MAWAC-ENA WORKSHOP

PARIS

November
2025

Cyber Security in Water Management

Bruno NGUYEN

W-SMART

Paris

Some digital events in 2025

Cyber Attack

Failure

X February 21st, in less than one hour, the Lazarus Group, a criminal organization sponsored by the government of North Korea, stole crypto money for around 1.5 billion USD, one of the top bank robberies ever seen.

X In April, in San Francisco, in the world annual cybersecurity summit, it was said that « if cybercrime were a legal industry, it would rank third in the global economy, behind the USA and China: 10,500 billions USD per year.

X In April a massive cyber-attack against Marks & Spencer in the UK was initiated by a hacker group named Scattered Spider: it cost nearly 400 million USD and market capitalization losses reached close to 800 million USD.

This summer, on July 25th, Internet satellite services provided by Starlink stopped for 2.5 hours due to a software failure. X

On October 20th, just a month ago, a breakdown occurred on a server at Amazon Web Services (AWS) in a data center in Virginia: according to Axios, this failure impacted 11 million people worldwide. X

Cybersecurity vulnerability increase in 2025

Huge data centers concentrate vital infrastructure in one place and not only contribute to severe environmental consequences but also significantly raise the potential level of impact of a single event like a technical failure or an attack.

The failure of the cloud and of the Internet is called the Big One. Not long ago, this denomination was used for the expected high magnitude earthquake that will hit California in the future; but its new meaning refers now to a digital earthquake.

40% of UK companies have been hit by a cyber-attack in 2025, like Jaguar Land Rover which was forced to stop its production for more than a month last summer.

According to the UK government, 25% of the companies of the country recognize that they have been subjected to ransomwares, and it is estimated that 94% preferred to pay.

Cyber attacks statistics and predictions

According to Sophos, ransomware in 2024 accounted for 59% of all cyberattacks faced by organizations; the average ransomware **payment reached 2 million USD**.

Cybersecurity Ventures states that by 2031, a ransomware attack will hit a business or consumer every 2 seconds; in 2021, it was every 11 seconds.

CFO reveals that 85% of cybersecurity professionals attribute the increase in cyberattacks to generative AI used by bad actors, who now have faster, smarter ways to exploit systems.

Gartner states that 17% of cyberattacks will employ generative AI by 2027.

In brief

- Number of cyberattacking has grown significantly in the past year.
- Cyberattack pressure is reinforced by Gen AI and we can presume that it will become worst in the future.
- Hacker use the vulnerabilities of Information Systems and the lack of employees' awareness and training (phishing..).
- For both causes, employees and specially OT & IT teams and operators need to be trained to avoid breaches (IS patching, daily reflex to adopt).

A SUCCESSFUL CYBER-ATTACK IS A CRISIS

Unlike for other risks (environmental, accidental, related to non-criminal human activities, etc.), there is always someone behind a cyberattack: this individual has been able to anticipate the reactions of the targeted victim and incorporate them into his attack plan to cause maximum damage.

➡ **Worst case scenario should always be considered in case of a cyber attack**

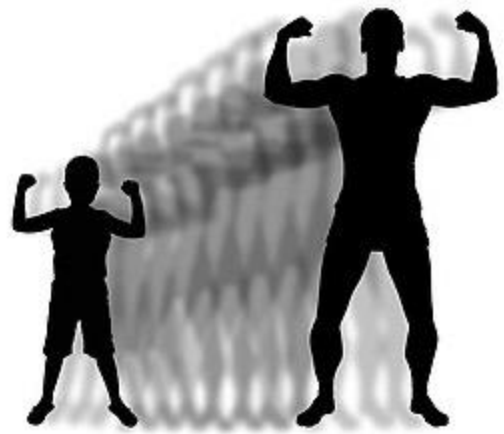
TRAININGS & EXERCISES ADDED VALUES

- Discovering weak points in the system without being in real crisis.

- Uniform language between the participants and other agencies

- Proper response in times of crisis at all levels.

- Improves the transitions from routine to emergency



Volunteer?

On stage training in VR

CONCLUSION

- ATHENA proposes a new learning method including VR, eLearning and Table-top tools for increasing cyber-security at critical water infrastructures' managing utilities.
- Training of vital water infrastructure operators is already partially available, and ATHENA consortium can propose free Beta testing to other water utilities.
- More scenarios for training including VR can be envisaged and designed by a collaborative work between ENA Megacities .
- Proposal for another ATHENA/MAWAC ENA workshop during next IWA WWCE in 2026 in Glasgow involving several ENA Megacities.

Thank you for your attention

NAME : Bruno NGUYEN

INSTITUTION : W-SMART

MEGACITY : PARIS

MAWAC- ENA PARIS

NOVEMBER 2025

ACCORD DE PARIS COP21 10 years PARIS AGREEMENT

Métropole du Grand Paris

eau de Paris service public de l'eau

SEINE GRANDS LACS

ARCEAU Île-de-France

RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

AGENCE eau SEINE NORMANDIE

Under the auspices of unesco Intergovernmental Hydrological Programme

WSMART Water Security Management Assessment, Research & Technology