cyberwatching.eu
The European watch on cybersecurity & privacy

Effective protection on Critical Infrastructures against cyber threats

Insights and recommendations from research and innovations projects & entities

2021

Acknowledgements

Cyberwatching.eu is grateful to the projects and individual experts that have contributed to the series of webinars of the project clusters on the topic of critical infrastructures and to the recommendations provided in this document. More details and contact details can be found in section 5.

Contents

List of Figures

1 Introduction

The critical infrastructures nowadays rely on advanced technologies and robust ICT components for efficiently managing the large amounts of data that are necessary for the daily operations, communications, and in general, to provide different kinds of services depending on the specific sector of their activity such as energy, water, health, finance, transportation, among many others.

The high use of technologies combined with the use of smart devices and different types of software and hardware makes critical infrastructures a vulnerable target to every day more sophisticated attacks coming from hackers and cybercriminals. During September 2020, fourteen attacks were reported by the Centre for Strategic & International Studies (CSIS)[1] and all of them targeted critical infrastructures not only from the European Member States but around the world (e.g. a ransomware attack on a German hospital which may have led to the death of a patient; the French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks; and two sets of cyberattacks targeting emails of several members and employees of the Norwegian parliament and public employees in the Hedmark region).

Fortunately, the European Commission understands the importance of effectively protecting these infrastructures, providing essential services to citizens, hence their investment in innovative systems contributing to tackling this situation.

In response, Cyberwatching.eu organised its 15th webinar entitled "Effective protection of Critical Infrastructures against the cyber threat"[2], which has been one of its largest yet, gathering over 140 live attendees out of 230 registered participants from 18 countries around the globe. As a remit, in this report, three (3) research and innovation (R&I) projects CyberSANE[3], CYBERWISER.eu[4] and ReACT[5], and the European Cyber Security Organisation (ECSO)[6], collaborated with Cyberwatching.eu to provide a consolidated overview of the most significant barriers and recommendations in the area of cybersecurity and privacy concerning critical infrastructures with advanced systems for timely detection, monitoring, handling and treating different risks and attacks.

[1] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
[2] https://cyberwatching.eu/effective-protection-critical-infrastructures-against-cyber-threats
[3] https://cyberwatching.eu/projects/1690/cybersane
[4] https://cyberwatching.eu/projects/963/cyberwisereu
[5] https://cyberwatching.eu/projects/1053/react
[6] https://ecs-org.eu/

2 Towards a trustworthy and resilient digital Europe

Critical infrastructure is a long-standing priority in Europe and globally.

Critical infrastructure describes the physical and cyber systems and assets which are essential to maintain vital societal functions. This term has expanded over the years, originally from the transportation infrastructure to utilities, to include healthcare, energy and various manufacturers.

With this, the threat landscape for critical infrastructure organisation continues to grow more precarious with more and more high-profile attacks taking place. This is also evolving as the way we work changes, as well as with the number of connected devices in many critical infrastructure environments increasing. This has been exacerbated with the Covid-19 pandemic with many of the workforces connecting remotely. This is also changing the definition of critical infrastructures, with making our personal protective equipment for instance included in this arena, and also the importance of supply chains as well with disruption during the pandemic potentially cutting its traffic.

2.1 Cybersecurity challenges that critical infrastructures are facing

2.1.1 Market and geopolitical environment

The global cybersecurity market is a fast-growing market with an estimated growth rate of €115 billion per market growth rate of more than 13% by 2022, based on the ECSO 2018 market analysis.

Europe is a market that is highly dominated by global suppliers from North America ((40%, as shown in Figure 1), also in Asia, such as China, Japan, etc., as most of the IT hardware and software products are built outside the European Union (often by European companies).

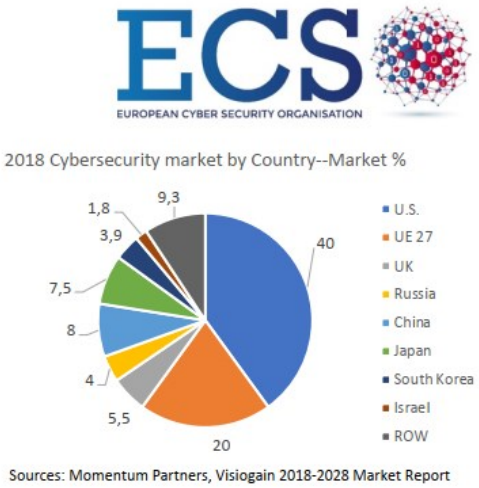

Figure 1. ECSO 2018 Cybersecurity market analysis by country

One of the challenges is an important consideration of **how the IT hardware and software products that are built outside Europe are integrated.** This is because the non-EU products are integrated with the critical infrastructure in the European supply chain.

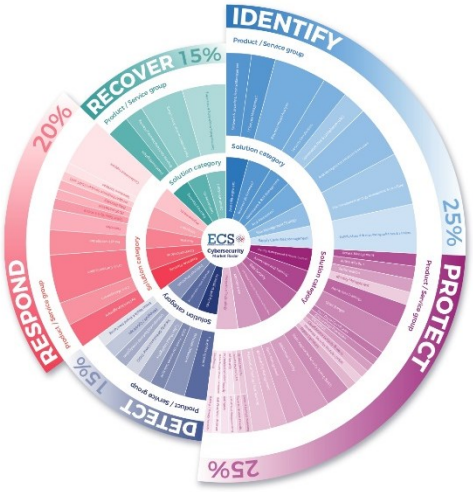

Figure 2. The Taxonomy of the ECSO Cybersecurity Market Radar

Based on the ECSO Market Radar (see Figure 2), the **European market** is quite large with €25 billion, made up of about 12,000 supplier companies (74% of them are Micro and SMEs).

In another analysis done by the ECSO Working Groups, in Europe there are innovative solutions produced by SMEs and different companies, but **Europe still has a fragmented market**.

At the same time, there is a growing appetite in Europe for more digital sovereignty and strategic autonomy. (in particular after COVID). Achieving strategic autonomy in a global and harmonised way in Europe might be challenging considering that all Member States do not have the same level of technological maturity and some rely heavily on products and solutions coming from third country.

Given this complex scenario, different aspects need to be considered which are at stake, such as

1. Citizen privacy
2. Society
3. European values
4. Democracy
5. Awareness
6. National security sovereignty.

In terms of the economy, there is a need to have a clear economic recovery and digital autonomy to ensure that there is competitiveness in Europe. Finally, the increasing crime in Europe is mentioned in a press release[13] published by the European Union Agency for Cybersecurity (ENISA)[14] in October 2020, identifying and evaluating the top cyber threats in Europe with an increase in phishing, identity theft, ransomware and monetisation as the top motivations for cybercriminals, and the COVID-19 environment has increased the fuelling of attacks on homes, businesses, governments and critical infrastructure.

2.1.2 The new challenges and objectives in Europe

2.1.2.1 Digital transformation

There is continuous evolution in cybersecurity. Digital transformation[17] is the integration of digital technology into all areas of a business, fundamentally changing how a company operates and delivers value to its customers. It is also a cultural change that requires organisations to continually challenge the status quo, experiment, and become comfortable with failure.

In particular, at the end of 2019, ECSO considered **digital transformation as one of the main issues**

[13] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020
[14] https://www.enisa.europa.eu/
[17] https://enterprisersproject.com/what-is-digital-transformation

in cybersecurity. Digital transformation has made an impact both on society, not only on the economy but also on the infrastructure and how it operates, and for the democratic process here in Europe.

In February 2020, the European Commission published its digital strategy "A Europe fit for the digital age"[18]. The EU's digital strategy defines an ambitious approach towards digital technological development, as well as how technology will be used to meet the climate-neutrality objectives. It also shows the different aspects that should be taken into consideration, such as the European industrial strategy link to the data strategy of SMEs and all the different technologies that will be key such as artificial intelligence (AI), cybersecurity, high performance computing (HPC) and connectivity (refer to Figure 3).

Figure 3. Screenshot from the European Commission's priorities for "A Europe fit for the digital age"

2.1.2.2 Green Deal

In December 2019, the European Green Deal (EGD)[21] set out Europe's new growth strategy that will transform the Union into a modern, resource-efficient and competitive economy. Its ambition is to overhaul many of Europe's economic sectors, most notably energy, transport, agriculture, goods production and consumption, and the housing stock. This initiative has an impact in looking for research, technology and industrial deployment of the cybersecurity solutions that are more energy featured.

2.1.2.3 Next Generation EU

In July 2020, the European Commission, the European Parliament and EU leaders agreed on a recovery plan that will help the EU emerge from the crisis and lay the foundations for a more modern and sustainable Europe. This initiative is known as "Next Generation EU (NGEU)[23]" and is

[18] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
[21] https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
[23] https://ec.europa.eu/info/strategy/recovery-plan-europe_it

unprecedented as for the first time in its history, it will offer support in repairing the economic and social damage caused by the coronavirus pandemic.

The Covid-19 pandemic is a ferocious event that surprised everyone, involving simultaneous disruptions to both supply and demand not only in Europe but also in an interconnected world economy. With this, there is a need for digital transformation to ensure that a resilient infrastructure in Europe has been accelerated even more by the Covid-19 situation.

While this is the case, the attack surface in terms of cybersecurity has changed as there are several workforces connected remotely, and at the same time have integrated new technologies that are brand new possible threat and vulnerability to look at.

2.1.3 Some challenges ahead

2.1.3.1 Cyber resilient digital infrastructures

Complex scenario	Some challenges ahead
● High-availability and controlled performances in highly complex/heterogeneous technologies (HW/SW, real/virtual) ● Presence of legacy systems/components and need to ensure security and privacy over mixed legacy and innovative technologies ● Complex digital infrastructures lifecycle management process across all stakeholders (supply chain w/o central authority) ● Heterogeneous regulatory scenario	● Real-time & situational awareness, automating mitigation / detection / response / recover ● Securing the whole digital infrastructure lifecycle, including training, education and safety aspects ● Innovation based on the integration of existing security/privacy components in legacy systems ● Distributed decision making and collaboration solutions, e.g., orchestration services. ● Secure virtualization technologies that are transversal to verticals

2.1.3.2 Deploying resilient digital infrastructures in the field

Complex scenario	Some challenges ahead
● Complex and cross-platform cyber-attacks / threat management ● Integrity and trustworthiness of communications and services ● Virtualization and softwarisation of networks and network functions and the interconnection of different technologies ● Complex trust models to address M2M interaction and to manage complex 5G infrastructures ● Impact of current cryptographic schemes	● Increase trust in information sharing mechanisms through control and formal analysis of data and sensors ● Design and implementation of new security mechanisms and automation of attack response mechanisms ● Realistic, open-source and configurable tools and simulators to evaluate new security solutions

and migration to quantum-safe ones	

3 The Recommendations for the Critical Infrastructure Domains

The Cyberwatching.eu webinar focused on how better cybersecurity is essential for protecting critical infrastructures and making them more resilient. In this webinar, several recommendations were provided by the four speakers with an overview of what the cybersecurity challenges are in critical infrastructures, and some answers in how team-leading experts in Europe are collaborating, thanks to funding from the European Commission (EC) to ensure that Europe's critical infrastructures remain resilient to cyberattacks.

3.1 The European Cyber Security Organisation

The European Cyber Security Organisation (ECSO) is a fully self-financed non-for-profit organisation under Belgian law, established in June 2016. ECSO is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP)[25] on cybersecurity.

The partnership aims to foster cooperation between public and private actors at early stages of the research and innovation (R&I) process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right to privacy and data protection.

Here are some of the important points on the timeline of the European approach to cybersecurity with an upcoming new strategy:

- 2009: EU stakeholders started to advocate for a specific “ICT security” approach on EU R&D
- 2011: Started the discussion with the EC about a possible Public Private cooperation
- 2013: First EU cybersecurity strategy (“building blocks”)
- **2016: Signature of the cPPP between the EC and ECSO**
- 2017: Update of the EU cybersecurity strategy
- 2018: Adoption GDPR and NIS Directive
- 2019: Adoption of Cybersecurity Act (new ENISA mandate, EU certification)
- 2020: Discussion on the next MFF (2021-2027). Recovery plan for the “new normal” after the COVID crisis. New EU Cybersecurity Strategy and revision of the NIS Directive (December)
- 2021: European Cybersecurity Centre / Creation of national Cybersecurity Centres; Horizon Europe - Digital Europe Programme; Starting discussions on Digital Service Act and European secure ID
- **2021: ECSO continues to support the growth of the European Cybersecurity ecosystem & Community**

During 2019, ECSO had an adoption from the Cybersecurity Act[27] with the new mandate for ENISA. Also, in Dec 2020, the proposal for a revised NIS directive[28] was presented. There was also a

[25] https://www.ecs-org.eu/documents/uploads/cppp-contract.pdf
[27] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[28] https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

discussion about the next multiannual financial framework (MFF)[29] (2021-2027) and strategies that are linked to the new EU Cybersecurity strategy that was applied, as well as the recovery plan for the "new normal" after the COVID crisis.

ECSO has six working groups (WGs), see Figure 5. During this webinar, the focus of the discussion is on WG6, which is linked to the Strategic Research & Innovation Agenda (SRIA) and cyber technologies. WG6 is collaborating with the entire ecosystem within ECSO, as the team looks at all possible issues linked to industrial policy, in the sense that when they look at the cybersecurity in Europe, they cannot only consider the research and innovation aspect but also the industrial policy, and the need to implement it. In particular, when they see the growing interest with respect to standardisation and certification, this is the key to guaranteeing that there are trustworthy solutions integrated into the critical infrastructure and ensuring that it is continuously measured.

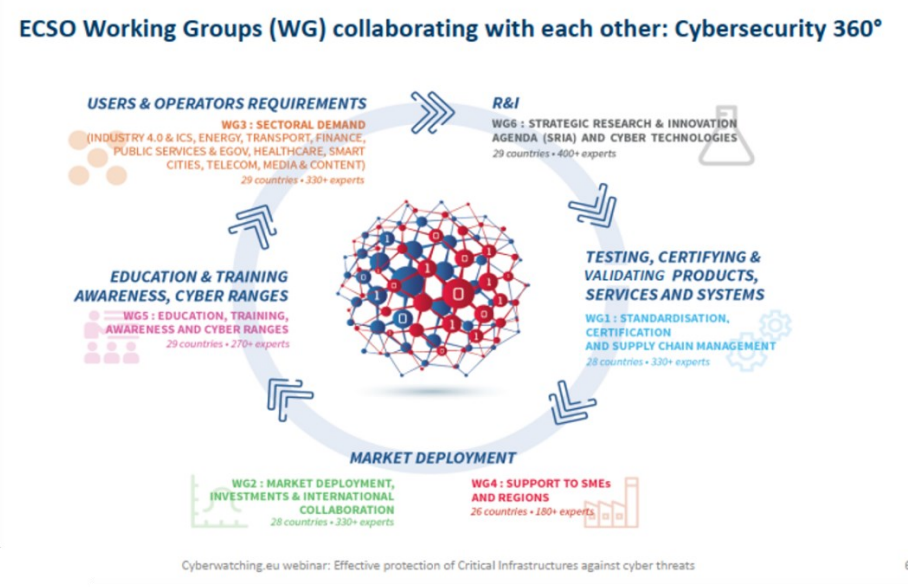

Figure 4. ECSO Working Groups

Main ECSO recommendations to the European Commission and Digital Europe Programme for a Cyber Resilient Europe

ECSO sent the recommendations to the European Institutions including the Commission and the Parliament because it is important to strengthen the cyber resilience in Europe in all different aspects.

- Support and protection of the European digital transformation – there is a need to support and have a long term EU vision for a European cybersecurity ecosystem based on EU values. **Having a comprehensive EU cybersecurity strategy accompanied by the implementation of a cybersecurity industrial policy is essential. It is important to envisage such a strategy in a holistic approach encompassing not only R&I requirements but also considering, certification/standardisation, investments, procurement, application domain specificities, support to SMEs and fostering their collaboration with regional and local authorities, education, training, skills and awareness among other things.**

[29] https://ec.europa.eu/info/strategy/eu-budget/long-term-eu-budget/eu-budget-2021-2027_en

- The recovery of our digital sovereignty and increase of our strategic autonomy should be accompanied by socio-economic development and a strengthen and sustainable next-generation public-private cooperation. Also, a clear support from EU legislations and policies, as well as public-private investments in capability development and capacity deployment are the angular stones of having trusted supply chains in Europe.

The aforementioned WG6 of ECSO is tasked to looking into new cybersecurity technological challenges, identify European R&I priorities and propose a roadmap to strengthen and build a resilient EU ecosystem, analysing the challenges of digitalisation of the society and industrial sectors to sustain EU digital autonomy by **developing and fostering trusted technologies.**

- **European R&I priorities**. ECSO has provided some scenarios and suggested priorities to the European Commission with respect to Horizon Europe and the Digital Europe Programme (ECSO 2021-2027 technology vision of the future shaping society and industry).

- **Trans continuum (link across techno sectors with other PPPs).** A joint initiative with other cPPPs in Europe (ETH4HPC, 5G, IA, BDVA, etc.) by looking at the digital contingent, in the sense that nowadays there are emerging technologies such as IoT, AI, Blockchain, HPC and 5G that are pushing towards digital transformation, and are sensitive elements that are integrated into the critical infrastructures to identify global challenges and need to address them in a transversal and coordinated way.

- **Collaboration**. Coordination with other PPPs, Jus, Pilot Project on the establishment of a European Cybersecurity Competence Centres, EC projects and other initiatives to monitor the evolution of the cybersecurity ecosystem and understand the gaps. ECSO has signed several Memorandum of Understandings with European bodies including ETSI, CEN/CENELEC, and other PPPs. ECSO is regularly cooperating with several European Agencies including among others ENISA, JRC, and the EDA on cybersecurity for dual-use technologies.

3.2 The Horizon2020 projects

3.2.1 CyberSANE: Cyber Security Incident Handling, Warning and Response System for European Critical Infrastructures

Over the past decade, critical information infrastructures (CIIs) were operating upon robust and reliable ICT components, complex ICT infrastructures and emerging technologies which are interconnected through complex networks, providing a high level of flexibility, scalability, and efficiency in the provided services and the supported processes. However, the increased usage of information technology in modern CIIs means that they are becoming more vulnerable to the activities of all kinds of malicious entities and individuals (e.g., hackers, terrorist groups, criminal gangs).

The above landscape puts the CIIs' operators under pressure to detect ongoing attacks and to combine and analyse all the threats-related information and evidence effectively and accurately. However, the lack of appropriate tools to anticipate and handle complex cyberattacks in a way that takes into account the heterogeneity and complexity of their environments has raised the need for

improved monitoring approaches.

CyberSANE aims to contribute towards the emerging need to improve the level of prevention, preparedness, reaction and resilience to cyber incidents and threats of the CIIs. In order to meet its objective CyberSANE will introduce an innovative, incident handling and response system which will support the security officers and operators, guiding them to recognise, identify, model, dynamically analyse, forecast, treat and respond to advanced persistent threats and handling daily cyber incidents utilising and combining both structured data (e.g., logs and network traffic) and unstructured data (e.g. data coming from social networks and the dark web).

Recommendations on cybersecurity priorities for the critical infrastructure domain

The critical information infrastructures should incorporate:

- Security monitoring and analysis capabilities for preventing and detecting any kinds of anomalies, threats, risks.
- Social information mining capabilities to extract data from distributed online web sources offering to the security operators' information on activities and situations that can become a threat to the infrastructures.
- Data fusion and event management capabilities to provide the intelligence needed for an effective and efficient analysis of a security event.
- Risk evaluation capabilities to thoroughly assess the vulnerabilities of their interconnected cyber assets and to continuously estimate the probability of all possible cyber-attacks.
- Threat intelligence capabilities to facilitate and promote the secure and privacy-aware sharing of incident-related information.

3.2.2 CYBERWISER.eu: Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training

The COVID-19 pandemic has changed the way many businesses operate, compelling them to find different solutions, shifting working environments and amplifying a lot of the challenges organisations were already facing.

As organizations around the world struggle to adapt to a strictly remote workforce, cyber-criminals have intensified their attempts at gaining access to sensitive and valuable data by using different techniques such as social engineering techniques, malware, phishing etc..

This context has been driving a rapidly growing need for well-trained cybersecurity professionals. Yet supply is not meeting the demand for skilled professionals in this field. This reflects a shortage of cybersecurity professionals worldwide which is expected to grow to 3.5 million in 2021.

While the provision of training and educational courses is increasing, it is not sufficiently available to fill entry-level cybersecurity vacancies in the market, both in terms of non-technical preparation and technical training for specialist cybersecurity positions. On top of this, IT teams are overwhelmed by the sheer number of threats and issues they have to deal with on a daily basis.

This is where CYBERWISER.eu comes into play.

CYBERWISER.eu delivers a flexible, risk-centred, capacity-building platform, combining a theoretical and practical approach to cybersecurity with innovative features including a cutting-edge cyber range. CYBERWISER.eu implements customisable training pathways in cybersecurity to fit a broad range of needs and capacity building targets, from juniors like threat and vulnerability analysts all the way up to information security risk managers and CISOs.

The CYBERWISER.eu Platform has been validated by three full-scale pilots covering three different domains (FSP#1 higher education, FSP2# transport and FSP#3 energy) who have used it to increase their students' or employees' skills on specific topics such as SQL injection, cross-site scripting, phishing, session hijacking etc..

CYBERWISER.eu is also offering the opportunity to test the platform for free to SMEs, research and Academia, large companies and any interested organisation who can apply to join the Open Pilot Stream[33] and start a dedicated training path.

Recommendations on cybersecurity priorities for the critical infrastructure domain

From a training perspective, the critical infrastructure sector could benefit from being able to:

- Simulate a complete corporate environment with real-world attacks/threats. The staff of critical infrastructure should have the opportunity to play both attacker and defender roles in order to better understand how vulnerabilities can be exploited and how to handle cyber-attacks and defence in real life.
- Train both technical and non-technical staff as people at all levels contribute to the risk and protection of an organization's cybersecurity practice. Organisations should consider a systematic delivery of awareness training programs as well as further development and practical training for staff in cybersecurity specialist roles.
- Easily access secure online tools for training and upskilling their employees. In accordance with most of the global and European bodies, this sector's experts are recommended to move away from the traditional training methods to those of the more tailored and practical ones.

In particular, ENISA called for greater use in cyber-ranges[35], such as the one embedded in the CYBERWISER.eu platform. Also, the ECSO report on 'Gaps in European Cyber Education and Professional Training'[36] states that training needs to move to more innovative forms such as a flipped classroom style and the greater usage of online tools.

3.2.3 ReACT: REactively Defending against Advanced Cybersecurity Threats

The presentation of ReACT started by placing the cybersecurity problem in context:

[33] https://www.cyberwiser.eu/open-pilot-stream
[35] https://www.enisa.europa.eu/news/enisa-news/stocktaking-of-information-security-training-needs-in-critical-sectors
[36] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

Is it a new problem? If not, why hasn't it been solved?

We argued that cybersecurity is an old problem, but since the Internet/ARPANET was accessible only to a small community (at least during its first couple of decades) cybersecurity was not a major problem. On the contrary, when the wider public started accessing the Internet in the mid/late '90s, then cybersecurity became a major problem and a significant concern. Unfortunately, by that time, it was too late to change some of the design decisions which were already embedded deep into the implementation of the network.

Next, the presentation explained the changing nature of computers. Indeed, although the traditional view of a computer is a device that has a screen, a keyboard, and a mouse, recently computers have started to fully transform themselves by becoming embedded in all sorts of devices: smart appliances, smart cars, medical equipment, etc.. Attacking these new kinds of computers/devices may have a devastating impact on human lives: medical equipment not working, faulty home appliances, dangerous cars, etc..

Finally, the talk focused on how the ReACT project proposes to deal with the cybersecurity problems: the approach of ReACT to cybersecurity involves a completely new mindset. ReACT argues that instead of rushing to protect computers (without really knowing what is their weakest spot), first try to make computers fail (crash), and then try to protect them by fixing the failures which were just found. ReACT argues that by trying to make computers fail, their weakest points can effectively be uncovered, which can then be protected from future cyberattacks. Using semi-automated fuzzing combined with manual inspection, ReACT partners have already discovered several vulnerabilities in popular software and hardware systems and have catalysed the distribution of security patches and updates for them.

Recommendations on cybersecurity priorities for the critical infrastructure domain

- Look at the security infrastructure with the eyes of a cyber attacker to find the weakness to break into the infrastructure. Only then will it be possible to discover the weakest points and only then will it be possible to secure them.
- Try to make computers crash before taking steps to protect them: if the result is to successfully crash the computer, then at least one weak point has been found.
- Before solving a problem ask "why has this problem not been solved yet?" This can reveal all the areas where previous attempts have failed and where new attempts may have an opportunity to succeed.

4 Conclusion

Cyberwatching.eu's webinar focussed on how better cybersecurity is essential in having effective protection of critical infrastructures against cyber threats and making them more resilient, in collaboration with the the European Cyber Security Organisation (ECSO), and the EC-funded projects CyberSANE, CYBERWISER.eu and ReACT.

The main recommendations from this document are detailed below:

- **Cybersecurity needs to be considered in 360° aspects**. It is a continuous process to ensure the security of the new technologies that are being integrated into critical infrastructure, which bring new vulnerabilities and changing attacks.
- Do not forget that not only are systems designed and maintained, but also the **skills**, which are an important factor, playing an important role also for the critical infrastructure when they operate in the field.
- **More efforts need to be applied to develop more advanced systems** that will rely on advanced technologies such as artificial intelligence (AI) and machine learning techniques to provide more advanced functionalities and be shared with the operators in order to deal with such threats.
- **Human aspects are also important, and training is fundamental**. Cybersecurity is not a destination, it is a journey, so it is key to keep up to date to cope with the fast-evolving threat landscape.
- Break things first and try to fix them later, and try to make the system fail in order to try to protect it.

5 Contributing projects and entities

The projects contributing to this document are the following:

Website: https://www.cybersane-project.eu/
Grant agreement number: 833683
Duration: 1 September 2019 – 31 August 2022
Contributor: Dr. Spyros Papastergiou[37], Senior Research Consultant at Maggioli

Website: https://www.cyberwiser.eu/
Grant agreement number: 786668
Duration: 1 September 2018 – 28 February 2021
Contributor: Niccolò Zazzeri[38], Communication & Web Marketing Specialist at Trust-IT Services

Website: https://react-h2020.eu/
Grant agreement number: 786669
Duration: 1 June 2018 – 31 May 2021
Contributor: Evangelos Markatos[39], founding head of the Distributed Computing Systems Lab at FORTH-ICS

Special thanks to the European Commission's partner in implementing public-private partnership on Cybersecurity.

Website: https://ecs-org.eu/
Contributor: Roberto Cascella[40], Senior Policy Officer at ECSO

[37] https://cyberwatching.eu/spyros-papastergiou
[38] https://cyberwatching.eu/niccolo-zazzeri
[39] https://cyberwatching.eu/evangelos-markatos
[40] https://cyberwatching.eu/roberto-cascella

Watch the recorded webinar video now!

You may also download the speakers' presentations on the webinar page.

How to reach us?

cyberwatching.eu
The European watch on cybersecurity & privacy

www.cyberwatching.eu

@cyberwatchingeu

in.com/company/cyberwatchingeu

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

University of Oxford

ICT Legal Consulting
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.