for sustaining such adaptive capacities are *inter alia* timing, coordination, initiative and reciprocity.

Arguing that different resilience perspectives are useful on their own terms, Grøtan and colleagues (2022) propose the "Resilience ABC" model, comprising three different theories of resilient outcome and attribution of its origin. In Theory A and B, resilience as *outcome* (e.g., rebound) is considered something one has; that is, an epiphenomenon of the safety and security work that is already done in terms of existing practices and activities embedded in a system. In Theory C, resilience is considered something one does, a distinct *process* or attitude to achieve or maintain adaptive capacity in the system (Grøtan, Antonsen, and Haavik 2022). In this context, we focus on the distinction between robustness gained from Theory A or B orientation, and resilience as distinct practice based on a Theory C orientation. The latter aims for adaptive capabilities beyond normative practices and rules, paying special attention to the rudiments of (Theory C) resilience, while at the same time acknowledging the value of coexistence with Theory A/B type of resilience.

3. Research Design and Approach

We employ an explorative research design, aimed at probing for the relevance of resilience perspectives in a digitalized water supply industry, and a deeper understanding of digitalization and security processes considering a changed threat picture. Accordingly, the paper is based on a single-case study, which is suitable when one seeks to understand ongoing processes and the characteristics of a situation (Yin 2018).

The case in question is the City of Oslo, Agency for Water and Wastewater Services (VAV). VAV is the only water supply agency in Norway subjected to the national Security Act, since vital national functions (e.g., Parliament and Government) reside in the capital.

The primary method is qualitative semi-structured interviews, supplemented with a document study. We have conducted four interviews with employees in central positions that work with physical and digital security in VAV.[a] For the purpose of anonymity, the names of the informants have been replaced by an identification number (e.g., ID01). To provide context, the document study involves analysis of official documents related to security and emergency preparedness in water supply, and central threat assessments by Norwegian national security services. All translations from Norwegian are done by the authors.

4. Analysis

The current threat picture is severe. National security services point to an increase in advanced cyberattack against Norway, and increased sabotage threat against critical infrastructure, and foreign intelligence operations (PST 2024; NSM 2023). In a highly distributed system like VAV, physical security also relies on digital systems. Physical security is also instrumental for safety of water delivery, safety at work, and for the security of operational control systems. Based on interviews and central documents, we analyze VAV with emphasis on drivers and processes for cyber- and physical security, their interaction, and robustness and adaptability related to digital and physical threats.

4.1 Drivers of cyber and physical security

VAV has over the years gone through major security work and digitalization processes (Grindheim and Almaas 2024). When asked about drivers of cyber- and physical security in VAV, our informants point to a multifaceted picture. Central is a municipal revision of information security and operation control systems back in 2010 that revealed basic and major vulnerabilities, including a lack of information security. Following the revision, the agency received a long list of requirements. This

[a] The data collection is approved by the Norwegian Agency for Shared Services in Education and Research (ref. no. 893668).

prompted systematic internal work on improving information security and security culture, and close vulnerability gaps. In addition, VAV began a parallel process on object security.

While the revision led to an increased security focus internally, it has also become a societal topic of concern externally. VAV was subjected to the Security Act in 2012-2013 to enhance the security of water supply systems, in light of increasing concerns regarding potential threats and vulnerabilities. Related, water supply was designated a fundamental national function by the Ministry of Health and Care Services. In 2019, the Security Act was amended, entailing a functional perspective that required further amendments to the security work (ID01). Another important driver is the resolution by the Norwegian Food Safety Authority from 2017. For decades, Oslo has had one source providing 90 per cent of its water. Growing impatient, the Food Safety Authority therefore required Oslo municipality to establish a reserve for water supply by 1 January 2028 (VAV 2023).

Upcoming regulations, such as the NIS2 Directive are also attended to. In the wake of 2022, the EU accelerated ongoing processes of enhancing resilience of critical infrastructure, both in terms of cyber and physical security. While not yet implemented in Norwegian law, the government is proposing a new legislation of basic security measures for important societal undertakings to prepare implementation (Meld. St. 9 (2024-2025)). These can be expected to be implemented soon, with further implications for VAV. While the impression is that VAV is rather compliant with NIS2 following existing procedures and legislation, they are working on increased documentation of what they do – denoting it as typical for IT and OT milieus to be very hands on and operative, and less attentive to documentation (ID04).

Finally, the threat picture was highlighted as an important driver. VAV has in the last years worked more closely with the threat picture, focusing on what they are securing against, with a view on what is happening in Ukraine. There are also indications of increased intelligence activities towards VAV. According to ID01, the overall picture sparks increased motivation to secure facilities more than before. Moreover, the security situation has anchored *inter alia* object security more firmly in the top management.

4.2 *Digitalization: Ongoing processes and challenges*

Before 2010, VAV is described as having one large network where "everyone was welcome" (ID03). However, since then VAV has used vast resources on information security and has reached a satisfactory level. In terms of digitalization, Oslo VAV is currently in the process of transferring administrative IT systems to Oslo municipality central following a political decision. As part of the transfer of administrative systems, a large mapping job has been necessary, in which 200 systems have been identified. In this vein, it is argued that the agency has become more robust as they have greater oversight and can better control systems and infrastructure (ID03). Technical systems (IT/OT), however, are still operated in-house. In this regard, VAV is building a new, modernized technical platform for both IT and OT systems – designed after best practice and the NSM ICT Security Principles. Currently, the perception is that VAV is best equipped having technical system on the premises (ID04).

The work in VAV has been characterized by compartmentalized silo mentalities, which the administration is aiming to counteract through reorganization. A measure involves establishing one section in charge of both IT and OT. Though, it is also noted that there is a long way to go before they see synergies of the reorganization (ID04). This is attributed *inter alia* to cultural differences and demarcation lines but also increased work pressure and challenging resource situation (ID03). According to ID04, having IT and OT under one umbrella makes sense since both are internal suppliers of IT infrastructure and systems. This also follows a broader industrial trend, in which boundaries between IT and OT are breaking down. The Norwegian National Security Authority (NSM) highlights that the integration between IT and OT systems increases by more sharing of real-time data, and the availability of critical industrial systems and process data. In turn follows increased vulnerabilities and risks for OT. The NSM also points to challenges following an increasing competence gap while more critical systems and functions are outsourced (NSM 2023). Hence, by operating IT and OT systems in-house, Oslo VAV arguably maintains a higher level of control.

4.3 *Physical security processes and interdependencies between the digital & the physical*

In terms of object security, the municipal revision and the subjection to the Security Act initiated work on securing designated critical national functions and those facilities considered most critical. Currently, there are ongoing processes of securing additional infrastructure. With the new Security Act of 2019, it is VAV that draws up requirements for a reasonable level of security for their facilities. According to one informant, requirements are now more defined and sharpened, leading to increased standardization of how facilities are secured (ID01). Another major project relates to the new water supply (Oslo Municipality 2024). While it is impossible to secure all infrastructure, the aim is to have redundancy for everything, in which a new water reservoir will be a crucial measure. At the same time, it is noted that the new water supply will also increase the complexity significantly, by constituting one third of the existing infrastructure for the entire city (ID01).

Overall, our informants highlight an increased dependency on IT and OT systems, including the interdependence between physical and digital security. An interesting case in point is two classified security networks. One network deals with object security, while the other is for information sharing in projects. The downsides of maintaining a classified network have caused VAV to consider extracting and transferring classified information from the network connected to object security to the network of general classified information (VBN), as this information is not necessary for daily operations. In turn, this will enable them to declassify the object security network to mitigate current downsides. First, it is very expensive having a classified network, which involves running fiber to all the locations that must be secured. Second, it is currently not possible to use 4G or 5G solutions, which exclude many locations. Third, the response time is high as it is necessary to access the network physically to recover errors. Thus, by declassifying the object security network, VAV can secure more locations by connecting them to the security network. A declassified network also gives the IT department an improved opportunity to surveil the system. Moreover, response time will be reduced as technicians can connect from other locations.

With increased interdependencies between physical and the digital security, those working with, for example, object security needs to bring in IT personnel. As such, it is highlighted that cooperation between the two spheres gets better and better (ID01). Simultaneously, they are currently not under the same department, which arguably has brought back silo walls (ID03).

4.4 *Robustness and adaptability in VAV*

Generally, VAV is described as an emergency preparedness agency, with characteristics such as “forward leaning”. As perceived by new employees, VAV entails a dedicated effort to stay tuned to the emerging threat landscape, and concatenating a vast, but hitherto fragmented body of risk and vulnerability assessments (ID02). Herein lies an intensive focus on security, and an emergency preparedness mentality – “if something happens, everyone contributes” (ID01). Informants also mentioned that when they started working in VAV, they were struck by an overwhelming attention to security (ID02, ID04). Importantly, it is highlighted that unforeseen operational incidents occur weekly, which they must act upon (ID01). In turn, these weekly incidents, alongside preventive security work, add to the preparedness for the unexpected.

The abovementioned silo-based work is a characteristic not only for IT but for the whole agency. For example, departments have conducted their own risk analyses, and there has been limited cross-departmental information sharing (ID02). Thus, there is ongoing work in reviewing the numerous existing risk and vulnerability analyses and collecting them into one system. Here, a central aim is to create synergies through coordination and achieve a better overview of interdependencies and totality (ID02). VAV has also completed a revision of the whole contingency plan framework.

For both cyber and physical security, our informants state that they are working more scenario based. For physical security, one informant notes a change in how they work considering the changes in the security political situation, including working towards scenarios (ID01). This follows the magnitude of the infrastructure that must be secured, which has increased in size and complexity. Another

informant working on risks highlight that "risk is what you are not prepared for" (i.e., unknown unknowns), and underscores the importance of building a form of preparedness in this regard, as well as redundancy (ID02).

Revisions and adaptations of contingency plans are partly based on exercises. Annually, VAV holds a major exercise based on different scenarios, in addition to several smaller exercises with different scenarios throughout the year. Those attending exercises are not told the scenario beforehand, and unforeseen aspects are played out to test the ability to adapt and think beyond foundational contingency plans. In this regard, one informant points out that "irrespective of how good the contingency plan framework is, you have to adapt to every situation, because the plan won't cover everything anyways" (ID01).

On the question of what makes adaptions possible, the informants point to the composition of personnel, the importance of the relations formed through daily interaction, and the importance of reflections after an incident or exercise, in the military denoted 'after action review'. At the same time, it is conceded that there is a desire to exercise more, but that daily operations require much time and exercises do not necessarily get prioritized.

The ongoing transfer of administrative IT services to Oslo Municipality also sheds interesting light on robustness. ID04 pointed out that a transition from a situation where few people manage the system very skillfully and in a dedicated manner but not 24/7, to a situation in which a higher number of less skilled people operate 24/7, requires better documentation and better plans. However, an overly detailed plan will always be at risk of being derailed by a missing detail. Thus, "they need to be detailed enough but not too detailed" (ID03). This perspective signifies a potential for robustness turning fragile but also impacts the potential for adaptivity. It also signifies the somewhat disturbing fact that the whole issue of maintaining operational control is increasingly OT or SCADA dependent. Their unavailability might render the organization paralyzed, while before, the operators were more energetic. Another interesting issue is that such a process of shifting responsibility sparks a process of thorough mapping and understanding of the systems that are in use, which might otherwise be left unattended. Management attention to inherent IT/OT tensions, demarcation lines and competence issues is a critical aspect anyhow.

5. Discussion

Taking the analysis a step further, this section discusses the above analysis with a focus on adaptability beyond established rules and procedures. Unsurprisingly, organizational arrangements and operational experiences signify a dominant emphasis on robustification, corresponding with Theory A/B. Though, when directly asked at a principled level, the need for adaptive capacity (Theory C) was acknowledged by several informants. Nevertheless, an acquired belief in the inherent flexibility of established procedures and practices stands firm in the foreground. Apparently, the perceived usefulness of contingency and continuity plans is more prevalent than a fear of becoming robust yet fragile.

It is tempting to ascribe this observation to the quite successful improvement process VAV have conducted from the rather bleak beginning in 2010, and that they so far have not experienced any fundamental surprises or severe consequences, despite ups and downs. A crucial question, then, is whether that presumption holds as the geopolitical situation and the threat landscape continues to deteriorate.

One informant claims that exercises indicate that a main cause for emergency plan failure is that it is actually *not* followed (ID04). However, observations also imply a practical resemblance to Theory C. The decision to declassify the network for physical object security to achieve more connectivity, coverage (including the new water capacity), agility and responsiveness may be interpreted strictly as a risk-based act of Theory B; at the same time, the *arguments* applied may also be conceived as implicit appreciation for constituents of Theory C. Similarly, the reported practice of identifying vulnerabilities in routines and changing them accordingly (ID01), also requires a sensitivity to failure and a willingness to act proactively that may be conceived beyond a strict Theory B trait.

Moreover, the description of VAV as an emergency preparedness agency with an emergency mentality, implies the possible presence of other rudiments that at least are

promising for the building of an adaptive capacity. One of these is that unknown unknowns are perceived as the real risk (ID02). Another is the acknowledgement that plans have limited validity when incidents materialize. A third potential rudiment is the claim that the overall contingency plan is valid independently of type of incident contingency, and continuity plans are "rather flexible" (ID04). Though, exactly what this flexibility in plans entails is somewhat unclear. There are some cues, however, that draw our attention to interpreting the potentials in this flexibility.

First, although it is stated that it is primarily the higher emergency staff that gains training through exercises, it is also stated that the same staff is clever in mobilizing the proper competence at lower organizational levels when needed. This happens spontaneously but is also enabled by preestablished relations due to the short distances in daily work (ID01). Second, but related, there is also a potential expressed as embedded in doing more systematic "after action" reviews related to daily work, in which people take the time to make a thorough judgement of *inter alia* which successful practices must be kept, what made them good, why they were taken into use, and what was gained. The presence of the "hamster wheel" impedes this, but it is recognized, from a managerial position, that this *should* be prioritized, because it "actually drives improvement" (ID01). Moreover, it is recognized that the collaborative process of finding a solution to a difficult problem, including raising new questions, is as valuable as the answer found (ID02), due to new dynamics and a "synapse party" (ID03) with new participants. Overfocusing on known risks is also recognized as source of blind zones which may turn critical in the encounter with threat actors (ID02). Finally, the interviews also demonstrate that the achievable robustness, the proximity of "robust yet fragile" and thereby the need for organizational attention to adaptive capacity, is highly dependent on the dedication, skills and working conditions for key professionals.

6. Conclusion

The aim of this paper was to probe into the relevance of resilience perspectives in a digitalized water sector considering a severe security threat landscape, drawing on VAV as a case. We have applied a broad conception of cyber resilience to address generic organizational and sociotechnical aspects, not confined by technological boundaries. While we cannot draw broad generalizations due to the limitations of the empirical data, there are interesting findings that contribute to the further discussion of adaptive capacity inspired by RE, as well as the topic of critical infrastructure security.

Overall, we observe that digitalization is accompanied by increased security awareness, but also lagging managerial attention to the organizational impact, including lack of recognition of IT/OT as separate domains with distinct legacies and incitements for development. This combination is not always satisfactory "hosted" organizationally. Back-and-forth reorganizations (de-siloing and, effectively, re-siloing) of the IT/OT relation (e.g., various forms of outsourcing) sparks valuable learning, but the optimal solution tends persistently to remain on the horizon. This also influences the prospects for adaptive capacity as the interactive patterns and relations constantly need re-establishment. We also observe that a successful journey of enhanced robustification and mantra of being an emergency organization has resulted in faith in the embedded flexibility of procedures and modes of operation, however, accompanied by an acknowledgement of the uncertain times ahead, and the presumed value of adaptive capacity. Lastly, we have identified key rudiments in VAV from which adaptive capacity may be built.

We argue that VAV demonstrates that digitalization processes comprise the opportunity to identify, nurture and develop needed adaptive capacities in conjunction with traditional robustification strategies. However, this will require managerial attention to key issues, and proactive strategies to avoid that rudiments are sacrificed for short-term gains. Exercises, however realistic, might become somewhat artificial if they do not challenge indefinite and uncomfortable boundaries. A central key is to foster the daily work which enables adaptations when outer boundaries are reached during an unexpected event.

Considering the limitation of the study in terms of generalizability, a relevant future research avenue is to address case studies of other water utilities (in e.g., different regions, countries, geopolitical contexts). Another

research avenue includes providing quantitative analysis as background to give insights on the size of the issues.

Acknowledgement

This paper is inspired by and thematically overlapping with the master's thesis at NTNU by Trude H. Grindheim and Kristoffer Almaas, however, based on own interview data with VAV and distinct focus on adaptive capacity. The paper is a part of the project TECNOCRACI, funded by the Research Council of Norway (grant no. 03489).

References

Bosco, Camillo, Alberto Campisano, Carlo Modica, and Giuseppe Pezzinga. 2020. 'Application of Rehabilitation and Active Pressure Control Strategies for Leakage Reduction in a Case-Study Network'. *Water* 12 (8): 2215.

Bosco, Camillo, Gema Sakti Raspati, Kebebe Tefera, Harald Rishovd, and Rita Ugarelli. 2022. 'Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study'. *Water* 14 (23): 3895.

Bosco, Camillo, Carsten Thirsing, Martin Gilje Jaatun, and Rita Ugarelli. 2023. 'A Cyber-Physical All-Hazard Risk Management Approach: The Case of the Wastewater Treatment Plant of Copenhagen'. *Water* 15 (22): 3964.

Bour, Guillaume, Camillo Bosco, Rita Ugarelli, and Martin Gilje Jaatun. 2023. 'Water-Tight IoT–Just Add Security'. *Journal of Cybersecurity and Privacy* 3 (1): 76–94.

Campisano, Alberto, Carlo Modica, Fabrizio Musmeci, Camillo Bosco, and Aurora Gullotta. 2020. 'Laboratory Experiments and Simulation Analysis to Evaluate the Application Potential of Pressure Remote RTC in Water Distribution Networks'. *Water Research* 183 (September):116072.

Creaco, Enrico, Marco Franchini, and Ezio Todini. 2016. 'The Combined Use of Resilience and Loop Diameter Uniformity as a Good Indirect Measure of Network Reliability'. *Urban Water Journal* 13 (2): 167–81.

Gleick, Peter, Viktor Vyshnevskyi, and Serhii Shevchuk. 2023. 'Rivers and Water Systems as Weapons and Casualties of the Russia-Ukraine War'. *Earth's Future* 11 (10): e2023EF003910.

Grindheim, Trude Haukeland, and Kristoffer Almaas. 2024. 'Resilienspotensialet i en digitalisert norsk vannsektor'. Master thesis, NTNU.

Grøtan, Tor Olav, Stian Antonsen, and Torgeir Kolstø Haavik. 2022. 'Cyber Resilience: A Pre-Understanding for an Abductive Research Agenda'. In *Resilience in a Digital Age*, edited by Florinda Matos, Paulo Maurício Selig, and Eder Henriqson, 205–29. Contributions to Management Science. Cham: Springer International Publishing.

Kurtz, C. F., and D. J. Snowden. 2003. 'The New Dynamics of Strategy: Sense-Making in a Complex and Complicated World'. *IBM Systems Journal* 42 (3): 462–83.

Meld. St. 9 (2024-2025). 'Totalberedskapsmeldingen - Forberedt på kriser og krig'. Justis- og beredskapsdepartementet. [online].

Norwegian Food Safety Authority. 2023. 'Sikre trygt drikkevann'. Mattilsynet. 28 April 2023. https://www.mattilsynet.no.

NSM. 2023. 'Nasjonalt Digitalt Risikobilde 2023'. Norwegian National Security Authority.

Oslo Municipality. 2024. 'Tildelingsbrev 2024 - Vann Og Avløpsetaten'. 23/5361-1. Byrådsavdeling for miljø og samferdsel.

PST. 2024. 'Nasjonal Trusselvurdering 2024'. Politiets sikkerhetstjeneste (PST). [online].

Rousso, Benny Z., Nhu C. Do, Li Gao, Ian Monks, Wenyan Wu, Rodney A. Stewart, Martin F. Lambert, and Jinzhe Gong. 2024. 'Transitioning Practices of Water Utilities from Reactive to Proactive: Leveraging Australian Best Practices in Digital Technologies and Data Analytics'. *Journal of Hydrology* 641 (September):131808.

Sandström, Erik. 2024. 'Flera inbrott i finländska vattenverk under sommaren – det här vet vi nu'. *Yle*, 12 July 2024, sec. Inrikes. https://yle.fi/a/7-10060468.

SWM. 2025. 'Water Sector Cybersecurity in 2024: High Stakes and Urgent Responses'. Text. Smart Water Magazine. Smart Water Magazine. 3 January 2025. [online].

Ugarelli, Rita. 2021. 'Cybersecurity Importance in the Water Sector and the Contribution of the STOP-IT Project'. In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*, edited by John Soldatos, Isabel Praça, and Aleksandar Jovanović, 145–58. Now Publishers.

VAV. 2023. 'Årsberetning 2023'. Oslo City, Agency for Water and Wastewater Services.

Woods, David D. 2018. 'The Theory of Graceful Extensibility: Basic Rules That Govern Adaptive Systems'. *Environment Systems and Decisions* 38 (4): 433–57.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. Sage Publications Inc.