BTO Verkennend Onderzoek

S E P T E D

Emerging cybersecurity and cyber-physical threats in water systems

Summary

Cyber-attacks and cybersecurity incidents have increased in frequency and magnitude in recent years, usually having the form of data breach events, traffic interception or malware, ransomware and phishing attacks. Critical infrastructure systems with exposed digital assets and - as part of them - water supply and distribution networks are not exempted from these rising threats, as a number of recent events have targeted specifically water systems, with diverse but worrying results. One of the indirect consequences of the global corona crisis is accelerated digitization, which could make water organizations more vulnerable to these threats. This trend alert explores the issue of cybersecurity in water, by looking at past cases and reflecting on the expected future impact of these events, as water systems get more digital and, eventually, more exposed to digital risks.

Consequences for you

	Low	Middle	High	Reason
Impact				Potential to completely halt operations e.g. of a water treatment plant, and damage reputations.
Certainty				The risk is high, while the predictability is low.

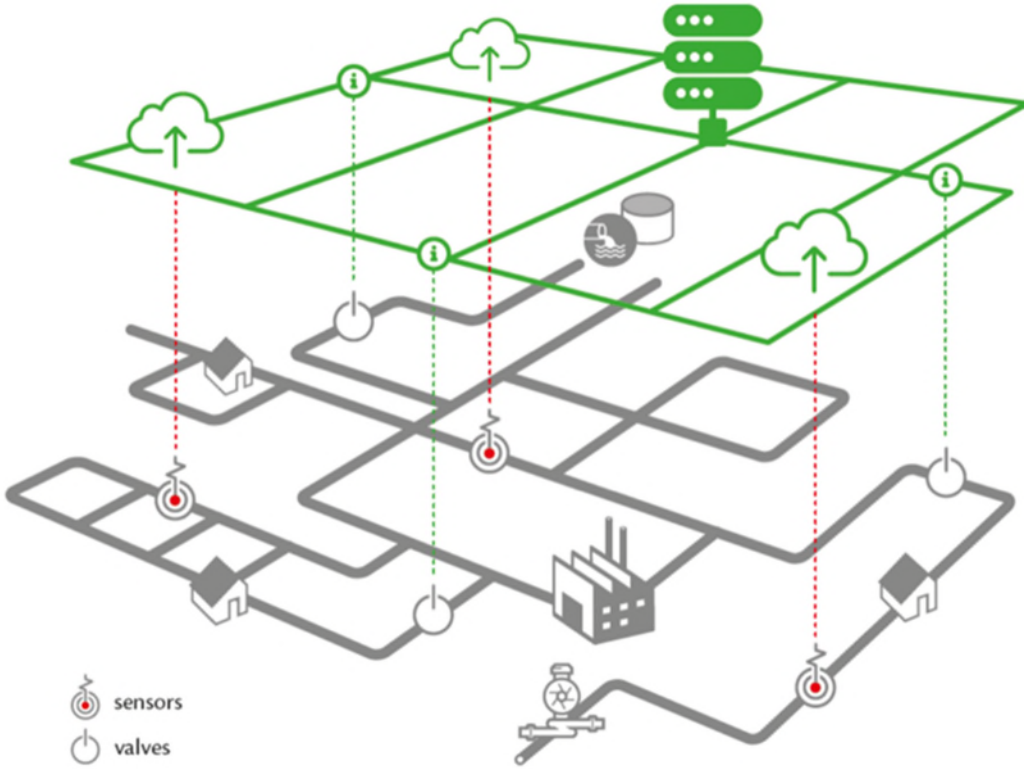

Image from the WaterShare STOP-IT pitch at IWA Tokyo (2018).

S = sociaal E = economisch P = politiek T = technologisch E = ecologisch D = demografisch

S E P T E D

Trend and background

The world is becoming increasingly digital. Laptops, smartphones and a growing network of sensor-embedded devices that constitute the Internet of things (IoT) ensure that a large part of modern life remains constantly connected online and exchanging information in real time. This digital revolution is fueled by parallel technological advances in computing, embedded systems, smart sensors and wireless communication protocols. Moreover, the digital transformation is likely to intensify in the coming years due to the introduction of faster communications (such as the deployment of 5G networks), continuing advances in processing power and also due to the growing application of Artificial Intelligence (AI) techniques to handle, process and extract meaning from (big) data.

The unexpected covid-19 situation has further accelerated this trend, as people actively avoid physical communication and shift to digital means. Common tasks, such as having meetings, doing payments or interacting with public services are now routinely done online. In light of the persistent covid-19 ebbs and flows across countries, companies and governments adopt online workflows and (hastily) go digital, thus exposing an increasing part of their core business to the digital realm.

However, this ubiquitous digitization doesn't come without cons. Such increased exposure to the digital world means that more and more aspects of our personal and professional lives are exposed to different forms of cyber-attacks, which aim to gain unauthorized access to privileged information or disturb online services for malicious purposes. These attacks have evolved alongside cyber systems and range from the use of specialized software that is able to spy or steal data, to generating heavy communication traffic in order to disrupt online services. In the era of cloud computing, when a growing number of services is provided through servers, these attacks have evolved to include sophisticated data breaches that affect thousands of users of online services and expose the digital security of large companies. An overview of common cyber-attacks, along with a short description, is provided in Table 1.

The afore-mentioned cyber-attacks occur with an increasingly alarming rate at different levels and target a range of end users, from individual persons to large companies. Individual users are prone to malware and ransomware attacks in their systems, but are also the prime targets of phishing attacks, where the attacker disguises as a legitimate financial service and fakes a data request. Phishing attacks that target individuals have grown significantly in recent months during the corona crisis, with multiple Dutch cases that got tricked with this form of fraud (WNL 2021).

Table 1: Common types of cyber-attacks.

Cyber attack	Description
Malware	Unwanted piece of software used to spy, steal information or obstruct normal functions.
Ransomware	A variant of malware that encrypts data and prevents their access until a "ransom" is paid to third parties, usually via digital currency such as bitcoin.
Data breach	A security violation where protected data is copied and stolen by an unauthorized third party. Data breaches may involve financial information or data stored in large servers, such as cloud companies.
Phishing	Phishing attacks rely on malicious e-mails that disguise as legitimate requests, convincing end users to give away sensitive information.
Distributed Denial of Service (DDoS) attack	An attack targeting online servers, overloading them with false user traffic that leads to the server slowing or shutting down.
SQL injection	This attack manipulates database queries (SQL code requests) to gain access to sensitive information in a server or database.
Man in the Middle (MitM) attack	An attack that occurs when a third-party manipulates the communication between two parties who believe they are directly communicating with each other.
Eavesdropping	A MitM type of attack involving the theft of information that is transmitted over unprotected wi-fi networks.

S E P T E D

At a global scale, international institutes report an all-time high of malware and ransomware attacks for 2020, with malware incidents showing an increase by 358% and ransomware attacks targeting one victim every 10 seconds (Forbes 2021).

Besides individual users, companies are prone to data breach attacks or disturbance in their digital assets (such as their servers) through, for instance, DDoS attacks. Large cloud service providers, including Yahoo, Apple, LinkedIn, DropBox and Microsoft, have experienced breaches in the recent past (StorageCraft 2020). Local systems can be also unsafe; a very recent case (February 2021) involved a sophisticated ransomware attack on European game developer CD Projekt Red, where the source code for multiple popular company products was leaked and auctioned off on a dark Web forum, seemingly for millions of dollars in bitcoin, with the intention of selling it to competition (The Verge 2021).

Governments and public services are also not immune to these forms of attacks to their digital assets. Cyber attacks have been used in the past as part of unconventional warfare (noted by some authors as cyberwarfare), with the most infamous case being the Stuxnet incident, a highly complex piece of malware targeting industrial assets (Langner 2011). Digital espionage can also reach national levels; a recent case in the US saw a simultaneous data breach of several US government bodies by Russian hackers, which was initiated by first breaking into the systems of SolarWinds, a company that makes corporate network management software used by most Fortune 500 companies and multiple governments (MIT Technology Review 2020). The hackers used complex methods that allowed them to proceed with data leaks for months without being detected. This threat of nationwide espionage has led to Dutch security services (such as AIVD and MIVD) requesting a bigger budget for cybersecurity, in order to adapt to foreign hacker attacks that occur on a daily frequency (NOS 2021).

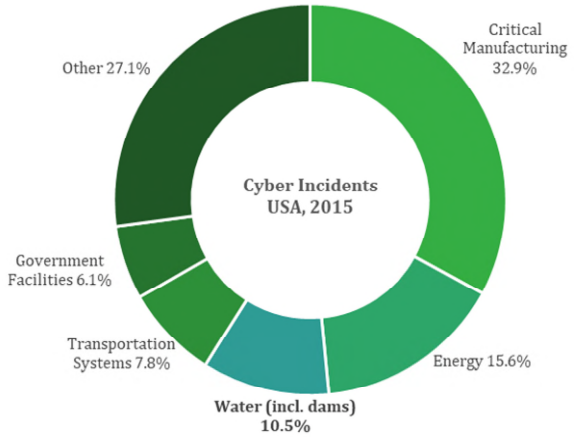

Figure 1: Distribution of 295 cyber-attack cases in the US (adapted from Nikolopoulos et al., 2020).

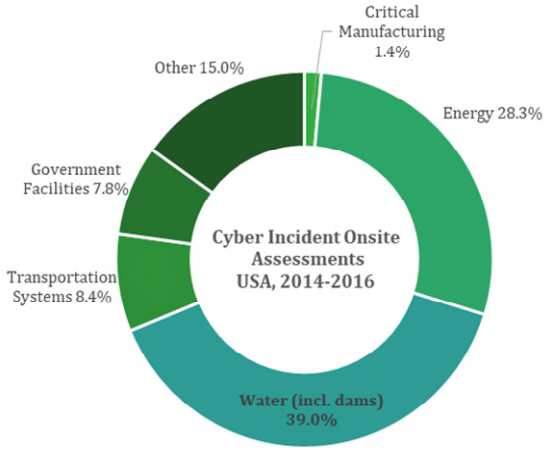

Figure 2: Distribution of cyber incidents requiring onsite response and assessment by cybersecurity services in the US (adapted from ICS-CERT 2016).

Water systems: digital threats, physical consequences

The water sector is not an exemption to digital risks. Being part of Critical Infrastructure (CI), along with energy and transportation systems, water systems (i.e. water supply and distribution networks, along with wastewater treatment plants – WWTPs) have been targets for cyber-attacks in recent years. Data from past cases reveal that the water sector is one of the most targeted critical infrastructure types, along with the manufacturing and energy sectors (ICS-CERT 2016; Nikolopoulos et al. 2020), with approximately 1/10 of the US cyber-attack incidents targeting water infrastructure (Figure 1). Moreover, such

S E P T E D

attacks are not trivial and require proper onsite response by cybersecurity services, as the water sector has been, despite the lower amount of incidents, the largest critical infrastructure sector in onsite assessments by the American cyber emergency response teams (ICS-CERT), as seen in Figure 2.

An interesting characteristic of cyber-attacks in critical infrastructure is that, while the target is usually a digital asset such as a server, SCADA system or connected device (sensor or actuator), the impact of an attack can lead to physical consequences, such as the erratic behavior of a pump that leads to insufficient water being delivered to clients. This is due to the fact that critical infrastructure are essentially integrated systems, where physical processes are monitored, coordinated and controlled by digital computing and communication systems (Lee 2008). This integration of physical with digital assets is also known as a cyber-physical system (CPS). Attacks on such systems can have dire physical consequences, including downtime to an important public service or even repercussions to public health.

These physical consequences have been significant in past cases, such as the Maroochy Water Services incident in Australia (Abrams and Weiss 2008), where a former disgruntled employee gained unauthorized access to the SCADA system, which remotely controlled the sewage pumps, leading to faulty pump configuration that resulted in the release of 1M liters of untreated sewage in the downstream river. Other past events include (Hassanzadeh et al. 2020; Tuptuk et al. 2021):

- a security breach at a water treatment facility in Pennsylvania, US (2006), where hackers installed malicious software on the plant's SCADA system.
- an attack in the diversion system of canals in Tehama-Colusa, US (2007) which was alleviated by a manual override in the canal operations.
- an incident in the Bowman Avenue Dam, US (2013) where hackers gained unauthorized access to a remotely-controllable sluice gate.
- a series of attacks in the smart meters of five different US water utilities (2014), leading to disruptions in their distribution systems.
- an incident in an undisclosed European water utility (2018), where a cloud-based infrastructure security firm, hired to monitor the utility network, discovered that the network was infected with malware. This infection led to nearly 40% of the SCADA bandwidth being reserved for illegal cryptomining, causing a significant surge in the system bandwidth consumption.
- a series of attacks in the water supply and treatment facilities in Israel (2019), which led to alerts by the national services (INCD) to raise their security levels.
- a recent security incident in Florida's water supply (2021), where an intruder remotely accessed the SCADA system and managed to increase the amount of sodium hydroxide by a factor of more than 100, which could have led to water contamination dangerous for human life (Tampa Bay Times 2021). The attack was averted by the situational awareness of the system supervisor.

These incidents, paired with considerations about the efficiency of current cybersecurity plans, are of concern to Dutch water actors as well. For instance, the cyber security management scheme of a Dutch utility was recently found to be inadequate and with an increased risk of exposure to incidents with possible consequences for the quality and reliable provision of drinking water (ILT 2021). This assessment prompted immediate action from the side of the utility to evaluate the overall management model and improve ICT services.

S E P T E D

Relevance

Cybersecurity prospects, scenarios and impact

While major cyber-attack incidents have a relatively low probability for water systems, they have – as one observes in existing cases and recent trends - the potential to lead to extensive data loss or the disturbance of critical asset operations, e.g., a water treatment facility or a main pump. These effects may lead to loss of service and severe damage to the otherwise very good reputation of the Dutch water sector. This is further aggravated by specific characteristics, such as:

- the dynamically evolving nature of cyber-attacks, which leads to novel risk vectors. For instance, until recently, ransomware attacks were considered science fiction, but were enabled by the progress in encryption technology. Cryptomining couldn't have been anticipated as well, but was conceived based on both hardware supply-demand needs and the rise of cryptocurrency as means of financial exchange.

- the lack of contingency cybersecurity planning. In business environments, cybersecurity is typically seen as an operational process dealt internally by part of the IT staff and is rarely discussed across groups and in tactical and strategic timelines. This lack of holistic planning means that trends are not monitored and communicated properly, which leads to many cyber-attack scenarios being unanticipated and without any form of reporting or cybersecurity protocols in place. This in turn increases the risk of being unable to even realize that a cyber-attack is happening, let alone manage and protect from it.

- the ad-hoc nature seen in multiple elements of the water critical infrastructure, which includes aging and exposed hardware, as well as intranet systems with specialized, obsolete (and, often, not updated) software. It should come to no surprise that critical infrastructure is particularly exposed to obsolete software security issues, as the software remains installed (even after the end of its service life) in specialized hardware, such as PLCs and SCADA units (Paganini 2014).

The low-predictability, high-risk environment of cyber threats leads to diverse scenarios for the water sector. The following basic hypothetical incidents, derived from past events in combination with recent trends, aim at merely highlighting the diversity cyber-attacks can have in terms of their technology, management, detection ability and impact:

1. Data at stake: the increasing risk of ransomware, paired with the tendency to store water sector data in larger volumes and more frequently, results in an increased likelihood of extensive, 'blind' ransomware attacks. In that scenario, a specific water service or firm might be targeted and have the majority or entirety of its data on a server encrypted by malicious ransomware. This will lead to: (a.) the immediate loss of a large volume of data, which might consequently affect asset operations (e.g., historical data on network operations and maintenance) or lead to legal problems (e.g., the compromise of sensitive client data), (b.) sensitive data being copied and illegally distributed to more hacking groups or the competition (similar to the ransomware case of Projekt Red (2021)).

2. Exposed assets: the ad-hoc nature of water systems makes them potential hacking playgrounds. For instance, cyber-attackers who gain control of critical cyber assets (such as SCADA units) could experiment with a change in PLC controls and lead to assets (such as pumps or valves) operating erroneously. In more sophisticated attacks and as seen in past events (Langner 2011), these alterations could be masked and hidden from the SCADA operators. Depending on the cybersecurity level of the utility and the integration of its systems, such an attack could take a while to notice; if the response mechanisms are not in place and proactive, the risk will not be averted quickly and the (physical) results in the utility service will be severe.

3. Hidden risks: the ever-growing risk and complexity of malware and eavesdropping attacks, paired with continuing progress on

S E P T E D

wireless technologies and the introduction of more connected, smart assets, means that sensitive operational information flows could be intercepted without the operators noticing. For instance, in the case of a wireless network lacking proper encryption, the attackers could obtain the information transmitted by wireless sensors. This could lead to sensitive operational information (about water quality, for instance) being extracted illegally and, potentially, used to identify system vulnerabilities that might be exploited in another attack (such as Scenario (2)). The same is likely for sensitive hardware, such as cameras or smart locks, which might be compromised and used to expose vulnerabilities. As these attacks do not have an immediate impact, they might also take weeks to be noticed and dealt with.

The future of cyber incidents in water

With water systems being part of the accelerating digital transformation, the water sector is expected to grow more susceptible to cyber-attacks in the coming years. Cyber threats are becoming more complex and well-orchestrated (Forbes 2021), addressing not only local (SCADA) systems but also cloud services or (wireless) communication streams between different assets. At the same time, water systems are becoming smarter, as more connected assets (sensors and actuators) become part of the operations while more information is collected and managed in data warehouses and is being used for decision-making. Undoubtedly, smarter networks lead to more efficiency and better decisions, but an often overlooked aspect is they also lead to an extended cyber-attack vector for water systems, which needs proper cybersecurity management strategies (Rasekh et al. 2016). The Dutch water sector, as part of the so-called 'vital infrastructure' of the Netherlands, is already adapting to face this transformation and placing higher importance in cybersecurity (VEWIN 2020). However, the high unpredictability of cyber risks, combined with the inherent complexity and digitization of water infrastructure, means that this problem will remain a high-priority point in the agenda for the coming years.

Given these prospects, the Dutch water sector, which already anticipates the growing risks of cyber (and cyber-physical) attacks in an operational context, needs to remain alert and pioneer methods of addressing and managing cyber risk at higher (tactical and strategic) scales. The key element for this is not only readiness and anticipation by IT teams, but efficient communication across stakeholders. Valuable lessons could be learnt by aligning with utilities abroad, as well as by reflecting on the outcome of relevant EU cybersecurity projects for water, such as STOP-IT. Experience, management plans and trends from other critical infrastructure and (more digital) business sectors are also important to scan emerging threats more efficiently. Moreover, vulnerabilities in current cybersecurity practice need to be pointed out and communicated more clearly, across and beyond IT teams and - perhaps more importantly - across management levels and utilities, in order to ensure that the needs of monitoring, response and mitigation services are covered and that holistic information control and management strategies exist in all workplaces.

More information

Abrams, Marshall, and Joe Weiss. 2008. *Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia*. MITRE CORP MCLEAN VA MCLEAN.

Forbes. 2021. "Alarming Cybersecurity Stats: What You Need To Know For 2021." https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=c1bec2c58d3d.

Hassanzadeh, Amin et al. 2020. "A Review of Cybersecurity Incidents in the Water Sector." *Journal of Environmental Engineering* 146(5): 3120003.

ICS-CERT. 2016. *ICS-CERT Year in Review*. Arlington, VA: Cybersecurity and Infrastructure Security Agency. https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.

ILT. 2021. "ILT Stelt Waternet Onder Verscherpt Toezicht." https://www.ilent.nl/actueel/nieuws/2021/04/02/ilt-stelt-waternet-onder-verscherpt-toezicht.

S E P T E D

Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security and Privacy* 9(3): 49–51.

Lee, Edward A. 2008. "Cyber Physical Systems: Design Challenges." In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, IEEE, 363–69.

MIT Technology Review. 2020. "How Russian Hackers Infiltrated the US Government for Months without Being Spotted." https://www.technologyreview.com/2020/12/15/1014462/how-russian-hackers-infiltrated-the-us-government-for-months-without-being-spotted/.

Nikolopoulos, Dionysios et al. 2020. "Cyber-Physical Stress-Testing Platform for Water Distribution Networks." *Journal of Environmental Engineering* 146(7): 4020061.

NOS. 2021. "Veiligheidsdiensten Willen Meer Geld Vanwege Spionage Uit China En Rusland." https://nos.nl/artikel/2368169-veiligheidsdiensten-willen-meer-geld-vanwege-spionage-uit-china-en-rusland.html.

NU.nl. 2021. "Waternet Onder Verscherpt Toezicht Om Verhoogd Risico Op Digitale Aanvallen." https://www.nu.nl/tech/6125645/waternet-onder-verscherpt-toezicht-om-verhoogd-risico-op-digitale-aanvallen.html.

Paganini. 2014. "Impact of Windows XP End of Life on Critical Infrastructure." *Cyber defense magazine*. https://www.cyberdefensemagazine.com/impact-of-windows-xp-end-of-life-on-critical-infrastructure/.

Rasekh, Amin et al. 2016. "Smart Water Networks and Cyber Security." *Journal of Water Resources Planning and Management* 142(7): 01816004.

StorageCraft. 2020. "7 Most Infamous Cloud Security Breaches." https://blog.storagecraft.com/7-infamous-cloud-security-breaches/.

Tampa Bay Times. 2021. "Someone Tried to Poison Oldsmar's Water Supply during Hack, Sheriff Says." https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.

The Verge. 2021. "Cyberpunk and Witcher Hackers Auction off Stolen Source Code for Millions of Dollars." https://www.theverge.com/2021/2/10/22276664/cyberpunk-witcher-hackers-auction-source-code-ransomware-attack.

Tuptuk, Nilufer, Peter Hazell, Jeremy Watson, and Stephen Hailes. 2021. "A Systematic Review of the State of Cyber-Security in Water Systems." *Water* 13(1): 81.

VEWIN. 2020. "Waterspiegel 4: Cybersecurity, Het Watersysteem En Vewin's Lobby-Agenda."

WNL. 2021. "Stand van Nederland." https://www.uitzendinggemist.net/aflevering/542594/Stand_Van_Nederland.html.

Keywords

cybersecurity, cyber-physical, smart systems