Under Pressure: Securing Europe's Resource-Constrained Critical Infrastructure

Max Smeets, Gijs van Loon, James Shires,
and Apolline Rolland

Virtual Routes

June 2025

This report is sponsored by

UNDER PRESSURE: SECURING EUROPE'S RESOURCE-CONSTRAINED CRITICAL INFRASTRUCTURE

Virtual Routes | www.virtual-routes.org
Design & Layout by YuYing Mak & Frank Wo | Edited by Katharine Khamhaengwong

Under Pressure: Securing Europe's Resource-Constrained Critical Infrastructure

Max Smeets, Gijs van Loon, James Shires,
and Apolline Rolland

Virtual Routes

June 2025

Executive Summary

There is a growing awareness that many critical infrastructure entities in Europe remain poorly equipped to defend against cyber threats. These organisations are essential to society but often lack the funding, personnel, and technical capabilities needed to meet expanding regulatory demands. While EU initiatives like the NIS2 Directive and the Cyber Resilience Act have advanced the European cybersecurity policy framework, their effectiveness depends on the ability of resource constrained entities to comply in practice.

This report identifies which parts of Europe's critical infrastructure are most in need of targeted cybersecurity support and outlines what forms of assistance would be most effective. It focuses in particular on the drinking water and wastewater sectors, which are increasingly exposed to cyber threats but receive limited investment and exhibit low cybersecurity maturity.

To explore this issue in depth, the report conducts a spotlight analysis of the drinking water and wastewater sectors. Though often grouped together, these two systems face distinct operational and cybersecurity challenges. Drinking water services tend to be small-scale and decentralised, while wastewater systems are more interconnected and environmentally sensitive. Both sectors suffer from poor cyber hygiene, limited staffing, aging infrastructure, and minimal coordination on threat intelligence.

The analysis documents a clear rise in cyber incidents targeting water infrastructure across Europe and beyond – including ransomware attacks, credential breaches, and attempted sabotage of treatment processes. These threats are amplified by inadequate remote access controls, legacy system vulnerabilities, and poor asset visibility.

In response, the report outlines a pathway to improved cybersecurity through a layered approach: improving basic cyber hygiene, enhancing asset visibility, deploying sector-specific safeguards, and developing crisis response plans. Throughout, the report emphasises the need for collaborative, cross-border support.

To advance this agenda, the report concludes with four policy recommendations for the EU:

Launch an EU Water-Cyber Hygiene Accelerator Program

Establish a grant-based accelerator to improve cyber hygiene in drinking and wastewater utilities, prioritizing multi-factor authentication, secure access, and regular patching. The program would combine sector-specific guidance from ENISA with financial support modeled after successful EU and US initiatives.

Establish a European Water Sector ISAC

Create a European Water ISAC to enable trusted information sharing, threat intelligence, and coordinated incident response among water utilities, regulators, and member-state CSIRTs, enhancing cross-border cyber resilience in the sector.

Mainstream Cyber Risk into Environmental and Public Health Governance of Europe's Water Systems

Integrate cybersecurity into EU water governance, ensuring cyber threats are accounted for in environmental and health regulations, water safety plans, and emergency preparedness strategies to protect water quality and public health.

Use Political Tools to Deter Malicious Activity Targeting Water Infrastructure

Leverage the Cyber Diplomacy Toolbox more actively against cyberattacks on water infrastructure. While it has been used for incidents like NotPetya and WannaCry, it remains underutilised for water sector attacks. Coordinated sanctions, public attributions, and diplomatic measures should be employed to signal that targeting water systems carries real consequences.

Table of Contents

Introduction

There is a growing awareness among policymakers about the inability of critical infrastructure entities to adequately mitigate cybersecurity risks. EU Commissioner for the Internal Market Thierry Breton notes:

> "Cybersecurity threats in critical sectors can have an impact on the everyday life of citizens, but also on businesses and public services throughout the EU.[1]

Many of the critical infrastructure entities in Europe face a dual challenge: they are attractive targets for attackers intending disruption or financial gain, due to their essential role in society, but often lack sufficient funding, skilled personnel, or advanced technical defences to counter cyber threats effectively. In other words, they are resource - constrained: both highly exposed and poorly equipped to respond to malicious cyber activity.

The European Union has taken significant steps through regulatory measures such as the Network and Information Security 2 Directive to enhance cybersecurity across member states. However, bridging the gap for resource constrained entities requires a more tailored approach. Policymakers must identify the most vulnerable critical infrastructure and ensure targeted support is provided where it will deliver the greatest benefit. The EU's diverse critical infrastructure landscape adds complexity, with wide disparities in cybersecurity readiness, regulatory frameworks, and funding models among member states.

This report has two primary objectives. First, it aims to identify specific subsets of critical infrastructure in Europe that are resource-constrained and should be prioritised for targeted cybersecurity assistance. The analysis finds that sectors such as banking and energy show relatively high levels of cybersecurity investment and maturity, whereas others – such as space, wastewater and drinking water – consistently report low spending, limited staff capacity, and reduced ability to respond to cyber threats.

[1] European Union Agency for Cybersecurity (ENISA), 'Cyber Europe tests the EU cyber preparedness in the energy sector,' June 20, 2024, https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector

Second, the report seeks to determine the types of cybersecurity assistance that would be most impactful in helping these sectors manage their vulnerabilities and improve their resilience to cyberattacks. We focus on drinking water and waste water as case studies, two sectors which the NIS2 directive outlines as highly critical, but have a low level of cybersecurity spending and maturity. Through a combination of regulatory review, sectoral analysis, expert surveys, and real-world incident data, the report assesses how cyber threats manifest across Europe's critical infrastructure, and what tailored interventions are most urgently needed. Spotlight analyses of the water sectors reveal a growing pattern of cyberattacks, a lack of baseline protections, and minimal coordination among operators.

To address these risks, the report concludes with actionable recommendations, including the establishment of a European Water Sector ISAC to improve threat sharing and the integration of environmental risk mitigation into cybersecurity planning. These proposals aim to help close the cybersecurity gap for Europe's most vulnerable – but essential – services.

EU Initiatives for Protecting Critical Infrastructure from Cyber Threats

Over time, the European Union (EU) has developed a framework to identify and protect critical infrastructure sectors essential for maintaining societal functions, public health, safety, and economic activities. This approach began with the European Programme for Critical Infrastructure Protection (EPCIP), introduced in 2006.[2] EPCIP emphasised an all-hazards approach, focusing on energy, transport, and Information and Communication Technology sectors, and required operators of critical infrastructure to develop operator security plans (OSPs). It also established other measures, such as an action plan, the Critical Infrastructure Warning Information Network (CIWIN), expert groups, information-sharing processes, and interdependency analysis.[3]

Timeline: Relevant EU initiatives, directives and legislation for critical infrastructure protection and cyber resilience

Introduced	Came into effect	Initiative / Directive / Regulation	Function
2006	N/A	The European Programme for Critical Infrastructure Protection (EPCIP)	Established a common EU approach to assess risks and improve the protection of critical infrastructures.
2008	2009	Council Directive 2008/114/EC	Created an EU process to identify and designate European critical infrastructures and enhance their security.
2016	2018	General Data Protection Regulation	Protection of personal data across sectors
2016	2016	NIS Directive	Introduced the first EU-wide framework to improve cybersecurity of essential services and digital infrastructure.

[2] European Commission, 'The European programme for critical infrastructure protection,' December 12, 2006, https://ec.europa.eu/commission/presscorner/detail/en/memo_06_477

[3] Ibid.

N/A	N/A	Cyber Diplomacy Toolbox	Framework for coordinated diplomatic responses to malicious cyber activities
2019	2019	EU Cybersecurity Act	Strengthened ENISA's mandate and established EU-wide certification schemes.
2020	2023	NIS2 Directive	Replaced the original NIS Directive, expanding its scope and enhancing oversight mechanisms.
2022	Proposed	Cyber Solidarity Act	Legislation to enhance EU capabilities to detect, prepare for and respond to cyber threats
2022	2024	Critical Entities Resilience Directive	Replace the 2008 directive with an all-hazards resilience framework
2022	2023/2025	Digital Operational Resilience Act (DORA)	Introduced cybersecurity framework for financial sector entities
2022	2024	Cyber Resilience Act	The first EU legislation to impose mandatory cybersecurity standards on products with digital components

The EPCIP laid the foundation for the adoption of Council Directive 2008/114/EC (European Critical Infrastructures Directive), which focused on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.[4] This Directive 'aims at building common tools and a common approach in the EU to critical infrastructure protection and resilience, taking better account of interdependencies between critical infrastructures, industry and state actors.'[5] The ECI Directive has since been repealed and replaced by the 2022 CER Directive (as discussed below).

Following early efforts like the ECI Directive, the EUs focus broadened to include the protection of personal data as a component of cyber resilience. Although primarily a data privacy law, GDPR is a binding regulation that has important cybersecurity implications across all sectors, including critical infrastructure. Adopted in 2016 and enforceable from May 2018, GDPR requires organisations to implement 'appropriate technical and

[4] Council of the European Union, 'Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,' December 8, 2008, https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng

organisational measures' to ensure the security of personal data (Article 32).[6] This effectively mandates robust cybersecurity practices for any critical service handling personal data (such as hospitals, finance, energy utilities with customer data) as part of compliance. GDPR also introduced a 72-hour personal data breach notification rule, forcing companies to have incident response plans.

In 2016, Directive 2016/1148, or the Directive on Security of Network and Information Systems, was also introduced. While the ECI Directive laid the groundwork for identifying and protecting critical infrastructure, the NIS Directive went beyond physical infrastructure to address the growing threats in the digital realm. The NIS Directive was 'the first comprehensive EU legislation aimed at boosting cybersecurity of network and information systems to safeguard vital services for the EU's economy and society.'[7] The NIS Directive introduced requirements for cyber resilience across a broader range of sectors, such as healthcare, digital services, and public administration. It extended obligations to operators of essential services and digital service providers, which were not covered by the ECI Directive.

In June 2019, the EU Cybersecurity Act came into force, seeking to strengthen the EU's cyber institutional and certification framework. First, it made the EU Agency for Cybersecurity (ENISA) a permanent agency with an enhanced mandate and resources (previously it had a time-limited mandate).[8] Second, the Act established the EU Cybersecurity Certification Framework for ICT products and services.[9] Certifications, which can be created for various categories of products, are voluntary unless otherwise required by EU law, but the framework harmonises standards across member states.[10]

Recognising the importance of the financial sector, the EU also advanced sector-specific legislation. In 2020, the Digital Operational Resilience Act was also proposed as part of the

---

[5] Ibid. However, by July 2019, the first evaluation of Council Directive 2008/114/EC revealed significant limitations. The European Commission determined that 'the directive is only partially effective and relevant, as the security context in which critical infrastructures operate has changed substantially since the time the directive entered into force.' In response, the Commission included a plan for enhanced critical infrastructure protection (CIP) in its 2020 work programme: European Parliament, 'European critical infrastructure: Revision of Directive 2008/114/EC,' February 3, 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662604

[6] Wojciech Rafał Wiewórowski, 'European data protection supervisor,' November 29, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XX1129(01)

[7] European Commission, 'NIS2 Directive: New rules on cybersecurity of network and information systems,' December 14, 2022, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[8] For a more detailed discussion on the evolution of ENISA see: Myriam Dunn Cavelty and Max Smeets, 'Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority', February 2, 2023, https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2173274. Also see: European Cyber Security Organisation, 'The EU Cybersecurity Act enters into force,' June 27, 2019, https://ecs-org.eu/the-eu-cybersecurity-act-enters-into-force

[9] European Commission, 'The EU Cybersecurity Act,' June 27, 2019, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[10] Also, in 2020, the EU introduced the Cybersecurity Toolbox, specifically aimed at addressing risks linked to the rollout of 5G networks. While more limited in scope, this toolbox marked an important step in defining coordinated national- and EU-level risk mitigation measures for critical technologies. It emphasised technical and non-technical controls and encouraged member states to assess suppliers based on security risk profiles, laying the foundation for future supply chain security approaches.

EU's Digital Finance Package (it was adopted in 2022 and came into force in early 2023).[11] The goal of DORA is to ensure that banks, insurance companies, investment firms, payment providers, and other financial entities can withstand and recover from ICT disruptions like cyber attacks. DORA also addresses ICT third-party risk by establishing an oversight regime for critical cloud and technology service providers to the financial sector.[12]

In December 2020, the Commission proposed revising NIS, resulting in the adoption of NIS2, which came into force in January 2023. NIS2 strengthens the EU's collective approach to cybersecurity by expanding its scope, clarifying requirements, and enhancing oversight mechanisms. It obligates Member States to bolster their cybersecurity capabilities, implement risk management practices, and adhere to reporting standards across a broader range of sectors. The directive also establishes rules for cooperation, information sharing, supervision, and the enforcement of cybersecurity measures.

The directive extends its coverage beyond the sectors included in NIS – such as energy, transport, healthcare, finance, water management, and digital infrastructure – to encompass new areas. These include providers of public electronic communication services, additional digital services like social media platforms, waste and wastewater management, critical product manufacturing, postal and courier services, public administration at all levels, and space-related activities. Medium-sized and large organisations operating in these critical sectors must implement effective cybersecurity risk management measures and report significant incidents to the appropriate national authorities.[15]

A more detailed overview of the critical infrastructure sectors in scope of the NIS2 is provided below. Note that the NIS2 makes a distinction between two categories: i) sectors of high criticality and ii) other critical sectors. Also, entities within the identified sectors are categorised as i) essential entities or ii) important entities, based on various factors such as size, sector, and criticality.

---

[11] European Insurance and Occupational Pensions Authority, 'Digital Operational Resilience Act (DORA),' January 17, 2025, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[12] Also see: Sebastian J. Barling et al, 'The EU's Digital Operational Resilience Act (DORA) – 2024 Update,' July 18, 2024, https://www.skadden.com/insights/publications/2024/07/the-eus-digital-operational-resilience-act

[13] Note that it was formally adopted on December 14, 2022.

[14] Also, under NIS2, Member States must develop and maintain a national cybersecurity strategy that addresses supply chain security, vulnerability management, and cybersecurity education and awareness. Additionally, they are required to compile and update a list of operators of essential services, ensuring these entities meet the directive's standards, see: European Commission, 'NIS2 Directive: New rules on cybersecurity of network and information systems,' December 14, 2022, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

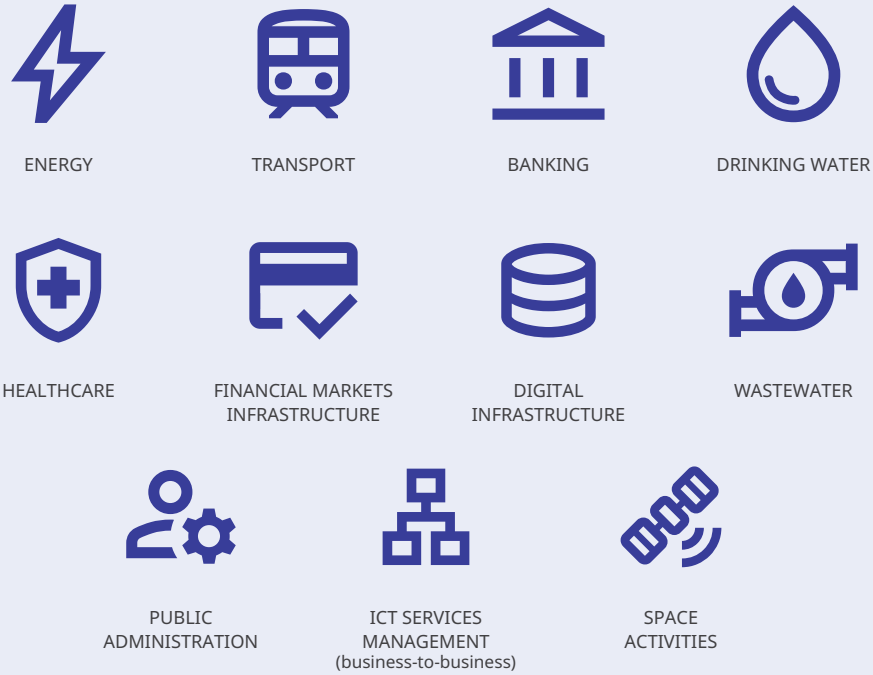
[15] Ibid.

Overview: When an organisation is covered by the NIS2 Directive

An organisation is covered by the NIS2 Directive if:

- it operates in one of the sectors listed in Annex I or Annex II of the NIS2 Directive, *and*
- it is a medium-sized organisation with at least 50 employees or an annual turnover or balance sheet total exceeding €10 million (qualifying it as an 'important entity'), *or*
- it is a large organisation with more than 250 employees, a net turnover exceeding €50 million, and a balance sheet total of more than €43 million (qualifying it as an 'essential entity').

Annex I of the NIS2 directive outlines the sectors considered highly critical:



Annex II of the NIS2 directive lists other critical sectors:

DIGITAL PROVIDERS

POSTAL AND COURIER SERVICES

MANUFACTURING

RESEARCH

WASTE MANAGEMENT

MANUFACTURING, PRODUCTION, AND DISTRIBUTION OF CHEMICALS

PRODUCTION, PROCESSING, AND DISTRIBUTION OF FOOD

The following micro and small businesses are automatically covered by the NIS2:

TRUST SERVICE PROVIDERS

TOP-LEVEL DOMAIN NAME REGISTRIES

DOMAIN NAME REGISTRATION SERVICE PROVIDERS

PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATION NETWORKS

PROVIDERS OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES

Government organisations active in the sectors listed above are also automatically covered by the NIS2 directive.[16]

Organisations covered by the NIS2 directive must adhere to several obligations:

- Duty of care: Conduct risk assessments and implement measures to ensure service continuity and protect operational information.
- Duty to report: Notify the relevant supervisory authority within 24 hours of incidents that significantly disrupt essential services. Cyber incidents must also be reported to the Cyber Security Incident Response Team (CSIRT).[17]
- Supervision: Organisations are subject to oversight to ensure compliance with the directive, including the duties of care and reporting.[18]

[16] Netherlands Enterprise Agency (RVO), 'Cybersecurity obligations for more companies in critical sectors,' March 25, 2025, https://business.gov.nl/amendment/nis2-directive-protects-network-information-systems/

[17] Reporting depends on factors such as the disruption's scale, duration, and financial impact.

[18] The assignment of supervisory bodies to specific sectors is ongoing. Also see: Netherlands Enterprise Agency (RVO), 'Cybersecurity obligations for more companies in critical sectors,' March 25, 2025, https://business.gov.nl/amendment/nis2-directive-protects-network-information-systems/

In the same year as legislators introduced the NIS2 Directive, the Critical Entities Resilience Directive was adopted, replacing the 2008 ECI Directive (it entered into force in January 2023).[19] This directive represents an 'all-hazards' approach to critical infrastructure resilience, covering both physical and cyber threats. In essence, it obliges Member States to identify critical entities in eleven essential sectors to ensure they take appropriate measures to prevent and recover from disruptive incidents (whether caused by cyberattacks, natural disasters, terrorism, or other emergencies).[20] The CER framework thus complements NIS2: while NIS2 focuses specifically on cybersecurity of network and information systems, CER covers a broader spectrum of threats to the continuity of essential services (including but not limited to cyber threats).[21]

While NIS2 and CER focus on securing essential services and ensuring the resilience of critical infrastructure operations, the Cyber Resilience Act (CRA) was introduced in 2024 to tackle cybersecurity deficiencies across critical and other sectors. The CRA establishes mandatory cybersecurity requirements for products with digital elements, such as IoT devices, software, and hardware.[22] In other words, the CRA seeks to address security at the product level, creating a baseline of protection for the technologies that underpin critical infrastructure.[23]

[19] European Commission, 'Critical infrastructure resilience at EU-level,' September 23, 2024,

https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en

[20] The eleven essential sectors are: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and food. Also, each Member State must adopt a national strategy for critical entities' resilience and perform regular risk assessments. Critical entities themselves must conduct risk assessments and implement 'technical, security and organisational measures' to boost resilience, including incident notification duties

[21] CER also introduces provisions for EU-level support and oversight – for example critical entities operating in multiple states can receive expert advice, and the Commission will build a Union-level overview of cross-border risks and best practices

[22] European Parliament and the Council of the European Union, 'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending regulations,' October 23, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

[23] CRA overlaps with the General Product Safety Regulation (GPSR) adopted in May 2023. GPSR incorporates cybersecurity as an element of product safety. The regulation is meant to fill any gaps left by sector-specific cybersecurity laws. Also see: https://products.cooley.com/2024/12/04/eus-general-product-safety-regulation-an-expanded-concept-of-safety/

EU Initiatives for Managing Cyber Crises Targeting Critical Infrastructure

In parallel to these regulatory developments and initiatives, the EU has progressively introduced mechanisms to improve its collective response to cyber incidents targeting critical infrastructure.

In June 2017, the EU ministers of foreign affairs endorsed the development of a framework for a joint EU diplomatic response to malicious cyber activities, known as the Cyber Diplomacy Toolbox (CDT).[24] As Erica Moret and Patryk Pawlak note, 'the primary intention behind the CDT – which includes, among a panoply of instruments, the imposition of sanctions – is to develop signalling and reactive capacities at an EU and member state level with the aim to influence the behaviour of potential aggressors, taking into account the necessity and proportionality of the response.'[25] In May 2019, the EU and its members also set up the EU framework for restrictive measures against cyberattacks threatening the EU, commonly known as the EU cyber sanctions regime.[26]

In 2020, as discussed, the European Union Agency for Cybersecurity (ENISA) was granted an expanded mandate under the EU Cybersecurity Act. It positions the organisation as a key actor with the EU's broader incident response ecosystem – complementing the Cyber Diplomacy Toolbox by providing technical expertise and operational coordination during major cyber crises.[27]

In 2023, the European Commission proposed the Cyber Solidarity Act, reflecting a shift toward deeper integration and mutual support in cybersecurity.[28] The Act includes three

[24] See for example this statement by the High Representative for Foreign Affairs calling out Russia for its activities against European government entities and critical infrastructure: Council of the European Union, 'Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation,' May 3, 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/

[25] Patryk Pawlak and Erica Moret, 'The EU Cyber Diplomacy Toolbox – Towards a cyber sanctions regime?,' July 21, 2017, https://op.europa.eu/en/publication-detail/-/publication/88cfb104-701b-11e7-b2f2-01aa75ed71a1/language-en

[26] Council of the European Union, 'Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its member states,' May 17, 2019, Decision - 2019/797 - EN - EUR-Lex; On the EU cyber sanction regime and its connection to the EU cyber diplomacy toolbox see: Adam Botek, 'European Union establishes a sanction regime for cyber-attacks,' https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/. For a discussion on effectiveness see: Stefan Soesanto, 'Inside the fourth EU cyber sanction package,' March 25, 2025, https://www.lawfaremedia.org/article/inside-the-fourth-eu-cyber-sanctions-package; Stefan Soesanto, 'After a year of silence, are EU cyber sanctions dead?', October 26, 2021, https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead

[27] For a more detailed discussion the challenges of this positioning see full article: Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority

[28] European Commission, 'The EU Solidarity Act,' April 14, 2023, https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

pillars. The first is the European Cyber Shield, composed of interconnected cross-border security operations centres (SOCs) that provide real-time threat detection and situational awareness. The second concerns a cybersecurity emergency mechanism, which funds preparedness efforts, joint incident response operations, and mutual assistance between Member States during large-scale incidents. The third is a cybersecurity incident review mechanism, designed to analyse major incidents post-facto and identify lessons learned to improve resilience. These initiatives mark a transition from cybersecurity as a primarily national competence to a shared European responsibility when it comes to responding to major cyber incidents.

In early 2025, the European Commission unveiled a sector-specific action plan to bolster cybersecurity in the healthcare sector and protect hospitals and providers from cyberattacks. The action plan integrates the NIS2 directive, Cyber Resilience Act, Cyber Solidarity Act, and the Cyber Diplomacy Toolbox, to prevent, detect, respond to, and deter cyberattacks against the frequently targeted sector.[29]

Taken together, the EU's regulatory frameworks and operational response mechanisms represent an increasingly comprehensive approach to protecting critical infrastructure from cyber threats. Yet, challenges remain. Not least, the diversity of critical infrastructure across member states, coupled with varying levels of cybersecurity maturity and funding mechanisms, creates gaps in resilience. Certain entities, particularly those classified as resource poor but target rich, lack the ability to defend themselves. Without tailored support mechanisms, there is a risk that existing regulations will benefit only those organisations already equipped to comply, while leaving the most vulnerable critical infrastructure exposed.[30] The next section of the report aims to address these limitations by identifying the most at-risk entities and the specific types of assistance most needed.

[29] European Commission, 'European action plan on the cybersecurity of hospitals and healthcare providers,' January 15, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_262

[30] Such as the aforementioned European action plan on the cybersecurity of hospitals and healthcare providers, Ibid.

Cybersecurity Spending and Maturity Across European Critical Infrastructure Sectors

In 2024, the European Union Agency for Cybersecurity (ENISA) released the fifth edition of its report on cybersecurity investments under the NIS Directive. The report is designed to provide policymakers with data-driven insights to evaluate the effectiveness of the EU's cybersecurity framework.[31] It specifically examines how the NIS Directive has impacted cybersecurity spending and the overall maturity of organisations within its scope. Drawing on data from 1,350 organisations across all 27 EU Member States, the report encompasses all sectors identified as highly critical under NIS2.[32] Aggregating the data from ENISA reveals distinct patterns in information technology (IT) and information security (IS) spending across sectors, with categories of high, medium, and low spenders.[33]

High-spending sectors such as banking, energy, and public administration allocate significantly more resources to IT, with average spending exceeding 100 million euros. Medium spenders like transport, health, and drinking water have lower average spending but maintain moderate investments in line with their operational needs. Low-spending sectors, including space, waste water, and financial market infrastructures, have limited resources for IT, with average spending below 50 million euros and medians indicating even tighter budgets for most organisations.

High Spenders on IT and IS	Medium Spenders on IT and IS	Low Spenders on IT and IS
Banking	Transport	Space
Energy	Health	Waste Water
Public Administration	ICT Service Management	Financial Market Infrastructures
	Digital Infrastructure	
	Drinking Water	

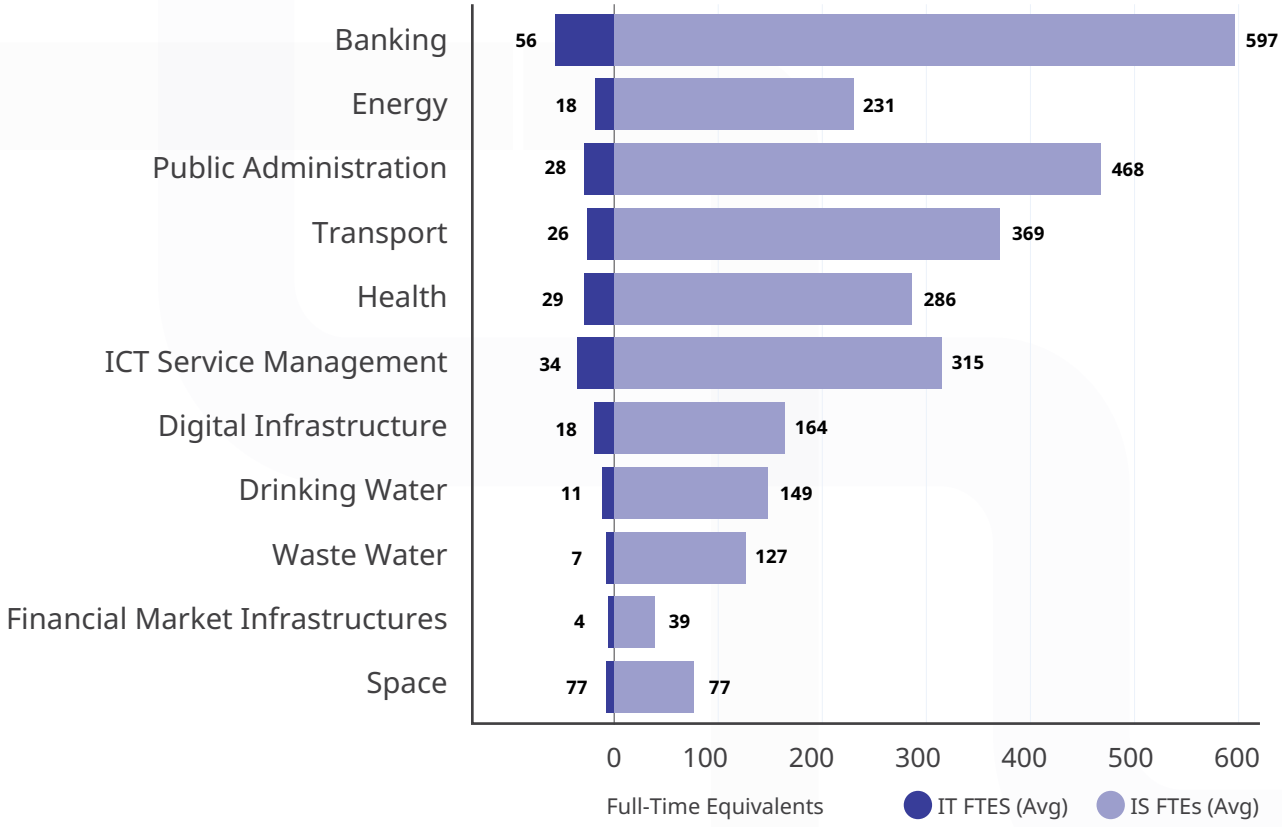
[31] European Union Agency for Cybersecurity (ENISA), 'NIS Investments 2024,' November 2024, https://www.enisa.europa.eu/publications/nis-investments-2024

[32] ENISA also surveyed the manufacturing industry, left out in this study as it is not considered as highly critical under NIS 2.

[33] However, as discussed, these observations come with important caveats, particularly regarding the lack of granular data on the sizes of organisations within these sectors.

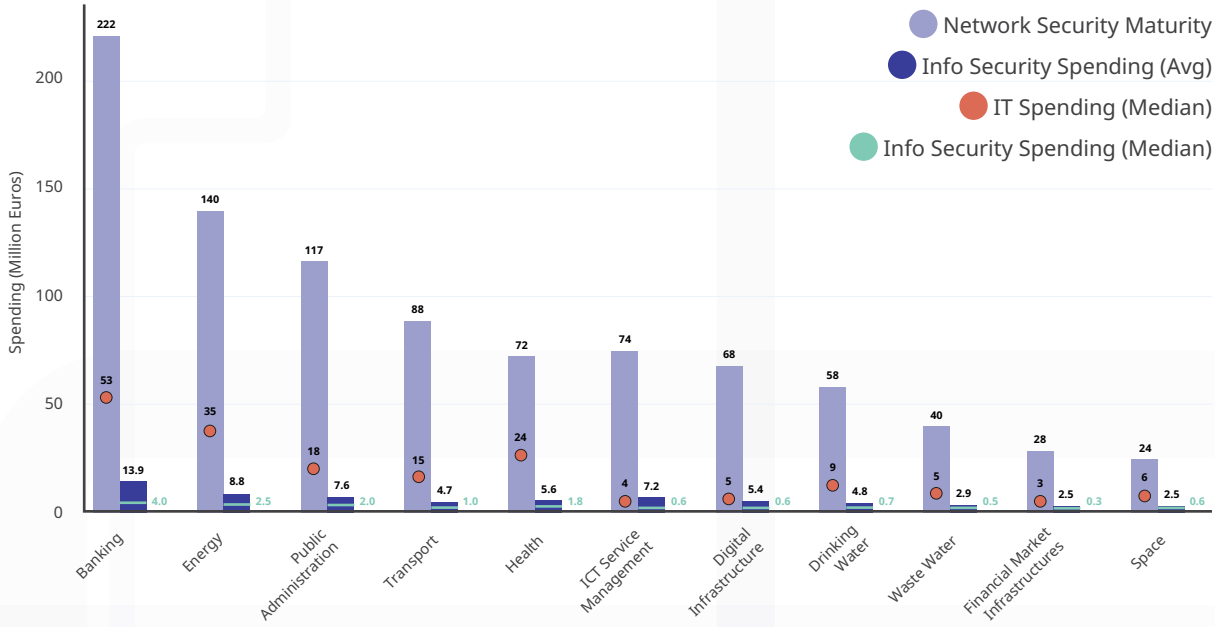
While IT spending correlates with full-time equivalent (FTE) counts, salary disparities may explain some differences. Banking employs an average of 597 IT FTEs and 56 IS FTEs, significantly outpacing sectors like space (average: 77 IT FTEs, 8 IS FTEs) and Waste Water (average: 127 IT FTEs, 7 IS FTEs). These disparities may suggest that high-spending sectors likely offer higher salaries and attract more specialised talent, further contributing to their cybersecurity maturity.

Figure 1: IT and IS FTEs, by Sector



When examining the allocation of IT budgets to information security, clear patterns emerge. Sectors with high IT spending also allocate significant resources to IS, but proportional spending varies. Some sectors, such as space, spend proportionately on IS despite low absolute spending (for space, 10.42% of IT budgets go to IS, almost exactly the median of 10%). Similarly, ICT service management allocates 9.73% of IT budgets to IS on average, with a remarkable median of 15%, likely due to the sector's reliance on service-level agreements and customer expectations for robust security. In contrast, transport allocates lower proportions, with an average of 5.34% respectively. This sector, while moderately digitised, may undervalue cybersecurity relative to other priorities. Such variations reflect differing perceptions of risk and the criticality of IT systems to sector-specific operations.

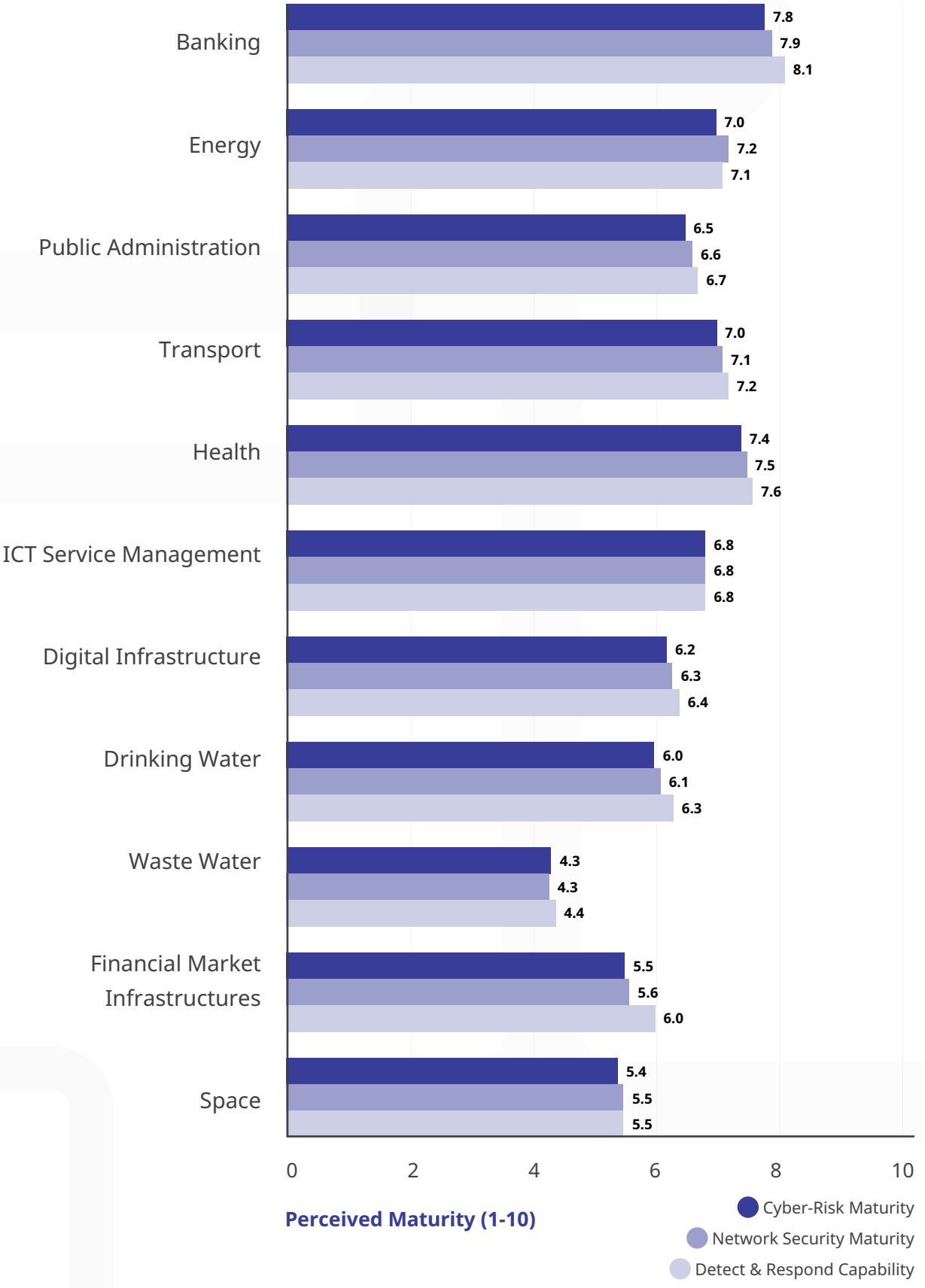
Figure 2: Information Technology and Information Security Spending, by Sector



However, simple spending data must be interpreted with caution. The European Union does not maintain a centralised database detailing the sizes of organisations within these sectors. As such, it is difficult to determine whether higher spending reflects sector-wide priorities or the dominance of larger organisations (such as multinationals in banking or energy). Conversely, lower spending in sectors like space or waste water might be a function of relatively smaller organisational size rather than a lack of cybersecurity focus. More importantly, the data measures spending levels but does not assess their outcomes. High-spending sectors may still face vulnerabilities if investments are misaligned or inefficient, while low-spending sectors might achieve proportionate resilience through outsourcing or other cost-effective strategies.

Given these caveats, it is helpful to combine spending data with self-reported perceptions of cybersecurity maturity also collected in the survey. Data on cybersecurity maturity provides valuable context for spending patterns, even if it also may reflect biases (like overconfidence in high-spending sectors or underestimation in low-spending ones). This data shows that high-spending sectors like banking and energy report correspondingly high maturity scores. For instance, banking has a cyber-risk maturity score of 7.8 (on a scale from 1-10) and network security maturity of 7.9, suggesting that organisations in this sector perceive themselves as well-prepared to manage threats. In contrast, low-spending sectors like waste water and space report much lower scores, with waste water at 4.3 for both cyber-risk and network security maturity, and space at 5.4 and 5.5, respectively.

Figure 3: Perceived Cybersecurity Maturity, by Sector



Threats to Critical Infrastructure in Europe

Critical infrastructure sectors in Europe face different risks. The table below shows the results based on an expert survey conducted with 57 participants from various sectors, including academia, government, and private industry, all specialising in cybersecurity and critical infrastructure protection.[34] This survey asked participants about the type of cyber threats each sector faces, and asked for further feedback on each sector. The survey distinguished between three categories:

Espionage (Including IP Theft): Focused on unauthorised access to steal information or surveil systems without necessarily disrupting operations.

Disruptive or Destructive Attacks: Aimed at impairing, damaging, or destroying systems or operations, with effects that could range from temporary service outages to irreversible damage.

Ransomware/Digital Extortion: Combines system compromise with financial extortion, either by encrypting data, threatening data leaks, or both. These malicious activities are typically conducted by criminal groups.

The survey aimed to assess perceived risks for these different types of cyberattacks across key sectors in Europe. Participants were asked to rate the risk levels - scale from 0 (no risk) to 10 (highest risk) – for each type of cyber threat across 12 critical infrastructure sectors. Definitions for each cyber threat type were provided to ensure consistency in understanding. Responses were averaged to identify the dominant perceived risk level for each sector and attack type.

[34] 22.8% from the private sector (including cybersecurity firms, critical infrastructure operators), 15% from government or public administration (including Critical Entities Resilience (CER) Directives, policy experts), 58% from academia and think tanks; 5.26% from 'other'. 76% operating in Europe.

Figure 4: Perceived Risk per Critical Infrastructure, by Sector

	THREAT TYPE		
	Espionage	Disruption/ Destruction	Ransomware/ Extortion
Banking	6	5.9	7
Energy	6.3	7.3	6.4
Public Administration	7.8	6.8	6.7
Transport	5.4	6.6	6.3
Healthcare	5.4	6.1	7.4
ICT Service Management	6.8	6.8	6.8
Digital Infrastructure	7.5	7	6.7
Drinking Water	4.4	6.5	6.5
Waste Water	4.7	6.5	6.3
Financial Market Infrastructures	7	6.4	6.6
Space	7.3	6.1	5.9

The survey results reveal clear variation in how different sectors perceive cyber threats – variation that often aligns with public awareness of major incidents. Ransomware/ extortion is viewed as a particularly severe threat in both healthcare and banking.[35] In healthcare, the risk is not only financial: disruptions can directly affect patient care, delay urgent procedures, and endanger lives. This helps explain the consistently high threat perception. The 2023 ransomware attack on Synnovis, a major healthcare services provider for the UK National Health Service (NHS), caused widespread disruption to hospital operations, led to thousands of cancelled procedures, and made national headlines for weeks.[36] Similarly, a 2024 ransomware campaign in Romania impacted 25 hospitals and forced dozens more to shut down systems preemptively.[37]

[35] For a discussion on ransomware's general impact on national security see: Max Smeets, *Ransom War: How cyber crime became a threat to national security,* (Hurst & Company, 2025)

[36] For a detailed overview see: National Health Service (NHS) England-London, 'Weekly Data,' September, 2024, https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/weekly-data/

[37] Sergiu Gatlan, 'Ransomware attack forces 100 Romanian hospitals to go offline,' February 12, 2024, https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-100-romanian-hospitals-to-go-offline/

Espionage threats, by contrast, are perceived as more sector specific. Public administration, digital infrastructure, and space are seen as particularly exposed. These perceptions might have been shaped by the particularly widely covered activity of Salt Typhoon, an advanced persistent threat (APT) group linked to China's Ministry of State Security (MSS) which compromised multiple US telecommunications networks to collect data on American individuals.[38]

Perceptions of disruption and destruction threats also reflect past headline events. The 2015 and 2016 cyberattacks on Ukraine's power grid, which led to major blackouts during winter months, remain among the most frequently cited examples of destructive cyber activity against critical infrastructure.[39] More recently, the 2023 Predatory Sparrow attack on Iran's train services, petrol stations, and ultimately a steel plant, demonstrated how cyber operations can have highly visible, physical consequences.[41] Sectors like transport, ICT services, and digital infrastructure are similarly rated as disruption prone.[41]

[38] For early reporting on Salt Typhoon see: Devlin Barret, 'What to know about the Chinese hackers who targeted the 2024 campaign,' October 26, 2024, https://www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html ; Also see: Erica Lonergan and Michael Poznansky, 'A tale of two typhoons: Properly diagnosing Chinese cyber threats,' February 25, 2025, https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/; There have of course also been other widely covered incidents, such as the 2024 breach of the UK Ministry of Defence, which compromised the credentials of hundreds of personnel, see: Richard Holmes, 'Russian hacking software used to steal hundreds of MoD log-ins,' November 29, 2024, //inews.co.uk/news/russian-hacking-software-steal-mod-log-ins-3406382

[39] See: Andy Greenberg, Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers (Random House USA Inc, 2019); For further discussion on Russia's activity see: Dan Black, 'Russia ushers in a new era of cyber-physical attack,' November 14, 2023, https://bindinghook.com/articles-hooked-on-trends/russia-ushers-in-a-new-era-of-cyber-physical-attack/

[40] James Shires, Max Smeets, and Hannah-Sophie Weber, 'Predatory Sparrow: Cyber sabotage with a conscience?,' December 9, 2024, https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/

[41] These patterns were echoed in expert interviews, which reinforced that ransomware threats are driven by financial incentives, while espionage and disruption threats often reflect strategic or geopolitical motivations.

Spotlight Analyses: The Waste Water and Drinking Water Sector

We conduct a spotlight analysis of two critical sectors: the drinking water and wastewater sectors. We do this for three main reasons. First, despite their importance, these sectors have received limited attention in EU-level cybersecurity reporting and policy efforts, especially when compared to other critical sectors such as healthcare or energy. This has left a significant analytical and policy gap. Second, as our analysis shows, both sectors consistently rank at the bottom in terms of cyber maturity and investment across the EU. Third, while they are generally perceived as low-value targets for espionage, they are widely seen as vulnerable to disruption and extortion – particularly through ransomware – which can have serious consequences for public health and environmental safety. These sectors are often grouped together under the broader label of the 'water sector', and indeed there is significant operational and regulatory overlap.[42] Many utilities – such as German Stadtwerke or Dutch water boards – manage both drinking and wastewater services, and the sectors are tightly linked through shared infrastructure and natural systems. There are EU-level regulations distinct to each sector, as well as some combined directives. The Water Framework Directive provides an overarching structure that explicitly links the Drinking Water Directive, the Urban Waste-water Treatment Directive, and the Sewage Sludge Directive, while the Environmental Quality Standards Directive applies to both sectors.[43]

> "Treating waste water and drinking water as one risks obscuring key differences.

[42] NIS2Directive, 'Essential Entity: Water Supply Sector' March 2023, https://nis2directive.eu/water/#:~:text=The%20NIS2%20directive%20places%20significant,remain%20resilient%20to%20cyber%20threats.

[43] European Commission, 'Water Framework Directive,' accessed March 13, 2025, https://environment.ec.europa.eu/topics/water/water-framework-directive_en; European Parliament and the Council of the European Union, 'Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy,' October 23, 2000,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0060-20141120; Also note that treatment plants for drinking and wastewater are often separate due to different processes involved, whilst tertiary treatment of wastewater may make wastewater suitable for drinking again, see: JMARK Systems; 'What's the difference between water and wastewater treatment?' accessed March 12, 2025, https://www.jmarksystems.com/blog/whats-the-difference-between-water-and-wastewater-treatment

Drinking water systems focus on supply reliability and quality control, while wastewater systems prioritise managing environmental risks and industrial pollutants. These differences not only shape their operational demands but also create distinct cybersecurity challenges – making a comparative spotlight analysis both necessary and valuable.

This spotlight analysis is structured around three components. First, we map the ecosystem of each sector to understand the key actors, systems, and (digital) interdependencies involved in the provision and management of drinking and wastewater services. Second, we conduct threat and incident diagnostics, drawing on public reporting and expert sources to trace how cyber threats have affected these sectors in recent years. Third, we outline pathways to improved cybersecurity, offering both sector-wide and entity-specific recommendations to address the distinct operational vulnerabilities of each sector and build resilience against future threats.

Spotlight Analysis Waste Water & Drinking Water Components

1	2	3
Mapping ecosystem	Threat and incident diagnostics	Pathways to cybersecurity

Mapping the Drinking Water and Wastewater Ecosystems and Their Cyber Risks

The drinking water ecosystem in the European Union encompasses entities responsible for ensuring the supply of safe and clean drinking water to residential, industrial, and commercial users. The drinking water sector encompasses all activities from raw water abstraction to treatment and distribution of potable water to consumers. Key players in this ecosystem include water utilities and providers, such as Veolia (France) and Thames Water (UK), which manage the sourcing, treatment, and distribution of potable water. These are supported by water treatment plants, such as Berlin Waterworks (Germany) and Águas de Portugal, which purify raw water to meet stringent EU quality standards. Governance and oversight are provided by municipal water authorities, which manage local water networks, and regulatory agencies, including the European Environment Agency (EEA), which ensure compliance with EU water quality directives. Additionally, the ecosystem includes private water suppliers, such as Evian and Nestlé Waters, offering bottled water and other specialised services.

While the EU establishes common water quality and safety requirements, the cybersecurity governance of drinking water systems varies significantly across Member

States. A comparative case study of the Netherlands and France – provided in the Case Study Box below – illustrates this variation. Both countries view drinking water as critical to national security and public health, yet they pursue distinct institutional models. The Netherlands prioritises full public control, centralised oversight, and strong integration of cybersecurity into statutory planning. Its small number of large utilities allows for consistent implementation and sector-wide coordination. France, in contrast, governs a fragmented and largely privatised system through contractual obligations and critical operator designations. This makes enforcement more uneven and dependent on contract strength, operator maturity, and regulatory capacity. Both models have strengths – public accountability and coherence in the Dutch case, private sector technical capacity in the French – but each must adapt as the EU's NIS2 Directive pushes toward more harmonised cybersecurity standards across essential services.

Comparative Case Study: Drinking Water Ecosystems and Cybersecurity, Netherlands vs. France

In the Netherlands, the drinking water sector consists of ten regional public water companies, each with a statutory monopoly over its service area.[44] These utilities are owned by municipalities and provinces, and they are legally obligated to ensure continuous delivery of safe drinking water. They operate under the Drinking Water Act, which mandates supply planning, service continuity, and quality control.

Cybersecurity is a regulated component of the water companies' mandatory four-year supply plans. The Human Environment and Transport Inspectorate (ILT) supervises these plans, evaluating whether cyber threats have been adequately assessed and mitigated. Additionally, the National Cyber Security Centre (NCSC-NL) works with the Water-ISAC, an information-sharing hub that connects the water utilities with national authorities and sector experts.[46]

France's drinking water system reflects a municipally led, contractually delegated model. While the majority of French municipalities manage the water provision directly, many have delegated daily operations to private companies, such as Veolia and Suez. Municipalities do, however, retain legal responsibility for ensuring water provision.[47] Such arrangements are formalised through 'public service delegation

[44] Jeroen Bezem, 'ILT niet bezorgd over cybersecurity Nederlandse waterbedrijven,' February 16, 2021, https://www.waterforum.net/ilt-cybersecurity-nederlandse-waterbedrijven-is-in-orde

[45] Ibid.

[46] Hudson Cybertec, 'Drinking water sector impressed with joint seminar Vewin and Water-ISAC,' accessed April 9, 2025, https://www.hudsoncybertec.com/en/2015/11/04/drinking-water-sector-impressed-with-joint-seminar-vewin-and-water-isac/

[47] Data from 2020, see: EauFrance, 'Observatory of public water and sanitations services in France: Overview of the services and of their performances,' June 2022, https://economie.eaufrance.fr/sites/default/files/2023-02/synthese_eaufrance_sispea_2020_anglais_vf.pdf

contracts,' in which local authorities set performance targets, determine tariffs, and maintain oversight.[48] The remaining share of services is managed by municipal régies (public utilities), with a growing interest in 'remunicipalisation' in some cities, such as Paris, which brought water operations back under direct public control in 2010.[49]

Regulatory responsibilities in France are distributed across different levels of government. At the national level, the French government defines standards for water quality, continuity of service and resource preservation. Municipalities must comply with these standards, as they are accountable for the water quality and the service provided. Local governments play a central role in negotiating and enforcing service contracts and monitoring performance, ensuring the contracted party (if any) upholds quality standards and adequate service levels. The Ministry of Ecological Transition, Biodiversity, Forests, the Sea, and Fisheries oversees abstraction licensing and environmental compliance, for example through the Code de l'environment, which is enforced and controlled by the French Water Police.[50]

Cybersecurity governance in the sector is embedded within France's critical infrastructure protection framework. Large drinking water operators are designated as operators of vital importance (OIV) by the French Cyber Security Agency (ANSSI).[51] As such, they are required to implement operator security plans (OSP), which detail both physical and cyber risk mitigation strategies.[52] These operators must also designate a dedicated security liaison and comply with the technical standards established by ANSSI.[53]

---

[48] 'Contrats de délégation de service public' are similar to public-private partnerships (PPPs), except that payment is made by users – through the operation of the service – rather than by the public authority, as is generally the case with PPPs. In addition, the financial and operational risks are transferred to the private contractors.

[49] Geert de Clercq, 'Paris' return to public water supplies makes waves beyond France,' July 8, 2014, https://www.reuters.com/article/markets/pariss-return-to-public-water-supplies-makes-waves-beyond-france-idUSL6N0PE572/; EurEau, 'The governance of water services in Europe,' September 29, 2020, https://www.eureau.org/resources/publications/150-report-on-the-governance-of-water-services-in-europe/file

[50] Ministry of Ecological Transition, Biodiversity, Forests, the Sea, and Fisheries, 'Gestion de l'eau,' accessed on April 16, 2025, https://www.ecologie.gouv.fr/politiques-publiques/gestion-leau-france; EurEau, 'The governance of water services in Europe,' September 29, 2020, https://www.eureau.org/resources/publications/150-report-on-the-governance-of-water-services-in-europe/file

[51] See: l'ANSSI, 'Le Dispositif SAIV,' August 18, 2022, https://cyber.gouv.fr/le-dispositif-saiv; The Secretary General of Defense and National Security, 'Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense,' June 17, 2016, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032749580

[52] Pascale Meeschaert, 'Cybersécurité : un enjeu élevé, des difficultés réelles mais des opérateurs qui ont décidé d'investir,' February 28, 2021, https://www.revue-ein.com/article/cybersecurite-reduire-les-vulnerabilites-des-systemes-m2m

[53] Additionally, those classified as operators of essential services (OES) under the EU NIS Directive must report cyber incidents and may be subject to regular audits and oversight by national authorities. Also see: Marcello Michael Serrano, 'Increase cybersecurity resilience using advanced data-science techniques for operators training,' November 8, 2024, https://smartwatermagazine.com/blogs/marcello-michael-serrao/increase-cyber-security-resilience-using-advanced-data-science

When it comes to cybersecurity, drinking water utilities operate key infrastructures such as intake facilities, treatment plants (for filtration and disinfection), pumping stations, storage reservoirs, and extensive distribution networks. These components are monitored and controlled via supervisory control and data acquisition (SCADA) systems – part of a broader class of industrial control systems (ICS) – to enable real-time management of flow, pressure, and water quality. The push for efficiency has led water providers to increasingly integrate ICT and automation.[54] Remote telemetry, IoT sensors (for leak detection, quality monitoring), and centralised SCADA allow operators to manage geographically dispersed facilities. While this digitalisation improves productivity, it 'makes [the sector] increasingly vulnerable to malicious cyberattacks or accidental cyber incidents,' as noted by Dimitra Markopoulou and Vagelis Papakonstantinou, researchers at the Vrije Universiteit Brussel.[55] Not all technological innovations in the sector are coupled with a necessary focus on cybersecurity, and outdated legacy systems are still prevalent.[56] As Xavier Cardeña from HMS Networks, a Swedish company that develops and manufactures products for industrial communication and IIoT (Industrial Internet of Things), notes, 'In the past there has been little awareness about OT cyber risks in the water sector. Many assets operated as an island, with little connection to the outside world, so difficult to attack, but now with the introduction of digitalisation and automation, the risks are much higher. There is the intention to connect legacy systems to new systems, but the former are not well prepared. And it's difficult to find ways to manage that.'[57] The sector also faces structural vulnerabilities: decentralised operations and resource constraints mean that smaller utilities often lack mature cybersecurity capabilities.[58]

The wastewater sector, in turn, manages collection, treatment, and safe discharge of sewage and industrial wastewater. There are almost 20,000 urban wastewater treatment plants (WWTPs) across the EU which process wastewater to remove contaminants before discharge.[59] Supporting these plants are sewerage authorities, like the Paris

[54] In other words, like in other sectors, for the drinking water sector, there is a trend towards convergence of operational technology (OT) and information technology IT-systems, see: Palo Alto Networks, 'What is IT/OT Convergence?', accessed March 12, 2025, https://www.paloaltonetworks.co.uk/cyberpedia/what-is-it-ot-convergence; Xavier Cardeña and Thomas Vasen, 'Whitepaper - NIS 2 and cybersecurity for OT operations in water industry: Unboxing the NIS 2 directive: Elevating cybersecurity to a top priority for water & wastewater companies,' July, 2025, https://media.hms-networks.com/image/upload/v1708430018/Documents/Whitepapers/NIS2_and_Cybersecurity_for_OT_Operations_in_Water_Industry_EN.pdf;

NIS2Directive, 'Essential Entity: Water Supply Sector,' March 2023, https://nis2directive.eu/water/#:~:text=The%20NIS2%20directive%20places%20significant,remain%20resilient%20to%20cyber%20threats

[55] Dimitra Markapolou and Vagelis Papakonstantinou, 'Digitalisation of water services and the water sector cyber threat landscape: Is the EU regulatory framework adequate?' November 1, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968932

[56] The issue of an often absent cybersecurity focus in digitalisation efforts came up in interviews with Xavier Cardeña (HMS Networks) and Eric Gervais (SKion Water)

[57] Interview Xavier Cardeña, HMS Networks, March 27, 2025

[58] Supported by interviews with Martin Silic (EurEau), Daniel Peregrina (Deltares), and Lessie Skiba, Kinsey Yow, and Matias Casas (Cyber Readiness Institute).

[59] European Environment Agency, 'Urban waste water directive treatment plants data viewer,' accessed March 13, 2025, https://www.eea.europa.eu/en/analysis/maps-and-charts/urban-waste-water-directive-treatment-data-viewer-urban-wastewater-treatment-directive-1

Sewerage Authority (SIAAP), which oversee the collection and transport of wastewater. The networks of wastewater treatment and sewerage systems vary in size and scope, ranging from metropolitan infrastructures serving densely populated areas, to smaller systems supporting small rural communities.[60] The ecosystem also includes industrial wastewater facilities, such as BASF's WWTP in Germany, which address the unique challenges of treating wastewater generated by specific industries.[61] Furthermore, stormwater management entities, like Amsterdam's municipal programs, prevent urban runoff from polluting waterways.

In the wastewater sector, we also see different governance structures, operational fragmentation, and cybersecurity integration within the EU. The comparative case box shows how Germany follows a decentralised, municipally based model with thousands of local operators, while Denmark has implemented a centralised and corporatised utility structure, consolidating service delivery into fewer, larger entities.

Comparative Case Study: Wastewater Ecosystems and Cybersecurity, Germany vs. Denmark

Germany's wastewater sector is characterised by a high degree of decentralisation (it is one of the most decentralised water systems in Europe). Responsibility for wastewater collection and treatment lies with municipalities, which typically operate their own treatment plants or collaborate through inter-municipal associations. Many local utilities operate as integrated 'Stadtwerke' that manage multiple services – including water, energy, and transportation – for their respective regions. Regulatory oversight is similarly decentralised. Municipalities are responsible for service delivery and infrastructure investment, while state-level (Länder) environmental agencies enforce compliance with national- and EU-level environmental standards, such as discharge limits under the Water Framework Directive. National industry associations – such as the German Association for Water, Wastewater, and Waste (DWA) and the German Technical and Scientific Association for Gas and Water (DVGW) – play a coordinating role by developing technical rules and best practices across the sector.[62]

[60] Ibid.; This depiction of the wastewater sector was also supported by Lessie Skiba, Kinsey Yow, and Matias Casas (Cyber Readiness Institute) and Xavier Cardeña (HMS Networks)

[61] The wastewater treatment plant operated by BASF is among the largest in Europe and is the largest on the Rhine, see for more information: BASF, 'Big and clever - The waste water treatment plant,' 2025, https://www.basf.com/global/en/who-we-are/organisation/locations/europe/german-sites/ludwigshafen/neighbor-basf/environment-and-safety/waste-water-treatment

[62] Bundesverband der Energie- und Wasserwirtschaft, 'Profile of the German water sector,' April 22, 2021, https://www.bdew.de/presse/presseinformationen/profile-german-water-sector-published-english

Cybersecurity governance in Germany is built around the country's critical infrastructure protection framework. Wastewater treatment plants serving 500,000 or more inhabitants are classified as critical infrastructure and are subject to the requirements of the Federal Office for Information Security (BSI).[63] These operators must implement appropriate cybersecurity measures and demonstrate compliance with legal standards, primarily by aligning with a sector-specific security standard (B3S Wasser/Abwasser) developed by DWA and DVGW.[64] However, the vast majority of smaller wastewater utilities fall below the threshold and are not directly regulated by BSI. As a result, cybersecurity maturity varies widely across the sector, with many smaller operators lacking the expertise, funding, or organisational capacity to adopt advanced cybersecurity practices.[65]

Denmark's wastewater sector presents a stark contrast to Germany's decentralised landscape. In 2009, Denmark undertook a significant reform of its water sector, requiring all municipal water and wastewater services to be corporatised into publicly owned companies operating under commercial principles.[66] This reform reduced the number of wastewater providers and led to the creation of larger, regionally focused utilities – such as BIOFOS in Copenhagen and Aarhus Vand – aiming to deliver services more efficiently across multiple municipalities.[67]

This consolidation seeks to enable greater consistency and efficiency, not only in service delivery and environmental performance but also in risk management. Regulatory oversight is coordinated at the national level through the Danish Environmental Protection Agency (under the Ministry of Environment), which sets discharge standards and oversees compliance. Economic oversight is provided by the Danish Utility Regulator, which aims to ensure that prices remain fair and performance remains high through benchmarking and annual reporting requirements.[68]

---

[63] OpenKRITIS, 'Wasser und Abwasser,' accessed on April 9, 2025, https://www.openkritis.de/it-sicherheitsgesetz/sektor_wasser.html

[64] Operators must also report major cyber incidents to BSI and are subject to audits and assessments. Also see: Uwe Marquardt et al, 'Nutzung des branchenspezifischen Sicherheitsstandards Wasser/Abwasser (B3S WA) in Verbundunternehmen,' November 30, 2018, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/Wasser/B3S-WA-in-Verbundunternehmen/b3s-wa-in-verbundunternehmen_node.html

[65] Initiatives such as UP KRITIS – a public-private partnership for critical infrastructure protection – provide voluntary support and guidance, but participation is uneven and largely concentrated among larger players. OpenKRITIS, 'Wasser und Abwasser,' accessed on April 9, 2025, https://www.openkritis.de/it-sicherheitsgesetz/sektor_wasser.html; also see: Nicolas Caradot et al, 'Cybersicherheit im Wassersektor: Analyse der zukünftigen Entwicklung der Wasser- un Abwasserinfrastruktur,' 2022, ttps://www.kompetenz-wasser.de/media/pages/forschung/projekte/cybersecurity/b30308e077-1702890607/cybersicherheit-im-wassersektor.pdf

[66] Eva Moll Sørensen, 'The Danish water sector reform - economic efficiency and central-local relations,' July 2010, https://www.vive.dk/media/pure/9892/2078549

[67] Today, a significant portion of Denmark's wastewater is treated by a relatively small number of centralised facilities, with 50% of national wastewater processed at just 31 plants, see: State of Green, 'The structure of the Danish wastewater sector,' accessed on April 9, 2025, https://stateofgreen.com/en/news/the-structure-of-the-danish-wastewater-sector

Cyberattacks on the wastewater sector could have significant consequences. Wastewater operations are energy intensive and depend on continuous power (for pumps and aerators, for example) and on communication links to coordinate remote lift stations.[69] Power failures or outages caused by malicious cyber activity can quickly lead to sewage backups or uncontrolled overflows, with environmental and public health consequences. As with drinking water systems, we have seen a convergence of operational technology (OT) and information technology (IT) - e.g.

> SCADA systems enable a small team to supervise many remote pumping stations, while advanced treatment processes rely on computer-controlled equipment. This connectivity, however, expands the attack surface and increases the risk of malicious cyber activity.[70]

Dragos Inc., an industrial cybersecurity firm, reported that in 2021–2022, 83% of water and wastewater organisations they assessed had undocumented or uncontrolled external connections into OT environments (often connections from the corporate network or even direct internet links to equipment). In many cases, these connections exist for legitimate reasons – such as remote support by vendors or inter-site connectivity – but are not properly secured or monitored.

> The Dragos analysis noted that no assessed water utilities had OT network monitoring in place up through 2022.[71]

[68] Eva Moll Sørensen, 'The Danish water sector reform - economic efficiency and central-local relations,' July 2010, https://www.vive.dk/media/pure/9892/2078549; Danish Environmental Protection Agency, 'Waste water' accessed on April 9, 2025, https://eng.mst.dk/water/waste-water; EurEau, 'The governance of water services in Europe,' September 29, 2020, https://www.eureau.org/resources/publications/150-report-on-the-governance-of-water-services-in-europe/file

[69] See for example: Alexandros Maziotis et al, 'A comprehensive assessment of energy efficiency of wastewater treatment plants: An efficiency analysis tree approach,' August 10, 2023, https://www.sciencedirect.com/science/article/pii/S0048969723021587?via%3Dihub

[70] Also see NIS2Directive, 'Essential Entity: Water Supply Sector,' March 2023, https://nis2directive.eu/water/#:~:text=The%20NIS2%20directive%20places%20significant,remain%20resilient%20to%20cyber%20threats; Marnix Dekker et al, 'ENISA NIS360 2024,' February 2025, https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf; and The Netherlands Ministry of Infrastructure and Water Management, 'Beleidsnota Drinkwater (2021-2026),' April 2021, https://open.overheid.nl/documenten/ronl-ae2317be-417a-409f-bd2d-59ec08a55620/pdf

[71] Water ISAC, '2022 Dragos ICS/OT cybersecurity year in review - insights on new activity groups, industrial ransomware and ICS/OT vulnerabilities,' February 16, 2023, accessed on April 10, 2025, https://www.waterisac.org/portal/2022-dragos-icsot-cybersecurity-year-review-%E2%80%93-insights-new-activity-groups-industrial

Furthermore, it frequently runs on legacy software, with few or no updates since initial installation.

Limited cybersecurity staffing and resources across the water sector amplify all the above risks. Many water treatment facilities, operated by small municipal departments or regional authorities, do not have dedicated IT security teams.[72] This resource gap means that known vulnerabilities may remain unaddressed simply due to lack of expertise or funding. It also means incident response is ad hoc.[73] In addition, as Inga Sokk from the Estonian Information System Authority notes, 'cyber awareness and readiness is generally low across the sector and this increases the risk for human error'.

Cyber Attacks Against the Drinking and Waste Water Sector

Over the past five years, the water and wastewater sector across the world has experienced a concerning rise in cyber incidents, ranging from nation-state sabotage attempts to financially motivated ransomware attacks. Below we provide a timeline with the most notable incidents from 2020-2025. It highlights key cases of ransomware attacks, disruptions, and espionage, with attribution to criminal groups, state-linked actors, and hacktivists. Together, these incidents illustrate a clear and growing threat.

In early 2020, Israel was hit by a series of cyber intrusions into its water infrastructure. These attacks, attributed to Iranian state-linked actors, sought to manipulate chemical dosing at water treatment facilities – an overt attempt to endanger public water supplies.[74] Defence measures prevented disaster, but follow-on attacks in June and July 2020 demonstrated a persistent campaign against Israeli water systems.[75] Meanwhile, water utilities in the United States have increasingly been targeted by cybercriminals and unattributed hackers. In 2021 alone, at least four US water treatment plants, in New Jersey, Nevada, Maine, and California, were hit with ransomware.[76]

---

[72] This aspect also came up frequently in our interviews, including with Inga Sokk (Estonian Information System Authority), Martin Silic (EurEau), Eric Gervais (SKion Water), Xavier Cardeña (HMS Networks), and Lessie Skiba, Kinsey Yow, and Matias Casas (Cyber Readiness Institute).

[73] Furthermore as Eric Gervais at SKion Water noted, 'The level of cybersecurity awareness and maturity varies tremendously across the sector. There is still a mentality prevailing that cyber threats might not apply to us. Whereas, the consequences of something going wrong in our sector can be detrimental to human life and public health.' Interview, April 16, 2025.

[74] Kevin Groves, 'Fighting the rising tide: Cyber crime and the water supply,' March 12, 2024, https://thomasmurray.com/cyber-series/fighting-rising-tide-cyber-crime-and-water-supply

[75] JD Work and Richard Harknett, 'Troubled vision: Understanding recent Israeli-Iranian offensive cyber exchanges,' July 22, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/#:~:text=Additional%2C%20as%20yet%20technically%20unattributed,Quds%20Electronic%20Army%20launches

[76] Cybersecurity and Infrastructure Security Agency, 'Ongoing cyber threats to U.S. water and wastewater systems,' October 25, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

Europe has not been spared either. In the UK, South Staffordshire Water suffered a ransomware breach in August 2022 that compromised customer data.[77] The following year, Portugal's second-largest city, Porto, saw its water utility knocked offline by a LockBit ransomware attack – an incident contained without service outages – and Alto Calora Servizi SpA became victim of Medusa ransomware (see Case Study Box).[78] Furthermore, in early 2024, Southern Water in England revealed a Black Basta ransomware infiltration that led to data theft from its systems.[79]

Case Study: Alto Calore Servizi SpA Ransomware Attack

On April 28, 2023, Alto Calore Servizi SpA (ACS), a publicly owned utility serving approximately 500,000 residents across 125 municipalities in Italy's Avellino and Benevento provinces, suffered a ransomware attack that rendered all of its IT systems inoperable.[80] While water distribution services remained unaffected, the attack severely disrupted administrative operations, preventing access to databases and halting functions such as customer service and billing. 'It will not be possible to carry out any operations or provide information that requires querying the database,' the company said in a statement.[81]

The Medusa ransomware group claimed responsibility for the attack. The Medusa ransomware group is a collective that operates a ransomware-as-a-service (RaaS) model. This structure enables affiliates – individuals or groups who partner with Medusa – to access the malware and supporting infrastructure needed to launch ransomware campaigns.[82] While the precise method used to breach the victim's network remains undisclosed, Medusa is known for employing a range of tactics, techniques, and procedures (TTPs). These often include exploiting internet-facing

[77] The attack was initially misreported as hitting the larger Thames Water. Alexander Martin. 'Ransomware group may have stolen customer bank details from British water company,' December 1, 2022. https://therecord.media/ransomware-group-may-have-stolen-customer-bank-details-from-british-water-company

[78] Jonathan Greig, 'LockBit gang takes credit for attack on water utility in Portugal,' February 21, 2023, https://therecord.media/porto-portugal-water-utility-cyberattack-lockbit

[79] Connor Jones, 'UK water giant admits attackers broke into system as gang holds it to ransom,' January 23, 2024, https://www.theregister.com/2024/01/23/southern_water_confirms_cyberattack

[80] Jonathan Greig, 'Italian water supplier serving 500,000 people hit with ransomware attack,' May 3, 2023, https://therecord.media/italian-water-supplier-ransomware-attack-disruptions-medusa

[81] Ibid. Also see; ISS Source, 'Ransomware attack at Italian water supplier,' May 22, 2023, https://www.isssource.com/ransomware-attack-at-italian-water-supplier/

[82] Maria Geronikolou, 'Darktrace investigation into Medusa ransomware,' June 10, 2024, https://www.darktrace.com/blog/medusa-ransomware-looking-cyber-threats-in-the-eye-with-darktrace; Anthony Galiette and Doel Santos, 'Medusa ransomware turning your files into stone,' January 11, 2024, https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/

systems with known vulnerabilities and compromising legitimate administrative accounts at both local and domain levels. Their ransomware is frequently distributed through phishing and spear phishing emails, which contain malicious attachments designed to deliver the payload.

Medusa claimed to have exfiltrated a significant amount of sensitive data from ACS, including customer information, contracts, internal reports, minutes from board meetings, and details about the company's pipe distribution and expansion plans. The group demanded a ransom of $100,000 for the deletion of the stolen data, offering a $10,000 extension to delay its publication by one day. A countdown timer was posted on their leak site, pressuring ACS to comply with their demands.[83]

Timeline

March 2019

Victim: Kansas-based WWS facility
Country: US
Attribution: Insider threat
Type: Disruption
Water type: Drinking water and waste water
Description: A former employee attempted to remotely access a plant computer using unrevoked credentials to threaten the drinking water supply, but the attempt was unsuccessful.

April 2020

Victim: Israeli water facilities
Country: Israel
Attribution: Unknown
Type: Disruption
Water type: Drinking water
Description: ICS systems at five Israeli water authorities were targeted in a campaign (likely by Iran) to manipulate chlorine. Prompt detection averted a potential crisis.

[83] The company issued a public statement acknowledging the incident and apologising for the outage, indicating that updates on system restoration would be communicated through press releases. There was no immediate confirmation on whether ACS intended to pay the ransom. Italian water supplier serving 500,000 people hit with ransomware attack | The Record from Recorded Future News

September 2020

Victim: New Jersey-based WWS
Country: US
Attribution: Makop ransomware
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Personnel at a WWS facility based in New Jersey discovered that potential ransomware Makop had compromised files on their system.

January 2021

Victim: Bay Area Utility Hack
Country: US
Attribution: Unknown
Type: Disruption
Water type: Drinking water
Description: A hacker used a former employee's TeamViewer credentials to gain access to a Bay Area wastewater treatment plant and delete critical treatment programs, but the flaw was detected the next day with no public damage reported.

February 2021

Victim: Oldsmar Water Treatment Plant
Country: US
Attribution: Human Error
Type: Human error
Water type: Waste water
Description: Oldsmar plant narrowly avoided contamination after SCADA was accessed and sodium hydroxide levels were altered. Incident initially thought to be an external hack later linked to poor IT hygiene and potential human error.

March 2021

Victim: Nevada-based WWS facility
Country: US
Attribution: Unknown ransomware
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: A Nevada water facility was hit with unknown ransomware that impacted both SCADA and backup systems, disrupting monitoring but not full control operations.

May 2021

Victim: Volue Technology
Country: Norway
Attribution: Ryuk ransomware group
Type: Ransomware/Extortion
Water type: Drinking water
Description: Volue Technology, a Norwegian industrial software provider for water utilities, was compromised by Ryuk ransomware in May 2021. The malware infection affected IT systems and spread into networks of approximately 200 municipal water supply companies that depended on Volue's software. Though water supply itself was not directly impacted, the incident highlighted the supply-chain vulnerabilities and risks to operational continuity from third-party providers.

July 2021

Victim: Maine-based WWS facility
Country: US
Attribution: ZuCaNo ransomware
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Hackers used remote access to deploy ZuCaNo ransomware on a Maine wastewater SCADA system, forcing the facility to operate manually until systems were restored

August 2021

Victim: California-based WWS facility
Country: US
Attribution: Ghost variant ransomware
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Hackers deployed Ghost variant ransomware at a California water facility, which went undetected for a month until 3 SCADA servers showed a ransom message.

2022 to 2024

Victim: Multiple OT systems in NA and Europe
Country: Multiple
Attribution: Russian hacktivist group
Type: Disruption
Water type: Drinking water and waste water
Description: Russian-aligned hacktivists conducted operations on water, wastewater, energy, and food sector OT systems between 2022-2024. Tactics included data wiping, DDoS, and leaks. Governments reported limited disruptions, but systemic weaknesses were exposed.

August 2022

Victim: South Staffordshire Water
Country: United Kingdom
Attribution: Clop ransomware group
Type: Ransomware/Extortion
Water type: Drinking water
Description: Clop ransomware hit South Staffordshire, disrupting corporate IT. Initially misidentified as Thames Water, the gang stole and published customer data. Water supply services remained unaffected.

April 2022

Victim: Reitzner AG/Donau Stadtwerke
Country: Germany
Attribution: LockBit rannsomware
Type: Ransomware/Extortion
Water type: Waste water
Description: Lockbit 2.0 ransomware struck Reitzner AG, disrupting electricity, water, and sewage services in multiple municipalities via IT supplier dependency.

August 2022

Victim: South Staffordshire Water
Country: United Kingdom
Attribution: Clop ransomware group
Type: Ransomware/Extortion
Water type: Drinking water
Description: Clop exfiltrated personal and banking information from South Staffordshire Water again. Leak misattributed initially to Thames Water.

February 2023

Victim: Aguas e Energia do Porto
Country: Portugal
Attribution: LockBit ransomware group
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Porto's main utility was hit by LockBit ransomware. LockBit added the entity to its leak site, demanding payment. Services continued as normal, and national cybersecurity teams were involved in mitigation.

February 2023

Victim: Municipality of Rodgau
Country: Germany
Attribution: Unknown
Type: Disruption
Water type: Drinking water and waste water
Description: Cyber incident in Rodgau disrupted municipal systems including utilities. Wastewater and sewage services remained operational.

April 2023

Victim: Alto Calore Servizi SpA
Country: Italy
Attribution: Medusa ransomware group
Type: Ransomware/Extortion
Description: Italian water utility Alto Calore Servizi was breached by Medusa group. The incident involved data exfiltration and temporary service disruptions.

November 2023

Victim: Aliquippa Water Plant (PA)
Country: US
Attribution: Cyber Avengers (or CyberAv3ngers) (Iran-linked)
Type: Disruption
Water type: Waste water
Description: Iran-linked group Cyber Avengers targeted a water pressure pump system supplied by an Israeli manufacturer. The message stated all Israeli-made OT equipment is a 'legal target'. The US Treasury later sanctioned Iranian officials over related campaigns.

November 2023

Victim: Drum/Binghamstown Water Co-op
Country: Ireland
Attribution: Cyber Avengers (or CyberAv3ngers) (Iran-linked)
Type: Disruption
Water type: Waste water
Description: The Cyber Avengers hacktivist group attacked an Irish water co-op. Operations were disrupted but resumed shortly after incident response.

November 2023

Victim: Service Public de l'Assainissement Francilien
Country: France
Attribution: Unknown
Type: Disruption
Water type: Waste water
Description: Cyberattack knocked offline key IT systems at the public sanitation agency in Ile-de-France. Limited service was maintained during restoration.

December 2023

Victim: Aqualectra
Country: Curaçao
Attribution: Akira ransomware
Type: Disruption
Water type: Drinking water and waste water
Description: Aqualectra, a power and water utility in Curaçao, experienced a cyberattack that disrupted internal systems and access to customer portals. Water delivery and electric grid functions continued without major interruptions.

December 2023

Victim: Rsvodokanal
Country: Russia
Attribution: Blackjack (Ukraine)
Type: Disruption
Water type: Drinking water and waste water
Description: Ukrainian-linked hacking group Blackjack deleted over 50TB of data and affected 6000 systems at the Russian water utility Rsvodokanal. Allegedly conducted with support from Ukrainian Security Service of Ukraine.

December 2023

Victim: Koh Brothers Eco Engineering Ltd.
Country: Singapore
Attribution: Unknown
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Koh Brothers, a firm specialising in water and wastewater treatment engineering, suffered data encryption and exfiltration in a targeted cyber incident.

February 2024

Victim: Southern Water
Country: United Kingdom
Attribution: Black Basta ransomware group
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: Southern Water faced a breach from Black Basta. Data, including IDs and personal details, was leaked. Water services were not impacted, but digital systems were compromised, prompting major response efforts.

January 2024

Victim: Veolia North America
Country: US
Attribution: Unknown
Type: Ransomware/Extortion
Water type: Drinking water and waste water
Description: A ransomware attack on Veolia North America disrupted billing and digital customer interfaces. Core water treatment operations were unaffected.

March 18, 2024

Victim: Fanø Vand
Country: Denmark
Attribution: Unknown
Type: Espionage/Disruption
Water type: Drinking water and waste water
Description: Consumer data services of Danish water provider Fanø Vand were breached, resulting in data theft and operational hijack. Little public detail is available on the breach extent or remediation timeline.

April 2024

Victim: Moscolletor
Country: Russia
Attribution: Blackjack (Ukraine)
Type: Disruption
Water type: Waste water
Description: Blackjack group disrupted Moscow's sewage monitoring network Moscolletor. Claimed destruction of 70 servers, 90TB of data, and over 80,000 sensors disabled.

April 2024

Victim: Tipton West Wastewater Treatment Plant
Country: US
Attribution: Cyber Army of Russia
Type: Disruption
Water type: Waste water
Description: Hacktivists tampered with the wastewater facility's SCADA systems. A Telegram video by Cyber Army of Russia claimed successful interference with automated fluid control operations at Tipton West, Indiana.

August 2024

Victim: Stanton Water Department
Country: US
Attribution: Cyber Army of Russia
Type: Disruption
Water type: Drinking water
Description: Russian hacktivist group Cyber Army of Russia claimed responsibility for compromising systems at the Stanton Water Department. While specific operational effects remain unclear, this incident is part of a broader campaign targeting small US water entities.

September 2024

Victim: Arkansas City Water Treatment Facility
Country: US
Attribution: Hazard Ransomware
Type: Ransomware/Extortion
Water type: Drinking water
Description: A ransomware attack forced the Arkansas City, Kansas water treatment facility to switch to manual operations. Systems were encrypted and data likely stolen. Water quality and delivery were not affected due to swift manual response.

September 2024

Victim: Catalan Waste Agency (ACR)
Country: Spain
Attribution: ProLock ransomware
Type: Ransomware/Extortion
Water type: Waste water
Description: Unknown threat actors targeted the Catalan Waste Agency in Spain. Their waste documentation system and some internal systems were affected by a ransomware attack. The scope was limited, but core administrative operations were temporarily impacted.

October 3, 2024

Victim: American Water Works
Country: US
Attribution: Unknown
Type: Disruption
Water type: Drinking water and waste water
Description: American Water Works, the largest publicly traded water utility in the US, experienced unauthorised access that caused operational disruptions. The company shut down part of its systems as a precaution. Though details remain limited, security analysts suspect a ransomware-style attack, though no ransom was publicly acknowledged.

January 11, 2025

Victim: Water for People
Country: US
Attribution:Medusa ransomware group
Type: Ransomware/Extortion
Water type: Drinking water
Description: Medusa ransomware group targeted the clean-water-focused NGO Water for People. The breach reportedly encrypted files, though no impact to operations or fieldwork was disclosed.

Overall, the water sector has been tested by cyber attacks of escalating frequency and severity. A challenging part of water sector cybersecurity is that defenders must now counter both nation-state actors and cyber criminals.[84] The above cases illustrate that both large and small water providers in Europe are now squarely in cybercriminals' sights for digital extortion. These criminal operations typically seek to encrypt and steal sensitive data, betting that the critical nature of water services will pressure victims to pay. While most ransomware-related outages in water plants have been confined to business IT systems or monitoring SCADA systems (not causing direct physical disasters), the risk is significant. An infiltration by a ransomware group that disables treatment automation or blinds operators' visibility could indirectly jeopardise water safety. The financial impact is non-trivial as well – Southern Water in the UK, for instance, incurred approximately £4.5 million in costs from the ransomware attack.[85]

The water sector, and especially the wastewater sector, has come under increased pressure during or in the aftermath of critical geopolitical events.[86] Incidents directly targeting wastewater treatment plants, sewage systems, and utility providers have taken place during the Russia-Ukraine war. Russian hacktivist and state-affiliated groups targeted North American and European wastewater facilities, allegedly over their support for Ukraine, while Ukraine has successfully targeted Russian wastewater infrastructure at least twice. Similarly, in the aftermath of the October 7 event in Israel and the war in Gaza, Iranian-linked groups have directly targeted the wastewater sector when there were Israeli manufacturers involved. These incidents have thus mostly been ideologically motivated and carried out by hacktivist groups, often with alleged backing from state actors.

Despite the range of actors, many cyber attacks on water and wastewater systems have exploited a common set of TTPs. A recurring theme is attackers taking advantage of remote access into operational networks.[87] For example, in the Bay Area utility incident, the hacker in the Bay Area intrusion used an old TeamViewer credential to remotely connect and delete critical programs.[88] Another prominent technique is spearphishing on IT

[84] Also, several incidents show that insiders and rogue employees continue to pose a cybersecurity risk. The 2021 Bay Area breach was enabled by an ex-employee's unused remote login, as was another case in 2020 where an insider at a Florida water utility planted malware after termination.

[85] Smart Water Magazine, 'Southern Water Reports £4.5M Cost from Ransomware Attack,' February 28, 2025, https://smartwatermagazine.com/news/smart-water-magazine/southern-water-reports-ps45m-cost-ransomware-attack

[86] For a broader discussion on how cyber operations are linked to geopolitical events see: Dan Black, 'Russia ushers in a new era of cyber-physical attack,' November 14, 2023, https://bindinghook.com/articles-hooked-on-trends/russia-ushers-in-a-new-era-of-cyber-physical-attack/; Taylor Grossman et al, 'The Cyber Dimensions of the Russia-Ukraine War,' April 2023, https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

[87] Note that initial reporting also suggested that the Oldsmar incident in Florida was caused by attackers leveraging remote desktop software which turned out not to be the case. See: Anna Ribeiro, 'Oldsmar water treatment plant incident allegedly caused by human error, not remote access cybersecurity breach,' April 4, 2023, https://industrialcyber.co/utilities-energy-power-water-waste/oldsmar-water-treatment-plant-incident-allegedly-caused-by-human-error-not-remote-access-cybersecurity-breach/.

[88] What the incidents also show is that attackers often turn existing admin tools against the system (for example, using VNC/TeamViewer to manually click through control software) instead of using custom malware for industrial control systems. See: Peter Chawaga, 'Public revelation of Bay Area utility hack latest in growing trend for drinking water systems,' July 1, 2021, https://www.wateronline.com/doc/public-revelation-of-bay-area-utility-hack-latest-in-growing-trend-for-drinking-water-systems-0001

networks as a path to further escalate access.[89] For example, the Ryuk ransomware attack on Volue Technology in Norway likely started by infiltrating the IT side of the company (as Ryuk often does via phishing) and then spread to customer-facing applications used by water providers.[90] If the IT and OT environments are interconnected or not properly segregated, the attacker can even pivot to industrial control systems from gaining initial access in the business environment through a phishing email or other access. Credential compromise is another cross-cutting technique. The Cl0p ransomware group claimed responsibility for the cyberattack on South Staffordshire Water, discussed above, asserting they had access to critical systems that control water treatment processes. They released screenshots displaying compromised credentials, highlighting the exploitation of weak or reused passwords.[91] Similarly, when Cyber Avengers claimed responsibility for targeting Israeli-made Unitronics programmable logic controllers (PLCs) in October 2023 (see timeline), they likely exploited the fact that these PLCs were internet-facing, used default or no passwords, and operated on default ports.[92]

Pathways to Securing Waste Water and Drinking Water

The sections above have shown that there are both significant risks in the wastewater and drinking water sectors and that these threats are actively being exploited. The question is: what pathways can we develop to improve cybersecurity in these sectors? We propose a pathway to improved cybersecurity through a layered approach: improving basic cyber hygiene, enhancing asset visibility, deploying sector-tailored safeguards, and developing crisis response plans.

First, as in many other sectors, the initial step is to build a basic foundation of awareness and hygiene. It is clear that many organisations involved in drinking and wastewater management are still at a stage where simple measures can yield major risk reductions. Based on how cybercriminals have previously gained access, enforcing multi-factor authentication (MFA) on all remote access systems, auditing shared logins, reviewing old credentials, and locking down insecure remote desktop tools should be immediate priorities.

---

[89] For a more detailed description of this operational playbook see: Max Smeets, *Ransom War: How Cyber Crime Became a Threat to National Security*, Oxford University Press: 2025; and Max Smeets, 'The Ransomware Playbook and How to Disrupt It,' March 2025, Virtual-Routes-Pharos-Report-Series_No-1_The-Ransomware-Playbook-and-How-to-Disrupt-It.pdf.

[90] Khobeib Ben Boubaker, 'Twenty years of cyberattacks on the world of water,' August 30, 2021, https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water

[91] Paul Smith, 'Understanding the South Staffordshire Water cyber attack,' August 23, 2022,

https://blog.scadafence.com/south-staffs-water-attack

[92] Cybersecurity and Infrastructure Security Agency, 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities,' December 18, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Efforts to improve cyber hygiene in the drinking and wastewater sectors would benefit from being organised across different strata, rather than focusing solely on national or regional levels. Tailored messaging, sector-specific training, and practical guidance can better reflect the operational realities of different sub-sectors. This approach also fosters trust and communication between organisations that manage similar infrastructure layers and face common challenges.

Once a foundation is in place, the next step is improving visibility. Most drinking and wastewater providers do not maintain an inventory of their IT or OT assets. Without a clear picture of what systems are in use – or how they are connected – it is difficult to prioritise security improvements or detect intrusions. One way to address this is by developing and distributing simplified self-assessment tools that allow small operators to identify their critical systems, map out remote access points, and evaluate risks. Cloud-based platforms could further enhance these tools by enabling centralised data storage, real-time collaboration, and scalable analytics across operators.[93] To enhance the effectiveness of these assessments, they could be supported by mobile or virtual 'cyber clinics' that assist with implementation, particularly in under-resourced municipalities. That said, the kinds of visibility required vary: drinking water systems typically need to track quality sensors, chlorination systems, and pipeline telemetry, while wastewater systems must monitor complex treatment stages, aeration cycles, and stormwater inflows. These differences require tailored asset-mapping templates and risk prioritisation matrices.

The European Union's Horizon 2020 STOP-IT project has already worked to create a platform that supports these efforts by enabling water utilities to access real-time data from various sources within a unified environment.[94] This data can be viewed simultaneously by both operators and decision-makers, with multiple visualisation options designed to prevent information overload.

Third, with a clearer understanding of system architecture, drinking and wastewater organisations can begin to secure their operations. This includes implementing network segmentation to separate business and operational environments – protections still lacking in many organisations, as the research from Dragos has shown.[95] These steps may require technical support. One option is for national agencies or trusted integrators to offer publicly vetted, pre-configured SCADA security packages specifically tailored for

[93] For example, see the Open storm framework on sensing that incorporates cloud services: Matthew Bartos et al, 'Open storm: a complete framework for sensing and control of urban watersheds,' August 17, 2017, https://arxiv.org/abs/1708.05172?utm. Another example of a platform offering cloud deployment options is GE Digital's Smallworld: GE Vernova, 'Smallworld GNM: A complete, accurate network model,' accessed on April 11, 2025, https://www.gevernova.com/software/products/geospatial-network-management-smallworld-gis

[94] The STOP-IT project has ended. STOP-IT, 'The STOP-IT Platform,' accessed on April 4, 2025, https://stop-it-project.eu/results/stop-it-platform/

[95] Water ISAC, '2022 Dragos ICS/OT cybersecurity year in review'

small operators. Funding mechanisms, such as conditional grants, could help incentivise the adoption of these critical safeguards.

In parallel, governments and regulators should promote the use of standardised, accessible cybersecurity frameworks that help resource-constrained utilities implement core protections without needing extensive in-house expertise. A strong candidate for adaptation is the US WaterISAC's '15 Cybersecurity Fundamentals for Water and Wastewater Utilities', a widely used guide that offers practical, step-by-step measures across critical areas like remote access control, asset inventory, backup management, and incident response.[96] Though developed in a US context, the fundamental principles are broadly applicable and could be localised for the European landscape. Aligning this type of checklist with existing European standards – such as ISO/IEC 27019, which addresses security for industrial control systems in the utilities sector – gives even smaller operators a credible, manageable roadmap to follow.[97]

Fourth, even with these protections in place, these systems remain at risk. Planning for cyber incidents must therefore be a priority. Many utilities currently lack formal procedures for handling cyberattacks or ransomware events. Developing basic incident response plans, conducting tabletop exercises, and identifying key national or regional contacts (such as Critical Entities Resilience (such as CERTs or regulators) Directives or regulators) will improve crisis readiness. These plans do not need to be complex; they should be easy to follow, operationally relevant, and grounded in real-world scenarios.

Whereas cyber hygiene outreach may benefit most from an approach that targets different strata within the ecosystem, scenario planning workshops should be more regionally focused. This is because different entities within a region often need to respond jointly to a crisis. National authorities can support this by developing response templates and making them available through these regional workshops.[98]

[96] Water ISAC, 'Cybersecurity fundamentals for water and wastewater utilities,' December 19, 2025, accessed on April 9, 2025, https://www.waterisac.org/fundamentals

[97] ISO, 'ISO/IEC 27019:2024: Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry,' October, 2024, https://www.iso.org/standard/85056.html

[98] Also, as noted by Daniel Peregrina from Deltares, an institute for applied research in the water sector, cross-sector collaboration is important and can be further improved: 'The interdependence with other infrastructure sectors is important to think of. A [cyber] attack on drinking water supply, also affects other sectors. Cascades and interdependencies need to be prevented. How? We often work on complex models and systems, and intersectoral research with stakeholders from multiple sectors could be advisable. How do they depend on each other? Have that conversation. That's more valuable.' Interview April 2, 2025.

Policy Recommendations

Based on the analysis of the above sections, we provide four main policy recommendations. These policy recommendations aim to create a resilient approach to cybersecurity across the EU's drinking water and wastewater ecosystems.

Recommendation 1: Launch an EU Water-Cyber Hygiene Accelerator Program

The first step in the layered pathway outlined above is cyber hygiene: multi-factor authentication, secure remote access, basic asset inventories, and timely patching. As discussed, many drinking- and wastewater utilities, especially those serving small communities, still lack the funds and in-house expertise to implement even these fundamentals.

We recommend the creation of a water-cyber hygiene accelerator program to help close this gap. This accelerator program should borrow the grant logic of the US State and Local Cybersecurity Grant Program (SLCGP) – a scheme that channels roughly US $280 million per year to states and municipalities for baseline controls and workforce training.[99] It should also take inspiration from the EU's own 2025 Action Plan on the Cybersecurity of Hospitals and Healthcare Providers, which pairs technical guidance with an ENISA-run 'support-centre'.[100] This new accelerator should fuse the strongest features of both models. Like the SLCGP, it would create a dedicated, program-specific funding – ideally within the Digital Europe Programme.[101]

In addition to institutional support, the program should invest in capacity building through the creation of a new role: water cyber coaches. ENISA would take on a coordinating role to train approximately 150 coaches across the EU who would work closely with utilities to guide them through implementation. Coaches would be responsible for verifying that

[99] CISA, "State and Local Cybersecurity Grant Program, September 16, 2022, https://www.cisa.gov/cybergrants/slcgp?

[100] Specifically, as part of the action plan, the ENISA support centre seeks to 'develop new Procurement Guidelines reflecting recent trends such as the 'cloudification' of patient data. These guidelines will provide practical tools for hospitals and healthcare providers to track supply chains, including managed security service providers and third-party risk assessments.' Mark Young and David Brazil, 'European Commission Publishes Action Plan on Cybersecurity of Hospitals and Heathcare Providers,' *Covington*, January 22, 2025, https://www.insideeulifesciences.com/2025/01/22/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/

[101] The Digital Europe Programme is an EU funding initiative aimed at enhancing Europe's digital capacities in areas such as cybersecurity, artificial intelligence, and digital skills, with a total budget of €7.5 billion for 2021-2027.

baseline controls are in place before final grant disbursements are approved.[102] Evidence from the Cyber Readiness Institute's pilot program for water utilities in the United States suggests that having a dedicated coach dramatically increases completion rates of the cyber hygiene program – 72% with a coach present, compared to 11% and 41% in two other pilots without.[103]

Over time, the accelerator program could evolve into a permanent Water Cyber Support Centre, mirroring the institutional architecture created for the healthcare sector. The EU's 2025 Action Plan on the Cybersecurity of Hospitals and Healthcare Providers offers a useful precedent for how a sector-specific cybersecurity initiative could be embedded institutionally.[104] At the heart of the health plan is a centralised support centre managed by ENISA, which provides tailored implementation guidance, near real-time threat alerts, sector-specific training, and rapid response coordination. Establishing a similar centre for the water sector would ensure that technical resources, coaching infrastructure, and live assistance remain accessible to utilities even after the initial grant phase winds down.

Recommendation 2: Establish a European Water Sector ISAC

Information-sharing and analysis centres (ISACs) let organisations inside a sector exchange threat indicators, practical mitigation advice, and incident-response experience in a trusted setting. Europe already relies on sectoral ISACs such as the Rail ISAC, the Energy ISAC and the Health ISAC to bolster collective cyber resilience.[105] The drinking and wastewater sector still lacks such an EU-level forum.

A first attempt has already shown the value of one. The Horizon 2020 STOP-IT project (2017-2021) linked dozens of utilities, researchers, and vendors, proving that operators will collaborate when a collaborative platform exists.[106] Yet, the project ended when its research grant expired, and its portal is now largely dormant. Meanwhile, successful national initiatives – most prominently the Dutch Water ISAC – remain self-contained and do not provide the cross-border coordination that multi-state incidents increasingly demand.

---

[102] To increase participation, the program could include a volunteer surge capacity modelled on the DEFCON Franklin project, which aims to connect OT-security professionals with small US municipalities for penetration testing, incident triage, and tabletop exercises.

[103] CRI Team, 'Resiliency for Water Utilities Pilot Interim Report,' December 4, 2024, https://cyberreadinessinstitute.org/news-and-events/resiliency-for-water-utilities-pilot-interim-report/

[104] European Commission, 'European action plan on the cybersecurity of hospitals and healthcare providers', January 2025,

https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en

[105] RAIL-Information Sharing & Analysis Center, 'Rail ISAC,' accessed April 9, 2025, https://rail-isac.eu/; First, 'Health-ISAC,' accessed April 9, 2025, https://www.first.org/members/teams/health-isac; European Energy Information Sharing & Analysis Center, 'Network of trust,' accessed April 9, 2025, https://www.ee-isac.eu/

[106] STOP-IT, 'STOP-IT has come to an end, a European water-ISAC is born?' Accessed April 4, 2025, https://stop-it-project.eu/stop-it-has-come-to-an-end-a-european-water-isac-is-born

The European Commission should therefore instruct ENISA, working with Directorate-General for Migration and Home Affairs (DG HOME) and national water regulators, to help stand up a European Water ISAC as a permanent operational capability. The centre would connect national water ISACs (where they already exist), individual utilities, research institutes and member-state Computer Security Incident Response Team (CSIRT), redistributing vetted threat intelligence EU-wide and maintaining a repository of sector-specific mitigations – from patch guidance for common Programmable Logic Controllers to ready-made public-communications templates.

A three-year pilot, funded at roughly €6 million, would cover a secure platform, an analyst team, joint exercises, and outreach to smaller municipalities. €1 million of the pilot budget would be reserved for mini-grants (€10-40,000 each) to hire accredited consultancies to implement ISAC recommendations (such as network segmentation or logging) for small utilities. After the pilot, costs could shift to a modest, size-based membership levy, with the EU Solidarity Fund underwriting surge capacity during cross-border crises.

Governance should balance public oversight and operator expertise. A board comprising rotating national water authorities and utilities of different sizes would set priorities and ensure transparency. Participation in the ISAC should contribute toward fulfilling NIS2 'duty of care' obligations, encouraging broad involvement without mandating it outright.

Recommendation 3: Mainstream Cyber Risk into Environmental and Public Health Governance of Europe's Water Systems

Cyberattacks on drinking water and wastewater infrastructure carry not only operational and economic risks, but also the potential for significant ecological and public health harm, from chemical contamination and discharge failures to compromised water quality. Despite this, the environmental and health dimensions of cyber risk remain underdeveloped in most national- and EU-level planning frameworks.

Cybersecurity has been increasingly integrated into governance of other sectors– particularly in energy, healthcare, and transport – but the water sector continues to lag behind. Regulatory frameworks such as the EU Drinking Water Directive and the Urban Wastewater Treatment Directive already require comprehensive risk assessments and service continuity planning. Yet neither directly accounts for the types of digital threats that have become increasingly common across Europe.

This recommendation calls for greater integration of cybersecurity into environmental risk mitigation for the drinking water and wastewater sectors. It aligns with the goals of

the EU Green Deal and complements the EU's growing emphasis on climate resilience and environmental sustainability. It also supports the Directive on the Resilience of Critical Entities, which endorses an all-hazards approach against a broad range of risks – including those posed by cyber threats.

To make this actionable, we propose the following steps:

- The commission should issue guidance under Articles 8 and 9 of the Drinking Water Directive, requiring that all water safety plans include a dedicated module assessing cyber threats to water quality, service continuity, and population health. This guidance should be developed in consultation with ENISA and national public health authorities and come into effect no later than 2026.[107]
- A joint review of cyber incidents with environmental or public health implications should be undertaken by ENISA and the European Environment Agency, with results feeding into river basin management plans, national emergency preparedness strategies, and updates to the EU's Zero Pollution Action Plan.
- To support implementation at operator level, the EU should reserve at least €5 million in combined funding under the Horizon Europe programmes for pilot projects that develop and test joint cyber-environment and cyber-health emergency response protocols within the water sector.

Recommendation 4: Use Political Tools to Deter Malicious Activity Targeting Water Infrastructure

Improved cyber hygiene, planning, and technical safeguards are necessary steps to enhance the security of Europe's drinking and wastewater sectors. Yet, these efforts alone are insufficient. Without proactive political action to discourage malicious activity against the water sector, the threat landscape is unlikely to improve.

The EU and its member states should more actively use the full spectrum of tools provided by the Cyber Diplomacy Toolbox to impose consequences on perpetrators of cyberattacks against water infrastructure. While the Toolbox was activated to openly respond to major

[107] Under the EU Drinking Water Directive (Directive (EU) 2020/2184), Articles 8 and 9 establish a comprehensive risk-based approach to ensure the safety of drinking water throughout the supply chain. Article 8 focuses on the risk assessment and management of catchment areas for water abstraction points. It requires member states to identify potential sources of contamination in these areas and implement measures to prevent or mitigate risks to water quality. Article 9 addresses the risk assessment and management of the supply system, encompassing the abstraction, treatment, storage, and distribution of water. Water suppliers are mandated to conduct thorough assessments to identify hazards, including those arising from climate change, infrastructure vulnerabilities, and operational processes.

campaigns such as NotPetya and WannaCry, no assertive EU-level diplomatic response options – such as sanctions and public condemnations – have been used in response to incidents affecting water systems, despite dozens of attacks since 2020. This is a missed opportunity.

The 2024 pro-Russian hacktivist intrusion into France's wastewater systems, LockBit's ransomware breach of a Portuguese utility, and repeated attacks on Italian and Spanish providers show how water infrastructure is being probed for leverage. Even when attribution to a state is difficult, repeated targeting of critical infrastructure by non-state actors operating from known safe havens should prompt a coordinated diplomatic signal. The EU has already taken steps in this direction, such as its decision to impose cyber sanctions on six Russian cybercriminals in the summer of 2024 - and approach it could now build on.[108]

Also, while nation state cyber operations are often tacitly accepted means of espionage, drinking and wastewater infrastructure in particular are never appropriate targets for intelligence gathering, especially if the manner of intrusion could also serve as the basis for a disruptive cyberattack. Other cyber operations determined to be *prepositioning* for disruptive or destructive attacks on critical infrastructure should be regarded by EU members as a 'threat' of force prohibited by the UN Charter.

Several member states have taken action at the national level – for instance, Italy has proposed a ban on ransom payments for essential service providers.[109] But these actions remain fragmented. The EU should encourage a more unified approach, particularly when evidence suggests the involvement of foreign-based actors. A clearer, graduated response policy – drawing on coordinated attribution where feasible and followed by proportionate diplomatic measures – would signal that cyber attacks on water systems carry real consequences.

[108] Government of the Netherlands, 'EU imposes first ever sanctions on leading cybercriminals,' June 24, 2024, https://www.government.nl/latest/news/2024/06/24/eu-sanctions-leading-cybercriminals

[109] Cyber Guru, 'A new bill to attack ransomware,' May 5, 2025, https://www.cyberguru.it/en/2025/05/05/a-new-bill-to-attack-ransomware; Also see the new legislative proposals from the UK, which includes the option for a payment ban: UK Home Office, 'Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting,' March 26, 2025, https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible#

References

'A new bill to attack ransomware,' Cyber Guru, May 5, 2025, https://www.cyberguru.it/en/2025/05/05/a-new-bill-to-attack-ransomware

Barling, Sebastian J., Ken D. Kumayama, David A. Simon, Nicola Kerr-Shaw, and Susanne Werry. 'The EU's Digital Operational Resilience Act (DORA) – 2024 Update,' *Skadden Publication / Cybersecurity and Data Privacy Update*, July 18, 2024. https://www.skadden.com/insights/publications/2024/07/the-eus-digital-operational-resilience-act.

Barret, Devlin. 'What to know about the Chinese hackers who targeted the 2024 campaign,' *New York Times*, October 26, 2024. https://www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html.

Bartos, Matthew, Brandon Wong and Branko Kerkez. 'Open storm: a complete framework for sensing and control of urban watersheds,' Cornell University, August 17, 2017. https://arxiv.org/abs/1708.05172?utm.

BASF. 'Big and clever - The waste water treatment plant,' Environment & Safety (blog), April 2025. https://www.basf.com/global/en/who-we-are/organisation/locations/europe/german-sites/ludwigshafen/neighbor-basf/environment-and-safety/waste-water-treatment.

Ben Boubaker, Khobeib. 'Twenty years of cyberattacks on the world of water,' *Stormshield*, August 30, 2021. https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/.

Bezem, Jeroen. 'ILT niet bezorgd over cybersecurity Nederlandse waterbedrijven,' Waterforum, February 16, 2021. https://www.waterforum.net/ilt-cybersecurity-nederlandse-waterbedrijven-is-in-orde.

Black, Dan. 'Russia ushers in a new era of cyber-physical attack,' *Binding Hook*, November 14, 2023. https://bindinghook.com/articles-hooked-on-trends/russia-ushers-in-a-new-era-of-cyber-physical-attack/.

Botek, Adam. 'European Union establishes a sanction regime for cyber-attacks,' The NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

Bundesverband der Energie- und Wasserwirtschaft. 'Profile of the German water sector,' April 22, 2021. https://www.bdew.de/presse/presseinformationen/profile-german-water-sector-published-english.

Caradot, Nicholas, Nikolaus de Macedo Schäfer and Elina Henning. 'Cybersicherheit im Wassersektor: Analyse der zukünftigen Entwicklung der Wasser- un Abwasserinfrastruktur,' *Kompetenzzentrum Wasser Berlin*, 2022. https://www.kompetenz-wasser.de/media/pages/forschung/projekte/cybersecurity/b30308e077-1702890607/cybersicherheit-im-wassersektor.pdf.

Cardeña, Xavier, and Thomas Vasen. 'Whitepaper - NIS 2 and cybersecurity for OT operations in water industry: Unboxing the NIS 2 directive: Elevating cybersecurity to a top priority for water & wastewater companies,' *HMS Networks*, July 2024. https://media.hms-networks.com/image/upload/v1708430018/Documents/Whitepapers/NIS2_and_Cybersecurity_for_OT_Operations_in_Water_Industry_EN.pdf.

Chawaga, Peter. 'Public revelation of Bay Area utility hack latest in growing trend for drinking water systems,' *Wateronline.com*, July 1, 2021. https://www.wateronline.com/doc/public-revelation-of-bay-area-utility-hack-latest-in-growing-trend-for-drinking-water-systems-0001

Council of the European Union. 'Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its member states,' Official Journal of the European Union, May 17, 2019. Decision - 2019/797 - EN - EUR-Lex.

——— . ‘Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation,’ May 3, 2024. https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/.

——— . ‘Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,’ Official Journal of the European Union, December 8, 2008. https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng.

Cybersecurity and Infrastructure Security Agency. ‘Ongoing cyber threats to U.S. water and wastewater systems,’ October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

——— . ‘IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities,’ December 18, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

——— . ‘State and Local Cybersecurity Grant Program,’ September 16, 2022, https://www.cisa.gov/cybergrants/slcgp?

Cyber Readiness Institute. ‘Resiliency for Water Utilities Pilot Interim Report,’ December 4, 2024, https://cyberreadinessinstitute.org/news-and-events/resiliency-for-water-utilities-pilot-interim-report/

Danish Environmental Protection Agency. ‘Waste water,’ Ministry of Environment and Gender Equality. Accessed on April 9, 2025. https://eng.mst.dk/water/waste-water.

De Clercq, Geert. ‘Paris’ return to public water supplies makes waves beyond France,’ *Reuters*, July 8, 2014, https://www.reuters.com/article/markets/pariss-return-to-public-water-supplies-makes-waves-beyond-france-idUSL6N0PE572/.

Dekker, Marnix, Jurgita Skritaite, Eleni Philippou, and Rossen Naydenov. ‘ENISA NIS360 2024,’ ENISA, February 2025. https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf

Dunn Cavelty, Myriam and Max Smeets. ‘Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority’, *Journal of European Cyber Policy*, Vol 3, Issue 7, February 2, 2023. https://www.tandfonline.com/doi/full/10.1080/13501763.2023.2173274.

EauFrance. ‘Observatory of public water and sanitations services in France: Overview of the services and of their performances,’ OFB, June 2022, https://economie.eaufrance.fr/sites/default/files/2023-02/synthese_eaufrance_sispea_2020_anglais_vf.pdf.

European Union Agency for Cybersecurity. ‘Cyber Europe tests the EU cyber preparedness in the energy sector,’ June 20, 2024. https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector.

——— .‘NIS Investments 2024,’ November, 2024. https://www.enisa.europa.eu/publications/nis-investments-2024.

EurEau. ‘The governance of water services in Europe,’ September 29, 2020. https://www.eureau.org/resources/publications/150-report-on-the-governance-of-water-services-in-europe/file.

European Commission. ‘Critical infrastructure resilience at EU-level,’ Migration and Home Affairs, September 23, 2024.
https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

——— . ‘European action plan on the cybersecurity of hospitals and healthcare providers,’ January 15, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_262.

——— .'NIS2 Directive: New rules on cybersecurity of network and information systems,' Digital Strategy, December 14, 2022. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

——— .'The EU Cybersecurity Act,' Digital Strategy, June 27, 2019. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

——— .'The European Green Deal: Striving to be the first climate-neutral continent,' Accessed on April 4, 2025. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.

——— .'The European programme for critical infrastructure protection,' December 12, 2006. https://ec.europa.eu/commission/presscorner/detail/en/memo_06_477.

——— .'The EU Solidarity Act,' Digital Strategy, April 14, 2023. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

——— .'Water Framework Directive,' Environment. Accessed March 13, 2025. https://environment.ec.europa.eu/topics/water/water-framework-directive_en.

——— .'Zero pollution action plan,' Environment. Accessed April 4, 2025., https://environment.ec.europa.eu/strategy/zero-pollution-action-plan_en.

European Cyber Security Organisation. 'The EU Cybersecurity Act enters into force,' June 27, 2019. https://ecs-org.eu/the-eu-cybersecurity-act-enters-into-force.

European Energy Information Sharing & Analysis Center. 'Network of trust,' Accessed on April 9, 2025. https://www.ee-isac.eu/.

European Environment Agency. 'Urban waste water directive treatment plants data viewer,' Accessed March 13, 2025. https://www.eea.europa.eu/en/analysis/maps-and-charts/urban-waste-water-directive-treatment-data-viewer-urban-wastewater-treatment-directive-1.

European Insurance and Occupational Pensions Authority. 'Digital Operational Resilience Act (DORA),' January 17, 2025. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

European Parliament. 'European critical infrastructure: Revision of Directive 2008/114/EC,' European Parliament, February 3, 2021. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)662604.

European Parliament and the Council of the European Union. 'Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption,' Official Journal of the European Union, December 16, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020L2184.

——— .'Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for Community action in the field of water policy', EUR-Lex, October 23, 2000. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0060-20141120.

——— .'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending regulations.' Official Journal of the European Union, October 23, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847.

First. 'Health-ISAC,' First.org. Accessed on April 9, 2025. https://www.first.org/members/teams/health-isac.

French Cyber Security Agency. 'Le Dispositif SAIV,' August 18, 2022. https://cyber.gouv.fr/le-dispositif-saiv.

Galiette, Anthony and Doel Santos. 'Medusa Ransomware Turning Your Files into Stone,' Palo Alto Networks, January 11, 2024. https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/.

Gatlan, Sergiu. 'Ransomware attack forces 100 Romanian hospitals to go offline,' *BleepingComputer*, February 12, 2024. https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-100-romanian-hospitals-to-go-offline/.

Geronikolou, Maria. 'Darktrace Investigation Into Medusa Ransomware,' *Darktrace* (blog), June 10, 2024. https://www.darktrace.com/blog/medusa-ransomware-looking-cyber-threats-in-the-eye-with-darktrace.

GE Vernova. 'Smallworld GNM: A complete, accurate network model,' Accessed on April 11, 2025. https://www.gevernova.com/software/products/geospatial-network-management-smallworld-gis.

Government of the Netherlands, 'EU imposes first ever sanctions on leading cybercriminals,' June 24, 2024, https://www.government.nl/latest/news/2024/06/24/eu-sanctions-leading-cybercriminals

Greenberg, Andy. *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York, NY: Random House USA Inc, 2019.

Greig, Jonathan. 'Italian water supplier serving 500,000 people hit with ransomware attack,' *Record*, May 3, 2023. https://therecord.media/italian-water-supplier-ransomware-attack-disruptions-medusa.

——— .'LockBit gang takes credit for attack on water utility in Portugal,' *Record*, February 21, 2023. https://therecord.media/porto-portugal-water-utility-cyberattack-lockbit.

Grossman, Taylor, Monica Kaminska, James Shires, and Max Smeets, 'The Cyber Dimensions of the Russia-Ukraine War,' European Cyber Conflict Research Initiative, April 2023. https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf.

Groves, Kevin. 'Fighting the rising tide: Cyber crime and the water supply,' *Thomas Murray Cyber Series*, March 12, 2024. https://thomasmurray.com/cyber-series/fighting-rising-tide-cyber-crime-and-water-supply.

Holmes, Richard. 'Russian hacking software used to steal hundreds of MoD log-ins,' *i Paper*, November 29, 2024. //inews.co.uk/news/russian-hacking-software-steal-mod-log-ins-3406382.

Hudson Cybertec. 'Drinking water sector impressed with joint seminar Vewin and Water-ISAC,' Accessed April 9, 2025. https://www.hudsoncybertec.com/en/2015/11/04/drinking-water-sector-impressed-with-joint-seminar-vewin-and-water-isac/.

ISO. 'ISO/IEC 27019:2024: Information security, cybersecurity and privacy protection — Information security controls for the energy utility industry,' *ISO*, October, 2024. https://www.iso.org/standard/85056.html.

ISS Source. 'Ransomware Attack at Italian Water Supplier,' May 22, 2023. https://www.isssource.com/ransomware-attack-at-italian-water-supplier/.

JMARK Systems. 'What's the difference between water and wastewater treatment?' *JMARK Systems* (blog). Accessed March 12, 2025. https://www.jmarksystems.com/blog/whats-the-difference-between-water-and-wastewater-treatment.

Jones, Connor. 'UK water giant admits attackers broke into system as gang holds it to ransom,' *Register*, January 23, 2024. https://www.theregister.com/2024/01/23/southern_water_confirms_cyberattack.

Lonergan, Erica, and Michael Poznansky. 'A tale of two typhoons: Properly diagnosing Chinese cyber threats,' *War on the Rocks*, February 25, 2025. https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/.

Markapolou, Dimitra, and Vagelis Papakonstantinou. 'Digitalisation of water services and the water sector cyber threat landscape: Is the EU regulatory framework adequate?' *Journal of Water Law*, Vol. 27, Issue 4, November 1, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968932.

Marquardt, Uwe, Ludger Terhart and Peter Thanisch. 'Nutzung des branchenspezifischen Sicherheitsstandards Wasser/Abwasser (B3S WA) in Verbundunternehmen,' Bundesamt für Sicherheit in der Informationstechnik, November 30, 2018. https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Sektorspezifische-Infos-fuer-KRITIS-Betreiber/Wasser/B3S-WA-in-Verbundunternehmen/b3s-wa-in-verbundunternehmen_node.html.

Martin, Alexander. 'Ransomware group may have stolen customer bank details from British water company,' *Record*, December 1, 2022. https://therecord.media/ransomware-group-may-have-stolen-customer-bank-details-from-british-water-company

Maziotis, Alexandros, Ramon Sala-Garrido, Manuel Mocholi-Arce, and Maria Molinos-Senante. 'A comprehensive assessment of energy efficiency of wastewater treatment plants: An efficiency analysis tree approach,' *Science of the Total Environment*, Vol. 885, August 10, 2023. https://www.sciencedirect.com/science/article/pii/S0048969723021587?via%3Dihub.

Meeschaert, Pascale. 'Cybersécurité : un enjeu élevé, des difficultés réelles mais des opérateurs qui ont décidé d'investir,' *La revue l'Eau, l'Industrie, les Nuisances*, February 28, 2021. https://www.revue-ein.com/article/cybersecurite-reduire-les-vulnerabilites-des-systemes-m2m.

Ministry of Ecological Transition, Biodiversity, Forests, the Sea and Fisheries. 'Gestion de l'eau,' Ecologie. Accessed on April 16, 2025, https://www.ecologie.gouv.fr/politiques-publiques/gestion-leau-france.

Moll Sørensen, Eva. 'The Danish water sector reform - economic efficiency and central-local relations,' *AKF*, July 2010. https://www.vive.dk/media/pure/9892/2078549.

National Health Service England-London. 'Weekly Data,' September 2024. https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/weekly-data/.

Netherlands Enterprise Agency. 'Cybersecurity obligations for more companies in critical sectors,' March 25, 2025. https://business.gov.nl/amendment/nis2-directive-protects-network-information-systems/.

Netherlands Ministry of Infrastructure and Water Management. 'Beleidsnota Drinkwater (2021-2026),' April 2021. https://open.overheid.nl/documenten/ronl-ae2317be-417a-409f-bd2d-59ec08a55620/pdf.

NIS2Directive. 'Essential Entity: Water Supply Sector,' March 2023. https://nis2directive.eu/water/#:~:text=The%20NIS2%20directive%20places%20significant,remain%20resilient%20to%20cyber%20threats.

OpenKRITIS. 'Wasser und Abwasser,' Accessed on April 9, 2025, https://www.openkritis.de/it-sicherheitsgesetz/sektor_wasser.html.

Palo Alto Networks. 'What is IT/OT Convergence?' Accessed March 12, 2025. https://www.paloaltonetworks.co.uk/cyberpedia/what-is-it-ot-convergence.

Pawlak, Patryk, and Erica Moret. 'The EU Cyber Diplomacy Toolbox – Towards a cyber sanctions regime?,' *European Union Institute for Security Studies*, July 21, 2017. https://op.europa.eu/en/publication-detail/-/publication/88cfb104-701b-11e7-b2f2-01aa75ed71a1/language-en.

RAIL-Information Sharing & Analysis Center. 'Rail ISAC,' Accessed on April 9, 2025. https://rail-isac.eu/.

Ribeiro, Anna. 'Oldsmar water treatment plant incident allegedly caused by human error, not remote access cybersecurity breach,' *Industrial Cyber*, April 4, 2023. https://industrialcyber.co/utilities-energy-power-water-waste/oldsmar-water-treatment-plant-incident-allegedly-caused-by-human-error-not-remote-access-cybersecurity-breach/.

Secretary General of Defense and National Security. 'Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R.

1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense,' *LegiFrance*, June 17, 2016. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032749580.

Serrano, Marcello M. 'Increase cybersecurity resilience using advanced data-science techniques for operators training,' *Smart Water Magazine*, November 8, 2024. https://smartwatermagazine.com/blogs/marcello-michael-serrao/increase-cyber-security-resilience-using-advanced-data-science.

Shires, James, Max Smeets, and Hannah-Sophie Weber. 'Predatory Sparrow: Cyber sabotage with a conscience?', *Binding Hook*, December 9, 2024. https://bindinghook.com/articles-binding-edge/predatory-sparrow-cyber-sabotage-with-a-conscience/.

Smart Water Magazine. 'Southern Water Reports £4.5M Cost from Ransomware Attack,' February 28, 2025. https://smartwatermagazine.com/news/smart-water-magazine/southern-water-reports-ps45m-cost-ransomware-attack.

Smeets, Max. *Ransom War: How Cyber Crime became a threat to national security*, 1st Ed. London, UK: Hurst & Company, 2025.

Smith, Paul. 'Understanding the South Staffordshire Water cyber attack,' *SCADAfence* (blog), August 23, 2022. https://blog.scadafence.com/south-staffs-water-attack.

Soesanto, Stefan. 'After a year of silence, are EU cyber sanctions dead?,' Lawfare (blog), October 26, 2021. https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead.

Soesanto, Stefan. 'Inside the fourth EU cyber sanction package,' Lawfare (blog), March 25, 2025. https://www.lawfaremedia.org/article/inside-the-fourth-eu-cyber-sanctions-package.

State of Green. 'The structure of the Danish wastewater sector,' Accessed on April 9 2025. https://stateofgreen.com/en/news/the-structure-of-the-danish-wastewater-sector.

STOP-IT. 'STOP-IT has come to an end, a European water-ISAC is born?' Accessed on April 4, 2025. https://stop-it-project.eu/stop-it-has-come-to-an-end-a-european-water-isac-is-born.

——— . 'The STOP-IT Platform,' accessed on April 4, 2025. https://stop-it-project.eu/results/stop-it-platform/.

UK Home Office. 'Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting,' March 26, 2025, https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible#

Water ISAC. '2022 Dragos ICS/OT cybersecurity year in review - insights on new activity groups, industrial ransomware and ICS/OT vulnerabilities,' February 16, 2023, accessed on April 10, 2025. https://www.waterisac.org/portal/2022-dragos-icsot-cybersecurity-year-review-%E2%80%93-insights-new-activity-groups-industrial.

——— . 'Cybersecurity fundamentals for water and wastewater utilities,' December 19, 2025, accessed on April 9, 2025. https://www.waterisac.org/fundamentals.

Wiewórowski, Wojciech Rafał. 'European data protection supervisor,' *Official Journal of the European Union*, November 29, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XX1129(01).

Work, JD, and Richard Harknett 'Troubled vision: Understanding recent Israeli-Iranian offensive cyber exchanges,' Atlantic Council, July 22, 2020. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/#:~:text=Additional%2C%20as%20yet%20technically%20unattributed,Quds%20Electronic%20Army%20launches

Young, Mark, and David Brazil 'European Commission Publishes Action Plan on Cybersecurity of Hospitals and Heathcare Providers,' Covington, January 22, 2025. https://www.insideeulifesciences.com/2025/01/22/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/

Timeline Sources

March 2019 (Kansas-based WWS facility):

Cimpanu, Catalin. 'US Govt Reveals Three More Ransomware Attacks on Water Treatment Plants This Year.' *Record*, October 14, 2021. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency. 'AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems.' Last revised October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

April 2020 (Israeli water facilities):

'Mekorot Continues Efforts to Secure Its Critical Infrastructure Against Cyber Attacks.' Global Water Intelligence. https://www.globalwaterintel.com/articles/mekorot-continues-efforts-to-secure-its-critical-infrastructure-against-cyber-attacks-mekorot.

Sharon, Jeremy. 'Iran Cyberattack on Israel's Water Supply Could Have Sickened Hundreds – Report.' *Times of Israel*, June 1, 2020. https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/.

Warrick, Joby, and Ellen Nakashima. 'Foreign Intelligence Officials Say Attempted Cyberattack on Israeli Water Utilities Linked to Iran.' *Washington Post*, May 8, 2020. https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html.

September 2020 (New Jersey-based WWS):

Cimpanu, Catalin. 'US Govt Reveals Three More Ransomware Attacks on Water Treatment Plants This Year.' *Record*, October 14, 2021. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency. 'AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems.' Last revised October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

January 2021 (Bay Area Utility Hack):

Chawaga, Peter. 'Public Revelation of Bay Area Utility Hack Latest in Growing Trend for Drinking Water Systems.' *Water Online*, July 1, 2021. https://www.wateronline.com/doc/public-revelation-of-bay-area-utility-hack-latest-in-growing-trend-for-drinking-water-system.

February 2021 (Oldsmar Water Treatment Plant):

Ribeiro, Anna. 'Oldsmar Water Treatment Plant Incident Allegedly Caused by Human Error, Not Remote Access Cybersecurity Breach.' *Industrial Cyber*, April 4, 2023. https://industrialcyber.co/utilities-energy-power-water-waste/oldsmar-water-treatment-plant-incident-allegedly-caused-by-human-error-not-remote-access-cybersecurity-breach/.

March 2021 (Nevada-based WWS facility):

Cimpanu, Catalin. 'US Govt Reveals Three More Ransomware Attacks on Water Treatment Plants This Year.' *Record*, October 14, 2021. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency. 'AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems.' Last revised October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

May 2021 (Volue Technology):

Ben Boubaker, Khobeib. 'Twenty Years of Cyberattacks on the World of Water.' *Stormshield*, August 30, 2021. https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/.

'Volue Releases Postmortem Report on Cyberattack.' *Volue*, June 23, 2021. https://www.volue.com/news/volue-releases-postmortem-report-cyberattack.

July 2021 (Maine-based WWS facility):

Cimpanu, Catalin. 'US Govt Reveals Three More Ransomware Attacks on Water Treatment Plants This Year.' *Record*, October 14, 2021. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency. 'Ongoing Cyber Threats to U.S. Water and Wastewater Systems.' Cybersecurity Advisory AA21-287A, October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

August 2021 (California-based WWS facility):

Cimpanu, Catalin. 'US Govt Reveals Three More Ransomware Attacks on Water Treatment Plants This Year.' *Record*, October 14, 2021. https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year.

Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency. 'Ongoing Cyber Threats to U.S. Water and Wastewater Systems.' Cybersecurity Advisory AA21-287A, October 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

Since 2022 (Multiple OT systems in NA and Europe):

Cybersecurity and Infrastructure Security Agency. 'Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity.' May 1, 2024. https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf.

April 2022 (Reitzner AG / Donau Stadtwerke):

'Ransomware-Angriff: Reitzner AG.' *DSGVO-Portal*. https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_reitzner-ag-1094.php.

August 2022 (South Staffordshire Water):

Forescout Research – Vedere Labs. 'Analysis of Clop's Attack on South Staffordshire Water – UK.' August 19, 2022. https://www.forescout.com/blog/analysis-of-clops-attack-on-south-staffordshire-water-uk/.

'South Staffordshire PLC/South Staffs Water/Cambridge Water Data Breach Claim.' Leigh Day. https://www.leighday.co.uk/our-services/group-claims/south-staffordshire-plcsouth-staffs-watercambridge-water-data-breach-claim/.

August 2022 (South Staffordshire Water):

Smith, Paul. 'Understanding the South Staffordshire Water Cyber Attack.' *SCADAfence Blog*, August 23, 2022. https://blog.scadafence.com/south-staffs-water-attack.

February 2023 (Aguas e Energia do Porto):

Greig, Jonathan. 'LockBit Gang Takes Credit for Attack on Water Utility in Portugal.' *Record*, February 21, 2023. https://therecord.media/porto-portugal-water-utility-cyberattack-lockbit.

February 2023 (Municipality of Rodgau):

Stadt Rodgau. 'Informationen zum Cyberangriff auf die Stadtverwaltung Rodgau.' https://www.rodgau.de/index.php?object=tx,2642.5&ModID=7&FID=2642.15957.1.

April 2023 (Alto Calore Servizi SpA):

Greig, Jonathan. 'Italian Water Supplier Serving 500,000 People Hit with Ransomware Attack.' *Record*, May 3, 2023. https://therecord.media/italian-water-supplier-ransomware-attack-disruptions-medusa.

November 2023 (Drum/Binghamstown Water Co-op):

Martin, Alexander. 'Two-Day Water Outage in Remote Irish Region Caused by Pro-Iran Hackers.' *Record*, December 11, 2023. https://therecord.media/water-outage-in-ireland-county-mayo.

November 2023 [Aliquippa Water Plant (PA)]:

Stanish, Erika. 'Municipal Water Authority of Aliquippa Hacked by Iranian-Backed Cyber Group.' *CBS News Pittsburgh*, November 26, 2023. https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/.

November 2023 (Service Public de l'Assainissement Francilien):

SIAAP. 'Bulletin Cyberattaque.' November 18, 2023. https://www.siaap.fr/presse-publications/publications/detail/actualites/bulletin-cyberattaque/.

'Le SIAAP Touché par une Virulente Cyberattaque.' *Le Monde Informatique*, November 20, 2023. https://www.lemondeinformatique.fr/actualites/lire-le-siaap-touche-par-une-virulente-cyberattaque-92175.html.

December 2023 (Aqualectra):

'Akira Ransomware Strikes Again: Compass Group Italia and Aqualectra Utility Hit by Data Breach.' Cyware Social, December 2023. https://social.cyware.com/news/akira-ransomware-strikes-again-compass-group-italia-and-aqualectra-utility-hit-by-data-breach-b883f56f.

'Aqualectra Customer Service Down After Cyberattack.' Ziptone, November 2023. https://www.ziptone.nl/en/nieuws/klantenservice-aqualectra-plat-na-cyberaanval/.

December 2023 (Rsvodokanal):

'Ukrainian Hackers Strike Back: Blackjack Cyberattack Disrupts Russian Water Utility.' *Cyber Express*, December 21, 2023. https://thecyberexpress.com/russian-water-utility-cyberattack/.

December 2023 (Koh Brothers Eco Engineering Ltd.):

'Koh Brothers and Koh Brothers Eco Engineering Hit by Cyberattack.' *ET CIO Southeast Asia*, December 4, 2023. https://ciosea.economictimes.indiatimes.com/news/security/koh-brothers-and-koh-brothers-eco-engineering-hit-by-cyberattack/105712224.

January 2024 (Veolia North America):

Ribeiro, Anna. 'Veolia North America and Southern Water Hit by Ransomware Attacks, Data Breach Concerns Arise.' *Industrial Cyber*, January 25, 2024. https://industrialcyber.co/utilities-energy-power-water-waste/veolia-north-america-and-southern-water-hit-by-ransomware-attacks-data-breach-concerns-arise/.

February 2024 (Southern Water):

'Southern Water Reports £4.5M Cost from Ransomware Attack.' *Smart Water Magazine*, February 28, 2025. https://smartwatermagazine.com/news/smart-water-magazine/southern-water-reports-ps45m-cost-ransomware-attack.

March 18, 2024 (Fanø Vand):

'Dansk Vandværk Ramt af Hackerangreb Mod Administrative Systemer.' *Version2*, accessed April 25, 2025. https://www.version2.dk/artikel/dansk-vandvaerk-ramt-af-hackerangreb-mod-administrative-systemer.

April 2024 (Moscolletor - Moscow sewage network):

Naprys, Ernestas. 'Ukrainian Hackers Left Moscow's Sewage System Without 87,000 Sensors.' *Cybernews*, April 11, 2024. https://cybernews.com/news/ukrainian-hackers-hit-moscows-sewage-system/.

'Ukrainian Hackers Launch Cyberattacks on Moscow Sewage System.' *Kyiv Post,* April 10, 2024. https://www.kyivpost.com/post/30890.Kyiv Post+6

April 2024 (Tipton West Wastewater Treatment Plant):

Ribeiro, Anna. 'Hackers Target Tipton Municipal Utilities Wastewater Treatment Plant, Prompting Federal Investigation.' *Industrial Cyber,* April 23, 2024. https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-tipton-municipal-utilities-wastewater-treatment-plant-prompting-federal-investigation/.

August 2024 (Stanton Water Department):

Brumfield, Cynthia. 'Russian Group's Hack of Texas Water System Underscores Critical OT Cyber Threats.' *CSO Online*, October 21, 2024. https://www.csoonline.com/article/3568804/russian-groups-hack-of-texas-water-system-underscores-critical-ot-cyber-threats.html.

September 2024 [Catalan Waste Agency (ACR)]:

Domínguez, MLuz. 'Un Ciberataque de Ransomware Impacta en la Agencia de Residuos de Cataluña.' *Bit Life Media*, October 1, 2024. https://bitlifemedia.com/2024/10/un-ciberataque-de-ransomware-impacta-en-la-agencia-de-residuos-de-cataluna/.

September 2024 (Arkansas City Water Treatment Facility):

'Arkansas City Water Treatment Facility Returns to Regular Operations.' *City of Arkansas City*, December 18, 2024. https://www.visitarkcity.org/city-manager/page/arkansas-city-water-treatement-facility-treturns-regular-operations.

October 3, 2024 (American Water Works):

Kerner, Sean Michael. 'The American Water Cyberattack: Explaining How It Happened.' *TechTarget*, October 18, 2024. https://www.techtarget.com/whatis/feature/The-American-Water-cyberattack-Explaining-how-it-happened.

January 11, 2025 [Water for People (NGO)]:

'Medusa Ransomware Operation Targets Water for People: $300,000 Ransom Demanded.' *Cyber Guru*, January 18, 2024. https://www.cyberguru.it/en/2024/01/18/cybercrime-ransomware-attack-no-ethics-in-sight/.

virtual routes

For more information, please visit:

www.virtual-routes.org

If you have any further queries, questions, or concerns, feel free to reach out via email at:

contact@virtual-routes.org