

The Future of CIP

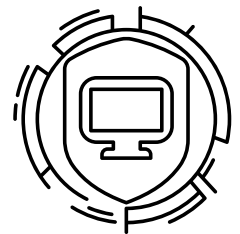
Trends and innovation in the Security Industry

July 2024

The building blocks of our society – administrations, power grids, schools, water treatment facilities, transportation and communication systems – collectively known as critical infrastructure, face an ever-evolving threat environment. Those threats are always increasing as all systems become interconnected and reliant on digital technology. As the security industry competes with imagination and technique to answer those new challenges and create a more resilient protection, these new technologies also create breaches in the traditional shield. This observation interrogates the future trends and innovation in the security industry, and how to apprehend them to make the best use out of them.

The Evolving Threat Landscape

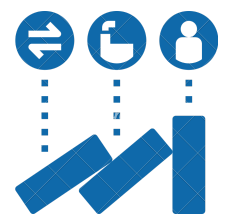
Traditionally, the threats to critical infrastructure were identified as physical and associated with sabotage and terrorism. However, the digital revolution opened a new playing field and with it a new breed of threats: cyberthreats. Those threats take various forms and exploit the vulnerability of the systems to control them, disrupt operations, steal data, or cause widespread outages. These attacks become more and more sophisticated with ransomware and advanced persisted threats (APTs). Every



individual can become a weakness to the system by the development of phishing campaign easily creating breaches. These observations underscore the urgency to fortify cybersecurity measures.

In addition to those ever stronger and more complex attacks, the system is also weakened by its interconnectedness and the development of new technologies.

Because of the systems interconnectedness a domino effect is easily triggered as an attack on one sector can cascade and disrupt another causing widespread chaos. This becomes an even more predominant challenge considering that the Internet of Things (IoT) creates new connections and thus new attack vectors requiring innovative security solutions. A very eloquent example would be the 2015 cyberattack on the Ukrainian power grid. Hackers gained access to the control systems and caused widespread blackouts that left hundreds of people without power for hours. It highlighted the vulnerability of critical infrastructure to cyberattacks and the potential for cascading disruptions across different sectors.



The trend toward of drones' miniaturization, long endurance and autonomous flight capabilities, render these systems increasingly difficult to detect, identify and intercept before they can do any harm.



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.



The breakthroughs in quantum physics call into question all encryption methods used to secure communication of critical infrastructure. Because of their renewed and improved calculus capabilities, quantum systems would be able to break widely used encryption algorithms like RSA or ECC used to secure communication and data storage in critical infrastructure. A new threat that is however already well identified by security practitioners.



These latter, in the light of those emerging or renewed threats, work on new approaches and trends to shape the future of CIP.

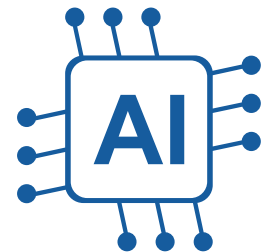
Trends Shaping the Future of CIP

Artificial Intelligence and Machine Learning

The most famous trend in the security sector might be Artificial Intelligence (AI). Its capability to handle great loads of data and to analyse them makes it a very useful and effective tool for threat detection. With its extensive and always updated knowledge of the system through Machine Learning, AI can also produce analysis for predictive maintenance and help security practitioners by improving decision making. For instance, French firm Cyberwatch developed a Vulnerability Manager to this end. This is a vulnerability management platform, with mapping of the information system, detection of vulnerabilities, prioritisation based on risk and business constraints, decision support and an on-board correction module.

Generative AI can also be used to simulate cyberattacks and help infrastructure identify and address potential vulnerabilities. Artificial Intelligence it is also at the core of autonomous systems operations.

Protection against cyber attacks tampering with AI software across the systems lifecycle is crucial to avoid breaches and dangerous malfunctioning.



Cloud and Zero-Trust Architectures

The shift towards cloud-based solutions for critical infrastructure management necessitates robust cloud security strategies. Zero-trust security¹, which assumes no user or device is inherently trustworthy, is gaining traction as it enhances access control and minimizes the attack surface.



¹ 3 principles of Zero Trust Architecture:

Verify explicitly: consider every data point before authenticating someone's access, including their identity, location, and device, as well as how the resource is classified and if there's anything unusual that might be a red flag -

Use least privileged access: limit the amount of information and length of time people can access something, instead of providing access to all company resources indefinitely.

Assume breach: segment networks so if someone does get unauthorized access, the damage is contained. Require end-to-end encryption





Blockchain technology

In a blockchain, every new block connects to all the block before it in a cryptographic chain in such a way that it is nearly impossible to tamper with. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is true and correct. By securing each part of the process, blockchain is proved to be a very safe-providing technology and is thus more and more used in CIP.



Integration of Physical and Cybersecurity

A siloed approach to security is no longer effective. The future lies in integrating physical and cybersecurity measures to create a holistic defense system. For example, if an AI system detects a cyberattack targeting a dam control system, it could automatically trigger physical security measures like locking down gates or deploying autonomous systems and security personnel to prevent possible concurrent physical attacks. This includes real-time monitoring of physical security systems like cameras and sensors, with the ability to trigger automated responses to cyberattacks that might manifest physically. This obviously calls for more cooperation and innovation in those critical sectors.

Some issues might be part of the solution

Technologies developed to carry hostile actions can also used very effectively to protect against those attacks.

Quantum technologies are also studied to know how to secure tomorrow's communication. Companies such as the French THALES, elaborate new encryption methods that could resist both traditional and quantum-based attacks. The challenge to the development of this new field will be the gap created by the implementation of the new system. Because of the time and costs involved, the risk is that critical infrastructure might be for a short time easy prey to any kind of attacks. This calls for preparedness and cooperation between sectors.



Following the same pattern, if drones are always smaller and technologically more advanced, equipped with sensors they can be used for enhanced surveillance and patrolling of critical infrastructure perimeters. For example, they could be very useful to keep nuclear power plants safe through facility inspection, monitoring radiation levels, physical security and operating in dangerous environments.

A call for Collaboration, Innovation and Resilience

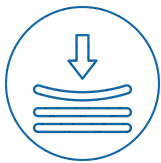
To answer all those challenges and to continue developing those new technologies, a strong collaboration between all the CIP actors is necessary. Industry, Academia and Policy Maker must align their goals as much as possible to avoid the creation of technological gap that would endanger our very interconnected societies.





These new challenges will also make emerge new actors, with new fields of expertise. It is already happening with the development of Ethical Hacking for example. Professional hackers are hired to try and attack organizations or infrastructure and thus identify their weakness. After the attack has been done, they send the result to the given organization which can then improve its resilience and security systems. Some start-ups, like Yogosha, are specialized in this field, putting hackers and firms in touch, and helping to understand and exploit the result of the hack.




These initiatives are what will keep Critical Infrastructure safe, being always one step ahead. Hence, innovators must be encouraged and supported by the sector.



In the end, building resilience is the last, but maybe the most important, challenge. This involves incorporating redundancy within systems, establishing rapid response protocols, and developing disaster recovery plans. The goal is to ensure critical infrastructure can bounce back quickly from disruptions with minimal downtime.

In a nutshell, the brightness of the future of technologies of the CIP sectors depend on its preparedness, its resilience and its capability to adapt itself. The sector faces a very ambivalent challenge: each technology can be considered as a weakness and as a strength depending on its use. This underlines the need to educate not only the security practitioners but also all people working in critical infrastructure and the need for a prepared and strong community, able to discuss and anticipate the challenges to come.

Eugénie Descour
European Organisation for Security

 <https://www.eucip.eu/>
 [@EUCIP_HorizonEu](https://twitter.com/EUCIP_HorizonEu)
 [@EU-CIP Project](https://www.linkedin.com/company/eucip-project)

