

# ECHO Early Warning System for Water Infrastructure Protection

Ilkka Tikanmäki<sup>1,2,1</sup>, Sara Jylhänkangas, Kitty Tapola and Jeni Awa

<sup>1</sup>Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland

<sup>2</sup>Department of Warfare, National Defence University, Helsinki, Finland

[ilkka.tikanmaki@laurea.fi](mailto:ilkka.tikanmaki@laurea.fi)

**Abstract:** Water is a valuable natural resource and essential for human life, so protecting critical water infrastructure is vital. Through directives such as the Network and Information Security Directive (NIS2), the European Union has made it mandatory to ensure that all critical infrastructure is adequately protected. Security measures taken to protect critical infrastructure are often limited to a national scope. The ECHO Early Warning System (E-EWS) is a tool that enables communication and cooperation across national borders. It focuses on a warning system that allows people to know almost immediately what is happening, to react appropriately and to disseminate this information to trusted partners. With geopolitical tensions and cyberattacks on the rise, this work in progress employs a literature review and case analysis to identify similarities between recent cyberattacks on critical water infrastructure and to determine what E-EWS could have done in these instances. The results show that key similarities correlate with current events: political threat actors, slow detection, fear as a weapon, information silos and people as weak links. With the E-EWS, threats are detected almost immediately, allowing mitigation actions to begin much earlier. By sharing information, knowledge grows, connecting and strengthening the overall security of E-EWS users. Attackers do not care about borders, so the cybersecurity of critical water infrastructure is no longer limited to national borders. International cooperation would help reduce the burden caused by some countries' own resource constraints. Based on these results, the E-EWS plays a key role in the future protection of EU critical water infrastructure.

**Keywords:** Cybersecurity, Critical infrastructure, DYNAMO project, E-EWS, Information sharing

---

## 1. Introduction

Water is a critical resource essential to human life. Due to this importance, many countries categorise it as falling under the classification of critical infrastructure (European Commission, 2025; European Parliament, 2022). Critical water infrastructure can range from the supply of safe drinking water to the transportation and handling of wastewater.

In January 2023, the Network and Information Security Directive (NIS2) came into effect in the European Union (European Parliament and Council, 2022). This directive requires critical infrastructure operators to make sure that there are adequate security measures in place and that they can report any security incidents promptly to the proper authorities. As technology progresses, so does the need to incorporate more modern technology into critical infrastructure systems. Ensuring that security is a top consideration when building up critical infrastructure systems is essential (ENISA, 2017).

This paper aims to discover common characteristics from recent cyberattacks against critical water infrastructure and use those characteristics as a basis to determine the part E-EWS could potentially have to play in boosting the security of critical water infrastructure.

Section 2 examines the common recurring characteristics of cyberattacks against critical water infrastructure. Section 3 describes the ECHO Early Warning System, explaining its core functions and potential benefits before, during, and after cyberattacks. Section 4 discusses the limitations of national-only defence approaches and examines the European regulatory framework, specifically the NIS2 Directive and the Cyber Resilience Act. Section 5 concludes with a summary of findings and recommendations for future research.

## 2. Common Characteristics of Cyberattacks

As technology becomes increasingly prevalent in daily life, so too has the occurrence of cyberattacks. Critical infrastructure has now slowly begun to incorporate various types of technology that are providing new openings through which attackers can gain access. The aims of gaining access via cyberattacks can range from extorting money from organisations to completely shutting the infrastructure down, rendering it useless. The attack vectors also vary just as much, ranging from malware to phishing attacks (Riggs et al., 2023). When comparing recent cases of attacks on critical water infrastructure side by side, several common characteristics arose, such as political threat actors, slow detection, using fear as a weapon, information silos, and humans proving to be the weak link (Bendovschi, 2015). All these characteristics reflect what is currently happening in the world. While

---

<sup>1</sup><https://orcid.org/0000-0001-8950-5221>

there aren't many things one can do to combat the reasons why an attacker chooses to perform an attack, there are ways to mitigate the issues that relate to people. The most critical thing that can be done is to provide information and training so that cyberattacks can be known, learned from, and responded to competently (Riggs et al., 2023). These training and information gathering sessions can come in many different forms, such as workshops, webinars, and courses (ENISA, 2025).

### **3. ECHO Early-Warning System**

The focus of the ECHO Early-Warning System (E-EWS) as a tool is to support an organisation's security operations. Security operation centres (SOC) provide a tool that allows for completely independent management of both incidents that occur and relevant cybersecurity data of their own organisation. At the same time, it allows them the capability to collaborate with others through the sharing of that same information. To ensure security, E-EWS works in conjunction with the Data Anonymisation Tool (DAT) for anonymisation and the Fine-Grained Access tool for encryption and decryption of cyber tickets.

Through E-EWS, an organisation can also have subscriptions to receive notifications on any type of information that they are interested in. An example of this would be that maybe an organisation is interested in getting a notification about the creation of a warning related to water plants. They would immediately receive a notification if this occurred within the E-EWS database (Almén et al., 2022; DYNAMO project, 2024).

E-EWS has the potential to be a benefit during all phases of an attack: before, during, and after. Before an attack occurs, E-EWS can provide organisations with knowledge of known threats and attacks. This knowledge would allow them to protect themselves better by implementing proactive measures to prevent attacks and to learn about what they could potentially be up against. Effective threat information sharing provides organisations with a deeper understanding of the threat landscape. This understanding enables the identification of affected platforms and the implementation of protective measures promptly.

During an attack, real-time sharing and collaboration via E-EWS allow organisations to manage dealing with the situation. They would easily find information relevant to mitigating any currently occurring incident. Having this kind of easy access to information and communication abilities allows organisations to feel more at ease, even when they are under attack. This helps reduce fear and human shortcomings, such as a lack of knowledge. It would also increase the speed with which incidents are noticed and dealt with. Information sharing facilitates responses against hybrid threats (Cybersecurity and Infrastructure Security Agency CISA, 2025), which seems to be what is lacking in many incidents, where detection times often range from hours to months.

After an attack, E-EWS allows sharing information about incidents. This would allow organisations to keep information for their own future use and ensure that others can learn and profit from their experiences. The system increases the degree of protection by reducing viable attack vectors across the entire network of participating organisations. When one organisation shares what happened, other organisations in the network can adapt and become more secure against similar attacks.

### **4. National-Only Defence**

The EU has created policies against cyber threats, such as the NIS2 Directive and the Cyber Resilience Act (European Commission. Joint Research Centre, 2024; European Parliament and Council, 2022). Policies alone cannot guarantee compliance or implementation. In recent years, there has been a rise in cybersecurity attacks across Europe, and when attackers decide to attack, they ignore borders. Being unable to communicate safely and effectively with a neighbouring country that is under attack could have devastating consequences. A unified EU has more capabilities to provide the right amount of help where it matters. Sharing information across the union will provide better defence against cyberattacks than a policy could accomplish by itself.

### **5. Conclusions**

The increase in cyberattacks will remain. Even though attackers are becoming more creative and adapting with the times, there are common characteristics that many cyberattacks often share. Some of these things, such as the motive behind an attack, are things that cannot be controlled or mitigated. Other things, such as slow detection, fear, information silos, and human weakness, are things that can be controlled. The implementation of an early warning system, such as E-EWS, is a benefit to the cybersecurity of critical water infrastructure. As attackers themselves are not held back by borders, neither should the cybersecurity of critical water infrastructure be held back by them. All the characteristics that can be mitigated relate to people and something that they are lacking, whether it be information, education, or time. E-EWS provides ways to help solve those

issues. When we investigate Finland's current situation, we can see that it is a good representation of the inherent flaws of a national-only-based defence system, but we are also able to see the positives, namely, that Finland understands the need for international cooperation and communication going into the future. Further research is necessary to determine the practicality of implementing E-EWS as part of the cybersecurity of critical water infrastructure. It would be necessary to research the best approach for each country and organisation's needs. Small-scale simulations might also look into the viability of E-EWS on a national and international scale.

## Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 101069601. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

**Ethics Declaration:** No human participants or personally identifiable information were involved. All data sources were publicly available.

**AI Tools Declaration:** Keenious was used for literature exploration, and ChatGPT 5.1 for drafting and refinement. Human authors verified all content.

## References

- Almén, C., Hagström, N., & Rajamäki, J. (2022). ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector. *Information & Security: An International Journal*, 53(1), 11–20. <https://doi.org/10.11610/isij.5301>
- Beek, K. (2025). *Russian Hacktivists Take Aim at Polish Power Plant, Again*. Dark Reading. <https://www.darkreading.com/cyberattacks-data-breaches/russian-hacktivists-polish-power-plant-attack>
- Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24–31. [https://doi.org/10.1016/S2212-5671\(15\)01077-1](https://doi.org/10.1016/S2212-5671(15)01077-1)
- Cybersecurity and Infrastructure Security Agency CISA. (2025). *Information Sharing*. Cyber Threats and Advisories. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing>
- Doyle, A. (2025a, February 27). *£4.5 Million Ransomware Bill for Southern Water After Black Basta Attack* [Security Spotlight]. <https://dailysecurityreview.com/security-spotlight/black-basta-ransomware-costs-southern-water-4-5-million/>
- Doyle, A. (2025b, August 22). *Norway Attributes Dam Cyberattack to Russian Hackers—Cybersecurity* [Cybersecurity]. <https://dailysecurityreview.com/cyber-security/norway-attributes-dam-cyberattack-to-russian-hackers/>
- DYNAMO project. (2024). *D4.1 – Initial prototypes of the cyber-threat intelligence gathering, extraction, sharing components and AI-based solutions*. [ <https://horizon-dynamo.eu/wp-content/uploads/2025/02/DYNAMO-RPT-D41-V2-0.pdf> ]
- ENISA. (2017). *Communication network dependencies for ICS/SCADA Systems*. European Union Agency for Network and Information Security (ENISA). <https://www.enisa.europa.eu/sites/default/files/publications/WP2016%203-1%202%20ICS%20SCADA%20Dependencies.pdf>
- ENISA. (2025). *NIS2 Technical Implementation Guidance*. European Union Agency for Cybersecurity (ENISA). <https://doi.org/10.2824/2702548>
- European Commission. (2025). *Critical infrastructure resilience at EU-level—Migration and Home Affairs* [Policy]. Critical Infrastructure Resilience at EU-Level. [https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en)
- European Commission. Joint Research Centre. (2024). *Cyber resilience act requirements standards mapping: Joint Research Centre & ENISA joint analysis*. (Analysis No. EUR 31892; p. 69). Publications Office of the European Union. <https://data.europa.eu/doi/10.2760/905934>
- European Parliament. (2022). *The resilience of critical entities*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557>
- European Parliament and Council. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227>
- Holm Security. (n.d.). *NIS & NIS2 in Norway* [Resources]. NIS2 & the EEA. Retrieved January 9, 2026, from <https://www.holmsecurty.com/nis2-in-norway>
- Khomenko, I. (2025, August 19). *Russian Hackers Breach Polish Hydropower Plant in Major Cyberattack*. UNITED24 Media. <https://united24media.com/latest-news/russian-hackers-breach-polish-hydropower-plant-in-major-cyberattack-10882>
- Pukėnaitė, I. (2025, August 19). *Russian hackers take control of Polish hydropower plant, turbines disrupted*. Cybernews. <https://cybernews.com/cybercrime/russian-hackers-target-polish-hydropower-plant-again/>
- Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, 23(8), 4060. <https://doi.org/10.3390/s23084060>