



# STORMSHIELD

OPINION ARTICLE

# WATER INFRASTRUCTURE: WHEN STATES AND CYBER ATTACKS REAR THEIR UGLY HEADS

**Khobeib Ben Boubaker**  
Head of Industrial  
Security Business Line,  
Stormshield

**Attempted cyber attacks targeting dams, irrigation systems or wastewater treatment plants have received little coverage in the media. However, these attacks exist and present an unusual strategic challenge. What's the worldwide situation with cybersecurity for water systems?**

Generally speaking, cyber protection for human beings is a major challenge, ranging from the supply aspect to that of health and water management. Over and above the critical issues inherent to this sector and the vital importance of this resource, the water industry must also deal with the scale of the cyber attacks directed against it. **Just like the industry itself, the cyber attacks targeting the water sector are complex and sophisticated.** They are often orchestrated by state-sponsored bodies whose objective is to destabilise a country's economy. Water companies must therefore simultaneously reconcile important production challenges and critical security requirements. The goal is to effectively protect all critical infrastructure and equipment by adopting a defensive position aimed at limiting the damage which could be caused by large-scale cyber attacks as far as possible.



## WHAT'S THE CURRENT SITUATION WITH CYBERSECURITY FOR WATER SYSTEMS?


The main digital developments in the water infrastructure field are related to the replacement of RTC connections (the communication method formerly used) which have become obsolete, and migration to the ethernet network or 4G and 5G networks which offer improved connectivity. All water industry sites are gradually implementing this migration and are therefore being connected to the outside world, which was not the case previously. In the good old days of RTC, most systems (such as PLCs) were insulated from the Internet. But with the end of this communication method, these systems are now being connected and are consequently facing new cyber threats.

*“The water industries are now having to give thought to securing their systems as they are part of the IoT or even the IIoT landscape, with all of its inherent security issues”*

**Raphaël Granger**, Named Account Manager Stormshield

This paradigm shift presents the water industry with a twofold challenge: converting ageing industrial systems and equipment (Windows XP and others) to better performing - and better connected - technologies **and taking onboard the notion of cyber security as an integral part of their industrial activities.** *“The water industries are now having to give thought to securing their systems as they are part of the IoT or even the IIoT (Industrial Internet of Things) landscape, with all of its inherent security issues”* explains Raphaël Granger, Named Account Manager at Stormshield.

However, the water industry must also face threats inherent to its very nature. Due to the existence of numerous physical sites (water treatment basins, distribution centres and water towers for example), the water industry uses distributed architectures through which messages and orders travel. The challenges of guaranteeing the integrity and privacy of such information flows have now become critical in order to guarantee the quality of a vital resource at the end of the chain, at a time when remote management is becoming commonplace. But these challenges also require genuine cyber-awareness by all participants - like the remote maintenance operators.






## A MULTI-SPEED REGULATORY APPROACH

In France, for several years now sensitive infrastructure assets related to the water industry have been **categorised as operators of vital importance**, as part of the military planning law. As a result, they are monitored closely by the French Network and Information Security Agency (ANSSI). By necessity, this close attention from the state is forcing the water sector to become more aware of the cyber challenges inherent to its activities.

Internationally, most major stakeholders in the water sector in the developed countries are also beginning to incorporate cybersecurity as a prerequisite. *"The cybersecurity levels of water systems do not yet match the threat levels with which the water industry is faced"*, explains **Nebras Alqurashi**, Business and Technical Development Manager (Middle East) at Stormshield. *"But more and more authorities are sounding the alarm and would like to get things moving for the better"*. On the other hand, in the developing countries, cybersecurity is way down the list of priorities for water companies. *"For these countries, the challenges are of a completely different kind: water scarcity, water treatment, efficiency of distribution networks, wastewater disposal, etc. Where water management and water access are concerned, not all countries are on an equal footing"*, stressed **Tarik Zeroual**, Global Account Manager at Stormshield. When you have inequality and scarcity (water is very rare in the Middle East for example) you soon get rivalry and conflicts developing around water and the control of its related industry. These economic and political circumstances help create an environment conducive to cyber attacks, which then become a means used by states to pressurise and destabilise one another.

## GEOPOLITICS, PUBLIC HEALTH AND MORE... THE HIGH STAKES INVOLVED IN THE CYBER ATTACKS CONDUCTED AGAINST WATER INFRASTRUCTURE

You could almost say that the water industry spawns problems when we consider the particularly vulnerable facilities and equipment (run on older operating systems), transition to the IIoT or the geopolitical and strategic challenges related to water resources. It's therefore impossible for critical infrastructure to avoid the unwelcome attention of cyber attackers.



As a result, water-related infrastructure is today in the cyber firing line and the preferred weapon used by attackers appears to be *ransomware*. According to the American company Gray Matter, more than 22 cyber attacks of this kind were recorded in 2019 in the United States alone. A water department in the state of North Carolina was targeted by a cyber attack using ransomware back in 2018, when the state was engaged in crisis management after the devastation caused by hurricane Florence a few weeks earlier. The attackers were suspected of using this crisis situation to try and attack water systems and harm the population. To gain access to the water system, they firstly used the Emotet malware and then, once inside the systems, injected the Ryuk ransomware - known for use in attacks on public structures among others - and encrypted part of the water department's data.

If we go back still further to 2017, cybersecurity researchers at Georgia State University developed a new form of malware capable of poisoning water by changing the chlorine levels used in drinking water production facilities. To simulate this attack, the researchers took control of the facility's PLCs (*Programmable Logic Controllers*). In their report retracing the simulation, the researchers described the operating methods attackers could use to take control of these vulnerable PLCs. These firstly involved a reconnaissance phase to detect Internet-connected PLCs (including by using the Shodan specialised search engine), and to use them as access points. Once inside the system, the attackers could then proceed to propagate throughout the facility's system, collecting key data about the facility such as information for accessing and controlling the PLCs. Finally, the last stage involved increasing the quantity of chlorine added to the water and displaying false readings.

Because this is also one of the objectives of the cyber attacks directed against water infrastructure: advanced strategic attacks, the impact of which may endanger the lives of part of the country's population. And bring about the destabilisation of an entire country. The challenge of protecting public health linked to water is a critical one, which the water companies must take into account as part of their efforts to combat cyber attacks. *"If you can affect a water distribution site you can affect the population, with the risk of significant physical harm. A successful cyber attack against the water industry is an attack which can generate an immediate risk"* warns Tarik Zeroual.

*"A successful cyber attack against the water industry is an attack which can generate an immediate risk"*

**Tarik Zeroual**, Global Account Manager Stormshield

Looking beyond the work carried out by this university, changing the chemical treatment of water could pose a real risk. Last April, Iran attempted to do just this using cyber attackers to affect the quality of the water supplying part of the Israeli population. The attackers firstly took control of American servers to cover their tracks before then moving on to attack the target water distribution systems. The attack ultimately failed, but had it succeeded, the harm to public health would have been considerable, with part of the population probably being poisoned.


Last July, Israel reported two new attacks against its critical water infrastructure. This time, it wasn't the urban water systems being targeted but those used for the agricultural sector. It was therefore a lower level attack, although Iran is suspected of being the originator of these attacks with the aim of destabilising the state of Israel and weakening it politically. For both attempts, the attackers once again used American servers to affect the pump control programs.

Cyber attacks against water infrastructure seem to be generally well-run and executed: they are anticipated, prepared and extremely well-documented. The attackers are familiar with the systems they are targeting. Nothing is left to chance and none of this is the result of opportunism. This leads us to suppose that cyber attacks targeting the water industry seem to be ordered by or for states and that the groups of cyber attackers carrying them out are certainly no amateurs. *"The cyber attackers acting against the water industry are organised groups - generally Russian, Chinese or Iranian APT groups - financed or headed by state bodies"*, explains Tarik Zeroual.

Water therefore offers the possibility to carry out large-scale cyber attacks with a real strategic dimension involved. The water companies consequently need to equip themselves to limit as far as possible the hijacking of their infrastructure for cyber warfare purposes, against a geopolitical background.

## **THE WATER INDUSTRY'S ANSWER: IMPROVED PROTECTION THROUGH SEGMENTATION**

Major problems require major solutions. To counter the cyber attacks targeting it, the water industry needs to filter everything arriving in its facilities from the outside world. To do so, the sector has introduced a segmentation policy on its different sites. This is a vital approach when it comes to protecting water infrastructure, all the more so as it can take varying forms. *"The water companies are segmenting each of their sites and controlling the communication flows transiting through them"*, explains Raphaël Granger. Over and above the segmentation of their operational sites, the water industry is also separating the IT environment (PCs, servers, users) from the OT environment (the operational environment) within them. This segmentation is designed to isolate the operational part in the event of an attack. Finally, within the OT part, it's possible to find another form of segmentation, with a separation between the supervision part and the implementation part (PLCs).



The key stakeholders in the cyber sector, including the software publishers, are supporting the water companies in this move to segmentation and through a certain number of securSantee *cyber security for water systems, the software publishers are helping the companies operating in this sector to check the reliability and compliance of their network protocols. Using industrial firewalls, the idea is to ensure that these protocols are not modified or compromised by a cyber attacker*", adds Raphaël Granger. For this industry, it's therefore very important to have solutions able to verify the legitimacy of the orders performed by the PLCs and to introduce systems making it possible to manage and secure remote access (for remote maintenance or alert management, etc.).

The water industry is organising to fight back against cyber attacks, but this is only just the beginning. In the near future, the industry will need to face a new challenge, that of extending its security policies throughout the whole chain, beyond the water treatment facilities, and adopting a more advanced IIoT approach which involves securing communications and systems from end to end, from the plant through to the consumer.



**STORMSHIELD**

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: [www.stormshield.com](http://www.stormshield.com)