MEDRC

TRANSBOUNDARY WATERS

PRACTIONER BRIEFING SERIES

Issue 5

WATER CYBER SECURITY

Tansboundary Approaches and Challenges

Water Cyber Security

Transboundary Approaches & Challenges

We often think of "cyber" in the sense of cyber-crime, such as identity theft, and as being limited to our personal computers or our credit cards. With the attending responsibility for preventing such crime belonging to individuals or businesses; having your email hacked, banking information stolen, or the theft of corporate intellectual property. The everyday cyber-crime of the corporate world. Beyond this, we think of cyber security as the concern of the banking sector, and the systemic risk of a hack that compromises an entire credit card company or a bank, and how this could affect the wider economy—global payments, trade, and the banking system. This is the responsibility of the company to protect their customer information.

Increasingly, however, more and more systems are becoming interconnected and networked, meaning, connected to the internet. This includes critical national infrastructure (CNI) such as water, electricity, or gas utilities, with cyber risk and cyber security becoming areas of national security with transboundary implications, both between economic trading partners, as well as those sharing natural resource basins. Transboundary electricity grids and the impacts of wastewater across borders becomes even more challenging when they can be sabotaged or used as a weapon. These concerns make transboundary cooperation more difficult, or fractured and incomplete.

The increased convenience, efficiency, and sustainability from making cities smarter, also makes them more vulnerable to new types of threats, which require new responses, additional safeguards, and best practices. Smart Meters and Smart Contracts running on distributed networks like blockchain can greatly reduce the cost of administering public goods like electricity and water, and keep data public and secure, but a more complex supply chain also provides more opportunities for exploitation.

The particular exposure of the critical utilities like electricity, gas, and water; pose unique challenges compared to that of individual corporate IT systems, or across a system like the financial sector. In this briefing we will explore some of the issues related to cyber security and public utilities or infrastructure, and how governments and private companies are responding to these challenges in their sectors.

Practical Summary

Technological advancements have allowed for the development of smarter machines and sensors that can adapt to situations and deploy precious environmental resources more efficiently. Such innovations have led to greater automation in wide variety of systems, from agriculture to water treatment and energy grids. The Internet of Things (IoT) has meant the increasing connection both within and between systems, and whereby new openings are also being created that can be exploited. Managing cyber risks of water utilities and other critical infrastructure is thus extremely important as industrial systems evolve.

Unlike other areas of cyber-crime, CNI are part of cyber-physical systems, which have immediate and practical real-world effects on basic necessities and can cause physical harm and danger, as opposed to purely financial damage. Much of this is due to the legacy systems used in infrastructure across the globe and industrial control systems (ICS).

Key areas of cyber security management include Access Management, Environment Management, and Data Security management, controlling who can access systems, how they are organized, and how data is protected. In addition, major fundamentals of cyber security include performing basic profile and risk assessments, minimizing control system exposure and access, developing

a cyber security culture, and robust threat detection and monitoring system that can respond quickly.

In the private sector, companies must take a serious and holistic approach to their IT management systems, with pro-active assessments of their vulnerabilities before they are attacked. Even if a business views itself as low-risk for targeting, modern ransomware can cause major problems and cripple a business while extracting an exorbitant fee. In public-private partnerships this is all the more important as the private entity takes on the role of a typically government-delivered service.

For governments, the cyber risk profile has continued to evolve from individual "black-hat" actors up to state-sponsored or led cyber operations, which target intelligence gathering, compromising personal information, and seek to probe CNI systems for weaknesses, to be used in the event of a larger conflict. The many layers of government operations from local bodies, to federal agencies, and from national parks to nuclear power plants makes it near impossible to address such challenges uniformly. While national security intelligence systems receive one level of treatment, the vulnerability of public utilities also requires substantial overhaul of systems for many nations and levels of government.

Chief among these simple steps is organization and access, limiting the scope of potential breaches, and training staff to be informed and vigilant against phishing attacks or compromised peripherals from USB flash drives to CDs. Cyber risks are not just limited to financial institutions anymore, and require greater efforts to protect critical resources.

Rise of Cyber Risk & Cyber Security

The increase of automation, digitalization, and networked systems, is typically referenced as making machines, systems, and cities smarter. They provide benefits to more closely monitor systems and conditions, to adjust quickly, and thus be used more efficiently. They can reduce administrative costs by requiring less time and man-power to calculate usage and costs. However, the Internet-of-Things also makes the systems vulnerable in new ways as well. Anything that is connected to the internet, or networked, is capable of being hacked. This can vary from the innocuous of hacking a printer or HVAC system to change the temperature, or the nefarious by gaining access to addition systems to target customer data. The weakest point in any system can be an entry point to the entire system.

A natural response then is to increase the security and integrity of every access point. But this is not of interest to a smart refrigerator manufacturer. Furthermore, even the most secure systems can still be hacked by others means, whereby authorized users allow bad-actors or malicious code through the front door unwittingly. It may not even be clear a breach has happened when accessed through hardware system, as they do not have an interface that would exhibit any potential signs of having been hacked. Keeping computers and mobile phones up to date can help to close gaps and prevent break-ins, but for much hardware these are not routinely updated, or cannot be, making it difficult to patch or fix.

This takes on a greater risk when applied to industrial systems, or shared networks between a worker's computer that controls a critical function, which also accesses email and an internet browser. Without the segmentation or separation of the various systems based on their different security profiles, access to one point can lead to control of another, with very dangerous consequences. More and more examples are happening each year, from compromised cars driven remotely, denial of service attacks to take systems offline, to ransomware that takes data and systems hostage for extortion, to the melting of industrial steel plants, or the destruction of nuclear centrifuges by attacking basic industrial controllers.

The connection between these issues is referred to as Cyber-Physical Systems—whereby a mechanism or process is controlled or monitored by a computer-based algorithm, such as an assembly line, or industrial process based on the input of data, and controlled over a network. The mixing of digital, analog, physical, and human components. Essentially there is a physical outcome through a cyber process. The Internet of Things is about connecting "Things" (Objects and Machines) to the internet and eventually to each other; while Cyber Physical Systems (CPS) are integration of computation, networking and physical process.

While the former is more likely an annoyance or a privacy risk, the latter is more likely to be dangerous or weaponized to attack an electrical grid, a chemical plant, or a water treatment facility. This increase in cyber risk requires a cyber security response.

The threat posed by cyber-attacks on critical national infrastructure (CNI) is unprecedented at this moment in time. The UK recently opened a National Cyber Security Centre in response to this growing phenomenon; at the time its director declared that Britain had been subject to 188 high level attacks, “many of which threatened national security”, in the space of three months. Likewise, former president Barack Obama passed an Executive Order in 2013 titled, “Improving Critical Infrastructure Cybersecurity”.

Successful cyber-attacks on infrastructure have demonstrated the danger posed by this threat, and the ease with which perpetrators are able to exploit weaknesses in the system. In December 2015 an attack on the Ukrainian power grid compromised the systems of energy distribution companies (Pyrkarpattya Oblenergo and Kyiv Oblenergo): a total of 95% of daily electricity consumption in the country was not supplied.

On a smaller scale, an Iranian working for a company with links the Revolutionary Guards was able to penetrate the operating system (OS) at Bowman Dam in Rye, NY. While the attack did not take over controls of the system, the OS was monitored and its data security compromised. It was reported that this was a case of mistaken identity and the true target had been the Arthur R. Bowman Dam, one of far larger scale located in Oregon.

These successful breaches of critical national infrastructure are evidence of the rising threat of cyber-attacks, and the need for greater emphasis on cyber security as part of national security.

A successful cyber-attack on water related CNI would fundamentally call into question the consumer’s premise of “safe drinking-water”. The ability to manipulate the OS and override commands causing malfunction or improper use of equipment not only affects delivery of the service but has the potential to lead to causalities. Clearly any compromise in the quality of water would have repercussions on industry, healthcare, and result in considerable economic cost to water providers.

Points of critical infrastructure are inter-related and reliant on one another for their operations; indeed, they are often located at the same geographic location, and a denial of power to wastewater treatment plant can be as good as eliminating it, thus widening the scope of any potential disruption to infrastructure systems and economic activity. Such attacks on infrastructure can be the result of ransom with financial motives, but is likely to be designed to cause damage.

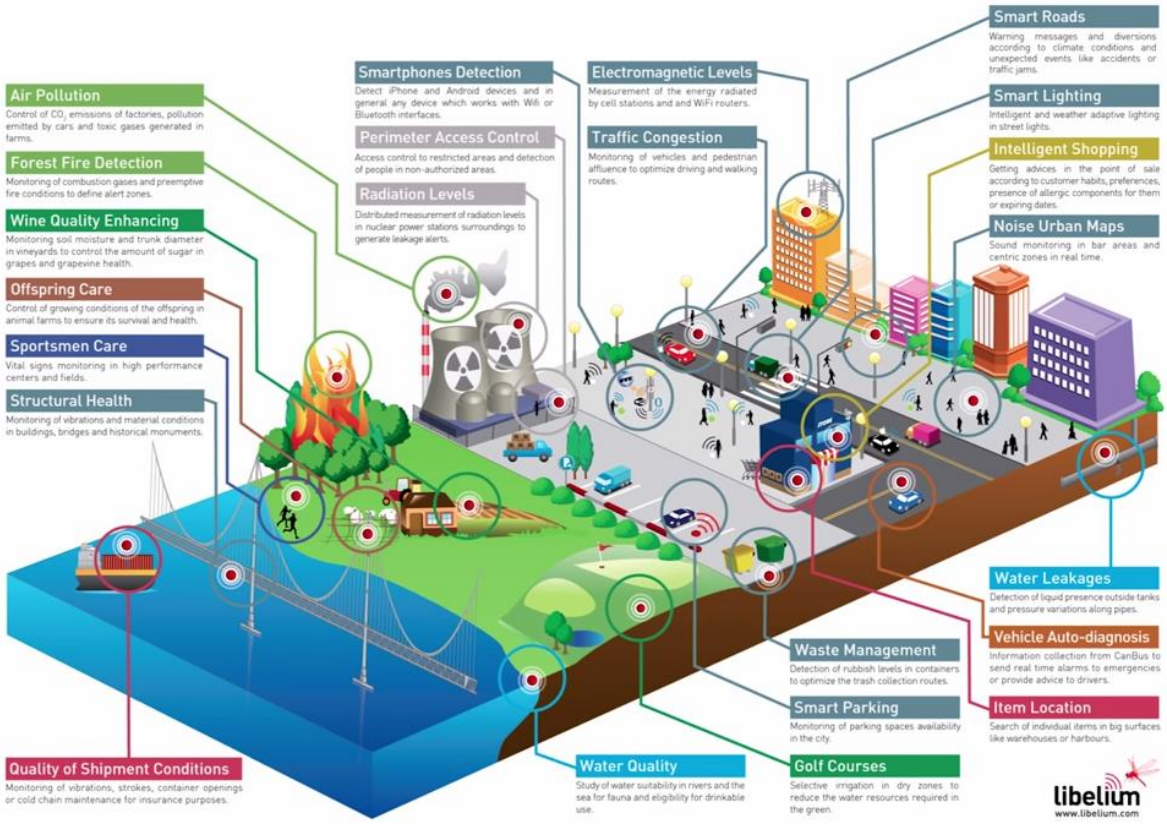
Cyber Risk & Real-World Impacts

As mentioned, the automation of many of the procedures in the water industry has created a far more efficient process, which helps to lower operation costs and make water cheaper to provide. However, this process has also increased the vulnerability of infrastructure to cyber-attacks. As shown in the figure below, more and more systems are becoming smarter and interconnected.

The primary method of these attacks is through the compromising of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Networks (SCADA), which control a majority of the commands delivered to the infrastructure as well as storing much of the data pertaining to it. These systems were designed to streamline industrial processes rather than for the purpose of security.

SCADA facilities are often located off-site from points of CNI, and often outsourced; the security of these sites is seldom seen as a priority, given that they are themselves not seen as a core element of the CNI. Security at such sites is frequently IP-led to reduce costs (run over the internet), an element that leaves them vulnerable to physical and cyber-attack. There are a number of practical steps that are recommended to mitigate the risks of such an eventuality.

- Incorporating manual overrides into the water system
- Improving hard and IP security on SCADA servers and sites
- Development of a crisis management team and protocols: in the Transboundary setting communication between governments and the respective private sectors at an early stage in the event of a malfunction will ensure that adverse effects are minimized
- Risk assessments and testing of backup/recovery plans
- Encryption and software: regular OS patches, anti-virus, encryption of devices
- Corporate culture: developing and implementing a policy that identifies and acts on points of weakness. In the transboundary setting, ensuring this culture is one of cooperation with the private sector or other entities, to enhance the security of infrastructure.
- Developing a culture of compliance and accountability between Government and private sector partners within individual states, and at a transboundary level will again help reduce risk.



Attacks on cyber-physical systems such as CNI can be accomplished in a variety of ways. For example, through the unwitting import of malicious computer code or worms, such as Stuxnet, Night Dragon, and Duqu—by improper management of data security and protocols. Or through the phishing of information by spoofed emails or internet connections. Code attacks are another variety that probe systems for weakness using SQL or MATLAB code injection to elicit a response that provides information to gain access, or to directly attack the control software doing specific functions. As more processes are automated and then outsourced, or accessed via an outside 3rd party, the vulnerabilities are spread to additional parties outside of a water utility's control. Much like having the same password for many websites, if one site is compromised, you are now compromised for all those sites.

As stated in the UK's Water Cyber Security strategy 2017-2021, "the ongoing implementation of automated Industrial Controls Systems (ICS) with the increasing interconnection of information systems, remote connection with reliance on 3rd party suppliers and integrators, has broadened the attack surface of information within water companies." While it is up to the water provider to fully own, understand and manage their cyber risks, it is also critical for governments to set the strategic direction of CNI, and to provide a legal framework that supports the industry.

The most commonly identified weakness of water and waste water utilities is a lack of appropriate boundary protection controls, whereby ICS networks and other internal networks can infect one another. The struggle in trying to eliminate this is the trade-off between the practical needs of remote access, and the isolation of control systems for protection. The result is a technology arms race to have better system protections through encryption and network segmentation, while keeping the benefits of automation and remote access. Even with encryption, corrupting data before it is encrypted at the sensor level can bypass a security regime by encrypting bad or "spoofed" data.

The most critical first step then, is a high-level risk assessment that accounts for every connection to a control system to eliminate redundancy and any unnecessary vulnerabilities. Information tools like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the AWWA Cybersecurity Guidance and Tool, and AWWA Process Control System Security Guidance for the Water Sector, provide the means to evaluate and provide a baseline assessment with a report of recommendations to secure systems from the real-world impacts of cyber risks.

Responses to Cyber Risk

In response to these increasing real-world risks from cyber threats, governments and companies need to take a holistic approach to their securing their systems. The WaterISAC (Information Sharing and Analysis Center) provides a breakdown of the 15 cyber security fundamentals or water and wastewater utilities to address Information Technology (IT) and Operational Technology (OT) attacks, particularly in the face of more advanced nation-state directed attacks on systems.

The 15 fundamentals are:

1. Perform Asset Inventories
2. Assess Risks
3. Minimize Control System Exposure
4. Enforce User Access Controls
5. Safeguard from Unauthorized Physical Access
6. Install Independent Cyber-Physical Safety Systems
7. Embrace Vulnerability Management
8. Create a Cyber Security Culture
9. Develop and Enforce Cyber Security Policies and Procedures
10. Implement Threat Detection and Monitoring
11. Plan for Incidents, Emergencies, and Disasters
12. Tackle Insider Threats

13. Secure the Supply Chain
14. Address All Smart Devices (IoT, IIoT, Mobile, etc.)
15. Participate in Information Sharing and Collaboration Communities

In short, utilities must know where they stand before they can make the necessary adjustments, and even the best systems can be compromised by the actions of employees, either due to bad intentions or a lack of education. It is also important to recognize the differences between the needs of the IT world, vs. the ICS world. For example, the temporary creation of networks to communicate can work for IT systems, but not for control systems and physical machines. IT hacking is primarily about stealing data and intellectual property for financial gain, while control system hacking is primarily about sabotage.

After performing a Risk Assessment to establish the facts on the ground, the documentation of policies and procedures to establish best practices that are then trained to personnel and any contractors interacting with the system. Furthermore, the architecture of the system in terms of segmentation and access control are the next tactical steps to prevent cyber attacks or infections. Distinct security zones and levels of access that include both credentials and physical barriers help prevent internal bad actors from breaching a system.
However, in spite of this, a simple email attachment can lead to the deployment of malware and screen recording software that gains access to an entire banking system and the lose of millions of dollars.

The Role of Government and the Private Sector

The UK's Department for Environment, Food and Rural Affairs (DEFRA) Water Sector Cyber Security Strategy sees a need to ensure close cooperation between government and private sector. While it states that "industry has a responsibility for the security of their systems" and must, "own, understand and manage the risks to their assets", the role of government is to provide strategic oversight, share information, and ensure a regulatory framework is in place to protect consumers and service providers in the event of a cyber-attack. This creates a number of challenges at the transboundary setting.

Firstly, governments will provide different regulatory requirements for their respective suppliers, or possibly at different levels of government (local, state, federal). In some instances, security pertaining to cyber-attacks could be highly sophisticated in one state (A), whilst a neighboring state (B) lacks stringent regulation. Meanwhile, a state (C) that is hostile to state A can exploit weaknesses present in state B to inflict damage. Regardless of state A possessing a strong regulatory culture and security, both states A and B suffer. In this light, cooperation is critical between governments and the private sector at a trans-national level to ensure that CNI remains protected from cyber-attacks at the regional level.

The UK National Cyber Security Strategy identifies "states and state-sponsored threats" as presenting a serious challenge to its cyber security defense network. Such attacks are motivated out of "political, diplomatic, commercial, technological advantages", and as the incidents in Ukraine and US prove multiple states have cyber capabilities that are able to penetrate defenses.

The success of Stuxnet as a "cyberweapon" that targeted Siemens industrial control systems and compromised the uranium enrichment facility at Natanz, Iran, indicates that "worms" are being developed with the intention of compromising CNI. That Iran perceived the attack as "an electronic war", indicates that we are entering a period in which states perceive cyber-crime as an effective platform with which to undermine their enemies. Russia is reportedly developing a cyber-espionage campaign named "Energetic Bear", which has been linked to the Havex malware first identified in 2014.

Government should play a prominent role in addressing and countering this threat; at a transboundary setting this may include bilateral/intra-national sharing of intelligence related to cyber-threats on CNI. In addition, tracing attacks that may have been routed through other countries servers, or spoofed (faked) to be from elsewhere, will require the cooperation of other nations to investigate the attack. Pro-active cooperation and data sharing are critical to help monitor threats and deploy solutions as quickly as possible.

The report also notes that insider threats, "malicious insiders" (i.e. those with access to operating systems), as posing the greatest threat. There is a precedent for such cyber-crime occurring, such as the Maroochy Water Services breach in 2000 which released 264,000 gallons of raw sewage into the water network. The perpetrator was found to have been an ex-employee motivated by personal grievances having not secured a job at the local council.

The private sector has a significant role in developing and implementing adequate procedures and policies which report and prevent cyber-crimes. Considered alongside the global, political threat, governments sharing transboundary water resources should strive for a secure and effective system of cyber security whilst developing contingency plans for the event of a cyber related malfunction to ensure a rapid response which minimizes damage.

Cyber Security in Transboundary Settings

Transboundary environmental issues are unique challenges that deal with problems in coordination, trust, sharing information, costs, and burdens, in a way that is mutually beneficial. The same is true of cyber security challenges.

In addition to the fact that attacks can come from anywhere in the world, in the context of shared infrastructure or shared resources basins, an attack or compromise in another nation can have detrimental effects on their neighbors—whether a wastewater treatment plant, an electrical grid, or general instability.

Cyber-attacks on water infrastructure at a transboundary setting pose a number of challenges. Shared water resources are inherently politicized locations; domestic and international conflicts are often the drivers of policy in such an environment. Any attack which compromises waste-water treatment plants, dams or water related CNI in a transboundary setting will have consequences on multiple parties, regardless of the origin of the security breach.

In the event of any cyber-related incidents, stakeholders at any transboundary water resource face the issue of accountability and liability not just in their own territory but potentially other states. Consequently, a breach of security at water related CNI could result in a deterioration of existing bilateral relations. It is therefore in the interests of all parties in a transboundary water setting to ensure that adequate security systems are in place to protect CNI.

Some recent examples of cyber security cooperation on a regional or transboundary basis include the US-Singapore ASEAN Cyber Security Technical Assistance Program, to share information on threats, best practices, and the provision of technical standards that build cyber security capacity, particularly with critical infrastructure protection. From the Cyber Security Agency of Singapore, "With cybersecurity as a transboundary issue, strong international partnerships remain key to navigating the increasingly complex cyber terrain."

Other examples of transboundary cooperation on cyber issues include hacking investigations via Europol, NATO cooperation, and other EU inter-governmental cooperation, such as between Estonia, Finland, Germany and Slovenia after a series of attacks in 2007. While only Estonia was attacked, the threat of similar attacks spreading to other countries provided incentive for them to

work together to share capacity and resources to protect themselves.

"Joint action in response to transboundary crises is more likely when states are uncertain about the consequences of attempts to unilaterally reduce their exposure to a transboundary crisis"

The Future of Cyber Security for Public Infrastructure

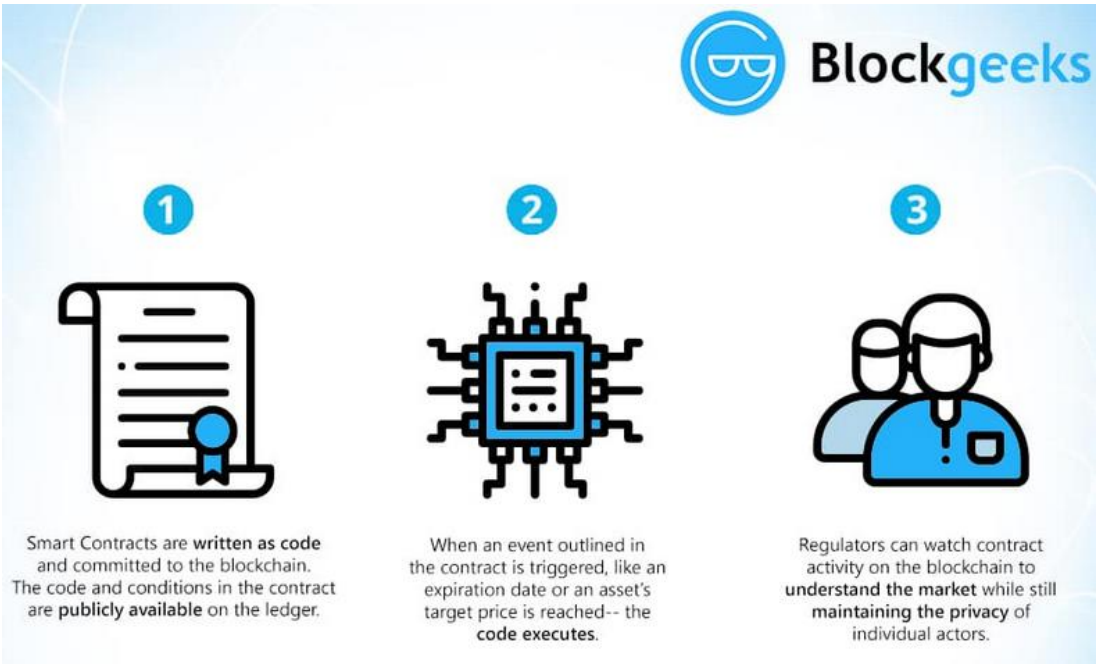
As previously mentioned, one way to protect data and information shared across networks is through encryption. A new method of encryption using a distributed system—which is harder to fake or manipulate—along with cryptography for security, is the blockchain. Blockchain is most simply a ledger of information, which is distributed, meaning spread throughout the internet. Every piece of information, or transaction, is a block of data, which is added to an unalterable chain. The key though, is the distributed nature that all must agree on in order to add another block. This means you can't alter the past data, and new data can only be added when it is verified by many different parties.

For the water sector, public utilities, or even hospitals, this means data can be stored and shared without fear of it being compromised. Most famously, blockchain has been used to make digital payments using cryptocurrencies. However, another usage is for "Smart Contracts," whereby a transaction can only take place when certain criteria are met, and the system has verified this across the distributed network. The data stays encrypted, but the blocks are verified, and a transaction only occurs if all conditions are met.

However, this can be utilized in a number of ways by building apps that run on these principles, and can be useful to share and protect public data. For example, as a government regime changes and wants to eliminate public information, data secured on a blockchain will stay public, such as climate data, or GPS information.

The sharing of water data between riparian parties is continuous political process that suffers from issues of data security and trust, which are inherent characteristics of blockchain. Using decryption keys and distributed public ledger, parties can share data securely while limiting access to the relevant parties, in a cost-effective way.

For a water utility the use of smart meters and smart contracts can greatly reduce the cost of



administration of billing for services, while safely securing the information of end-users that is less susceptible to hacks that reveal customer information.

"In the previous two decades the Internet has reshaped our lives like nothing else before, however, today most of our online interactions require some kind of impartial third-party mediator. Lately, these mediators tend to build business models that are gravitating around using and/or misusing the data collected during the process of mediation. Moreover, the activities that are needed to establish the trust among the stakeholder of a certain process are placing huge overhead in terms of time and money. The blockchain offers a way to resolve these issues that surround traditional transaction systems by making trust obsolete and in the same time making these interactions safer, cheaper and faster."

Case Study: State-sponsored Cyber Attacks – Russia, U.S. attacks, Stuxnet

Over the last several years critical control systems in American infrastructure, ranging from nuclear powerplants to water and electric systems, have been attacked and compromised by hackers thought to be from Russia, with the potential to sabotage or shut off systems at will. In response, the US has reportedly deployed similar attacks against Russian infrastructure targets as a deterrent, which also has the potential to further escalate tensions and an outbreak of conflict. A new generation of MAD, or mutually assured destruction.

The nature of the attacks touches on the same vulnerabilities mentioned earlier—the industrial control systems (ICS) that manage the operation of CNI. Such efforts have been probed since 2012 according to reports, with invasions meaning the potential for attacks lying dormant until political motivations change and they are utilized.

A landmark example in the history of cyber warfare and cyber security is the Stuxnet worm that was uncovered in 2010. It is a critical inflection point as the cyber landscape was altered, into that which existed before Stuxnet, and existed after. Once the code was released, and eventually discovered, it could then be reverse engineered to recreate the worm, and be used by others elsewhere in different permutations.

Stuxnet, was a malicious computer worm that was designed to search out a specific target, but otherwise lay dormant and undetected. Its purpose was to sabotage centrifuges used in the Iranian nuclear program, by selectively targeting specific systems, spreading through networks and systems intelligently looking for its target. As a type of worm, the code is introduced to the system often by an infected USB, which then burrows through the networks looking for a particular software used to run the PLCs being targeted in the attack.

In the case of Stuxnet, an infected USB flash drive introduced the code, which scanned and spread looking for the Siemens Step7 software on computers controlling a specific PLC—programmable logic controller. The PLCs were then misused to run the centrifuges too quickly until they tore themselves apart and were destroyed. PLC units are specifically designed to execute industrial processes efficiently and can communicate over networks in SCADA (Supervisory Control and Data Acquisition) systems—ruggedized automation for harsh industrial environments.

Considering the information presented thus far, it is easy to see how such a worm being able to be dormant while filtering for its target in a secret nuclear facility, could also be deployed against very public water, electrical, or gas infrastructure, with serious consequences. Stuxnet was able to clandestinely destroy thousands of Iranian centrifuges before it was discovered.

In the case of Stuxnet and other attacks, one or more Zero-Day exploits were utilized in order to execute the cyber-attack. Zero-Day exploits are vulnerabilities in systems that are not currently known to system administrators or the outside-world—unknown unknowns—which only become known once they are utilized, and only if they are traced back. This further shows the critical importance of using due diligence and best practices in cyber security regimes and policies. Even highly sophisticated and air-gapped systems can have numerous vulnerabilities once that air-gap is breached, such as with an infected USB.

These state-sponsored hacking efforts exemplify the much larger scale of operations and available resources that can drastically outweigh the level of support that an average company or public utility may be able to defend against.

Case Study: Kemuri Water Company

Our final example comes from a report by Vericlave regarding a water company under the pseudonym of Kemuri Water Company, or KWC.

Verizon, a security firm, was contracted to conduct an assessment of KWCs systems and cyber security profile to identify potential weaknesses. They found that KWC had a poor network and security architecture, with unsecured and out-of-date systems, plagued with known exploitable vulnerabilities and legacy operational technology (OT) systems. During this process of conducting this assessment, Verizon found that a current threat actor was at work stealing financial records, and manipulating industrial control parameters used to purify water at the plant.

"Behind the scenes, KWC was a likely candidate for a data breach. Its internet facing perimeter showed several high-risk vulnerabilities often seen being exploited in the wild. The OT end of the water district relied heavily on antiquated computer systems running operating systems from ten-plus years ago. Even more concerning, many critical IT and OT functions ran on a single AS400 system. KWC referred to this AS400 system as its SCADA platform."

As referenced in our 15 principles before, KWC was operating on out of date OT, with a vulnerable SCADA system, that was not properly segmented to protect it from known vulnerabilities, let along unknown zero-day hacks. This included allowing the corporate network systems, which are directly exposed to the internet, to interact with the ICS/SCADA systems making it very simple for an infection to spread laterally and through the system.

The AS400 system, "which functioned as a router with direct connections into several networks, ran the water district's valve and flow control application that was responsible for manipulating hundreds of Programmable Logic Controllers (PLCs), housed customer PII (personal information) and associated billing information, as well as KWC's financials. Moreover, only a single employee was capable of administering it. If a data breach were to occur at KWC, this SCADA platform would be the first place to look."

The conducted assessment report indicated that SQL code injection and phishing were the primary attack vectors deployed to gain access to the water company's payment portal website and the water district's internal AS400 system. Accessing the AS400 server provided attackers with approximately 2.5 million customer records, the ability to manipulate SCADA controls (valves, chemical mixtures, and water flow), additional password files, back-office system configuration settings, and other sensitive data.

As mentioned, SQL code injection (malicious code probing) followed by social engineering (spear phishing scam), are fairly basic hacking methods that can be prevented from having hardened systems, and better training of employees on cyber risks. Even a sophisticated hacking strategy could have been mitigated or limited in impact of the proper segmentation strategies were employed by KWC.

Basic network hygiene and best practices would reduce many of the vulnerabilities. Segmenting systems, meaning to be separated or sandboxed, better prevents intrusion, and protect critical systems from breaches in other areas of the company. This should include separating the AS400 central processing system and the ICS/SCADA system to control the plants physical operation, from the financial payments system with customers, or the corporate IT system.

Furthermore, having pre-configured devices only able to communicate with isolated systems or zones of operation provides another layer of protect to prevent exfiltration.

KWC is one example of how hackers can penetrate into physical infrastructure, cause real-world problems, and do so in a way that is undetected, or lying dormant to be used at a later date. CNI needs to be better protected and thought about more critically, with greater sharing and interaction between countries and regions to identify, monitor, and prevent cyber risks.

Sources for Further Learning

American Water Works Association

Cyber X (IDE Technologies)

Dragos

Vericlave

Websites & Articles

Introduction to Smart Contracts

Blockchain Basics

Cyber-physical attacks: Hacking a chemical plant - CSO Online

Dubai Aims to Be a City Built on Blockchain - Wall Street Journal

Hackers pop German steel mill, wreck furnace: Phishing proves too hot for plant - The Register

How blockchains could save us from another Flint-like contamination crisis - Venturebeat

The internet of things can be hacked–and the risks are growing every day - TechRadar

Managing cyber risk in the electric power sector Emerging threats to supply chain and industrial control systems - Deloitte

Musings on how the blockchain might help streamline California's water markets - Argo Labs

Now That Everything Is Connected, Everything Will Get Hacked - Popular Mechanics

U.S. Escalates Online Attacks on Russia's Power Grid - New York Times

U.S. Water Utility Breach and ICS Cyber Security Lessons Learned - Belden

Using Blockchain to Keep Public Data Public - Harvard Business Review

Using the Ethereum Blockchain for Data Sharing in Healthcare - ETHNews

Water and Wastewater Cyber Security: Strengthening the Chai - WaterWorld

Books & Reports

7 Steps to ICS and SCADA Security - Tofino Security

15 Cybersecurity Fundamentals for Water and Wastewater Utilities - Water ISAC

Cybersecurity Principles for the Water Industry - Water UK

Cybersecurity Risk and Responsibility in the Water Sector - AWWA

The Kemuri Water Company Hack - Vericlave

National Cybersecurity Awareness Month Resources - US Department of Homeland Security

Water Sector Cyber Security Strategy 2017 – 2021

Acknowledgements

The MEDRC Transboundary Waters Practitioner Briefing series has been developed for water industry practitioners and government officials at the request of MEDRC's member countries, with sponsorship provided by the Netherlands and Sweden. The briefings are meant to be informative and practical, providing an overview of the subject matter material, while remaining accessible to various backgrounds and disciplines. The briefings serve to develop shared knowledge and serve as a basis of further discussions between partners. If you would like to learn more about these subjects, please see the section "Sources for Further Learning."