Virtual meeting WATER AND CYBER SECURITY PROTECTION OF CRITICAL WATER-RELATED INFRASTRUCTURE
18 November 2020

The meeting was attended by 150 participants online.

Key conclusions/messages:

The majority of water utilities/water infrastructure is still not using systems that allow to optimally prevent cyber-attacks and minimize negative impacts. There are a few key issues that need to be addressed to make societies more resilient against malicious, criminal and terrorist activities.

1) There is a significant gap between legal framework, political discussion and practical operation of water infrastructure. This gap can be addressed by:
   - More and better practical guidelines/standards to strengthen local capacity;
   - More information and communication around the topic to sensitize regional and local level.

2) Key human and technical capacity is lacking or the dots of existing capacity are not connected. This shortfall can be addressed through:
   - Training at local and regional/river basin level;
   - Developing shared regional procedures and methodology to create more peer to peer learning and education;
   - More tools and use cases should be openly available and help local level increasing their capacity and system robustness;
   - Possibility to validate/test/improve systems/staff in a secured environment.

3) Coordination and cooperation is lacking both in country, between sectors (policy/operations/legal sector). This deficit can be addressed through:
   - Establishment of observatories/information centers that allow to share experience, methodology/technology and serve to connect players at national and regional level

Further steps: An enlarged group of interested countries will follow up discussing concrete possibilities to catalyze actions related to resolving the key issues. Partnerships will be sought and a next step will be discussed and proposed by early 2021.

Minutes of the meeting:

Prof. Petteri Taalas, Secretary-General of the WMO, opening remarks:
- Cyber-attacks on water-related infrastructure have become an increasing problem that have to be dealt with on top rising water demand, climate change impacts. Vulnerability of critical water infrastructure is increasing.
- There is a need to strengthening coordination among Members, multilateral and regional organizations, civil society, businesses and other stakeholders.
- International cooperation contributes to safety and security of critical infrastructure that is needed to protect people and feed the populations.
- Climate change is important to tackle – global warming a bit misleading.

- Drought, flood, lack of water, mentioning host organizer who have been facing out these challenges (Israel drought, Slovenia severe flooding and droughts) playing a leading role.

Dr Uroš Svete:
Water will be high on the agenda during the EU Council Presidency in the second half of 2021, where also cybersecurity, as part of strengthening the overall EU resilience, will be one of our main priorities. In the EU, the NIS Directive is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity. The Directive on security of network and information systems was adopted by the European Parliament in 2016.

Mr Joze Tomec
Today, the functionality of the water supply systems depends on the networks where information, communication and operational technology and the internet, respectively, meet and cooperate. He stressed the importance of recognizing the cyber security as one of the most important factor of the drinking water supply systems' safety. The adequate cyber security policy, confirmed by top management, risk management, thorough planning and implementation of the effective protective measures are the key elements of the high level of the cyber security in the drinking water supply systems. The nation legislation and the international standards provide us an important framework for achieving that.

Mr Danny Lecker
- Main issues on Cyber Security: Human beings cannot exist without water; Water is consumed by everyone daily; Water supply cannot stop.
- Israel Cybersecurity Forum.
- Cybersecurity is crucial for operations continuity.
- Continuous service and supply of all facilities of water: doing routine check-ups and drills to make sure water consumers are protected.
- Israel experienced attacks in past and is open to share best practices – creation of relationships on the subject.
- Water supply detected by Cybersecurity.
- Water suppliers must be well trained.
- One advice to water suppliers – make sure that facilities are disconnected from Internet and operate with other connection levels.

Mr Raanan Adin
"Unique characteristics of the water sector" - Water has unique characteristics in view of cyberthreats. The different vulnerabilities of IT (Information Technologies) and OT (Operation Technologies) are explained and a focus on OT is recommended. A case study is presented, demonstrating the complexity of risk assessment and mitigation by showing how disrupting sewage pumps might cause water supply shutdown and evacuation of a city.

Mr Tamás Belovai
- Surface and ground water resources.
- Waste-water infrastructure.
- Protecting water resources.

- Flood protection resources, dykes, reservoirs, barriers, hydropower structures
- Threats; Nature side – Flooding, climate change; Human side – hackers, terrorists, armed forces.
- How to increase awareness and resilience of water sector against cyber-attacks.
- User training to take place at 3 levels: Senior management, decision makers; Priority users; normal users.
- Training is the most important plan – e-learning, live performance, newsletters, etc.
- How to improve cyber security in transboundary water mechanism?
- Close cooperation on used developed applications and adopt good solutions.
- Appropriate communication about experience.
- Sharing knowledge.

Mr Jon Albert Fanzun

- No cyber-attacks on water infrastructure in Switzerland.
- Domestic level – Confederation works closely with municipalities – municipalities own their own drinking water.
- Hydro power generated from these sources, electricity and power station.
- Public private sector is a key element.
- Water supply and energy facilities.
- Valuable guidance in the protection of water from cyber-attacks.
- Switzerland will stay engaged with critical water infrastructure.
- Resilience system in terms of water security.

Mr Leonardo De Vizio

The presentation was about the NIS Directive (the first EU horizontal cybersecurity law applicable to the drinking water management sector, among others) and its impact on the protection of the cybersecurity of operators of essential services across Europe. I will provide an overview of the results achieved so far and describe which are the main features that the Commission is looking at in the current evaluation process, which may lead to its revision.

Ms Sonja Koeppel

60% of all freshwater flows in shared basins. Cyber-security attacks on water-related infrastructure in one country, e.g. located upstream can have significant impacts in other riparian countries. Cooperation on infrastructure in shared basins is important, and in some basins, such as the Senegal and Gambia basins in Africa, dams and water storage infrastructure is even jointly constructed and owned by all Member States. Such cooperation can then also cover cyber-security, if relevant. The Convention on the Protection and Use of Transboundary Watercourses and International Lakes (Water Convention) provides a unique global legal and intergovernmental framework for transboundary water cooperation.

Ms Kaja Ciglic

- What is the concept of Microsoft and how do you deal with the Cyber Security?
- Increasingly scarcity in certain water reservoirs.
- Disconnect technologies from water supply.
- Ensure that leaks could be detected easily.
- Microsoft policy focused on risk management.
- Ensuring particular aspects of information.

- Ensuring how the infrastructure sewerage and drinking water not being attacked.
- Establishment of platform work together not just operators but also the water companies
- Impact of attacks in ensuring to collaborate in sharing knowledge

Mr Tadej Slapnik

By providing a secure, transparent and distributed ledger to record transactions between parties, blockchain technology could fundamentally transform the way water resources are managed and traded. Blockchain based solutions and applications for protection of critical water-related infrastructure require fast, secure and scalable blockchain infrastructure. He presented SI-Chain - national blockchain infrastructure enabling testing of existing and new blockchain applications for the public and private sector in Slovenia. Collaboration and sharing good practices, on-going projects on building collaboration has concrete results Cooperation between or among private sectors is required at different levels

Dr Sara Bitan

Water control systems are in the process of migration to smart water grids, where there is tighter integration between water and information. This integration increases the attack surface of the water system and makes them more susceptible to attacks. At the core of the water control system lies the PLC. In this device a bit stream enters on one end, and things are moving on the other end. But they are vulnerable, as we demonstrated in our attack on Siemens S7-1500 PLC that we presented in Blackhat conference last year. When the attacker can communicate with the PLC it is game over. So, we have two alternatives: 1) the water system experts can build a good and efficient system with more layers of defense. 2) build securely, which requires cyber security experts to become familiar and knowledgeable in water security, and the water experts, to understand cyber security. Sara advises that both experts cooperate from the beginning as integral part of the system.

Mr Shaul Rom

- Does global trend of using cloud computing exposes utilities to cyber threats or provides better protection?
- Investigation of attack happened in 2020 shows that no cloud SCADA was penetrated while traditional SCADA systems that were connected did suffered from the same attacks.
- Cyber technologies used by modern SCADA systems are evolving exponentially, similar to information growth.
- Modern cloud SCADA minimize infrastructure of control centers and at the same time extend connectivity and integration of data from many different sources.
- Cloud technologies enable the implementation of all components required to modern organizations: real Time Remote control, Analytics, notification and more.
- Cloud computing is the only was to share information and control among countries sharing the management of the same infrastructure.

Mr Enrico Formica

- Water conflict – Climate change.
- Conflict use of technologies.
- Prevention from malicious acts.

- Practice of good office cooperation.

Dr Kubo Mačák

Recent years have shown that malicious cyber operations disrupting the provision of essential services to the civilian population may pose significant risk to human life. The International Committee of the Red Cross is particularly concerned about the potential human cost of cyber operations conducted against critical civilian infrastructure, including water infrastructure. This presentation will focus on the protections that international law affords against malicious cyber operations targeting water infrastructure during armed conflicts.

Hichem Khadhraoui

Water infrastructure across the globe is being digitized and automated much like any other critical infrastructure. Attacks against water infrastructure could be by both state and non-state actors. Humanitarian consequences could be massive with floods of entire areas and interruption of essential services with long term consequences. What is the role and influence of ANSAs in cyber-attacks on water related infrastructures? While ANSAs do not play major role today, it may become an important aspect of the war in the future. What the international community should do to mitigate the risks on civilian populations?

Andraz Kastelic

To reduce the risks and manage potential future instability, States should do their utmost to observe and implement the norms of responsible State behavior in cyberspace, suggested by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2015 (UNGA RES 70/237). Accordingly, States should, first and foremost, implement measures to protect their own critical infrastructure. Second, States should refrain from directing their offensive cyber capabilities against foreign water systems and do their utmost to prevent malicious actors under their territorial jurisdiction from doing so as well. Last but not least, when a malicious cyber operation does affect a water management system, States should respond to calls for assistance or mitigation by the affected nations.

Mr François Münger

The Geneva Water Hub (GWH objective is to prevent water-related conflicts and even to promote the use of water as an instrument of peace. Growing opportunities created by digital technologies are paralleled by stark abuses and unintended consequences. In this connection, we would like to contextualize the issue of cybersecurity for water and water-related infrastructure: Water data are essential to build water cooperation and peace; Transparent exchange and sharing of water data are key to build trust and cooperation; it is mandated by the global water conventions and human rights; Cybersecurity is a necessary, though not sufficient element to protect critical water-related infrastructure. GWH will include cyber security specific principles in the Geneva List for the protection of the water infrastructure during the armed conflicts.

Dr Jovan Kurbalija

- Global and digital cooperation.
- Real problem with digital (digital policy is done in silence).
- Discussion on not having reflexion on standardization

- Key challenges form national to global.
- Global digital policy connection, data governance, cyber security.
- Cross cutting policy – development of some formal information to keep this issue.
- A place where country can voice their problems.
- Establishing a group of friends in Geneva.

Key words from interventions:

- cooperation is very useful -good areas of opportunities
- cross cutting issues
- topic is very important to bring states, private businesses together
- coalition and partnership
- sharing of good practices. Essential norms
- follow-up include in the Geneva list the question of water and cyber security – not only to write articles but to work together with partners
- development concerning the cyber security
- take care of standardization include water relevance issues
- reduce loss in translation
- organize training for water people
- increase the cross-cutting state responsibility very useful in digital fields
- create observatory to follow development
- human connection is important
- urgent need for int'l cooperation
- exchange views for cyber security