



# ENERGY SHIELD

## Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

### WP8 EXPLOITATION & SCALE UP

### D8.6 STANDARDIZATION REPORT

#### Document info

Contractual delivery	30/06/202
Actual delivery	30/06/202
Responsible Beneficiary	SIMAVI
Contributing beneficiaries	ALL
Version	1.0



This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907



## DOCUMENT INFO

<b>Document ID:</b>	<b>D8.6</b>
<b>Version date:</b>	30/06/2022
<b>Total number of pages:</b>	48
<b>Abstract:</b>	This task will focus on promoting EnergyShield results in standardization groups at both European level (CEN/ CENELEC/ETSI) and ISO/IEC level. Various vehicles might be considered such as CWA (CEN Workshop Agreement), TR (Technical Report) or TS (Technical Specification). The most relevant format will be selected so that EnergyShield findings can be disseminated to the EPES sector
<b>Keywords</b>	Standardisation, policy, workshop,

## AUTHORS

<b>Name</b>	<b>Organisation</b>	<b>Role</b>
<b>Otilia Bularca</b>	SIMAVI	Overall Editor/
<b>Ana-Maria Dumitrescu</b>	SIMAVI	Contributor
<b>Matthias Rohr</b>	PSI	Contributor
<b>Anna Georgiadou</b>	NTUA	Contributor

## REVIEWERS

<b>Name</b>	<b>Organisation</b>	<b>Role</b>
<b>Yasen Todorov</b>	CEZ	Overall Reviewer
<b>Magda Zafeiropoulou</b>	SC	QA Reviewer

## VERSION HISTORY

<b>V0.1</b>	10/04/2022	Table of content
<b>V0.2</b>	12/05/2022	Release of 2nd draft
<b>V0.3</b>	12/06/2022	Feedback & contributions from partners
<b>V0.4</b>	20/06/2022	Version ready for internal review
<b>V1.0</b>	30/06/202	Final version, released to the EC

## EXECUTIVE SUMMARY

The current report presents the efforts done by the EnergyShield Consortium to promote the results of EnergyShield project to standardisation and policy bodies. The groups targeted are at both European level (CEN/CENELEC/ETSI) and ISO/IEC level.

Standardization is identified in Horizon 2020 as one of the innovation-support measures. Standardization can help bridge the gap between research and the market, by enabling the fast and easy transfer of research results to the European and international market. Starting from this assumption, EnergyShield consortium followed a five steps conceptual pathway to identify the most suitable ways to contribute to standardization and policies related to cybersecurity and EPES: a) brief, b) act, c) show, d) liaise, d) publish.

Having in mind this approach throughout all the 36 months of implementation, partners have contributed to promoting the results and adapting based on the external factors (market changes and online migration due to COVID-19)

This report is public and will be disseminated to EPES stakeholders.

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
List of figures .....	6
List of tables .....	7
Acronyms .....	8
1. Introduction .....	9
1.1. Scope and objectives .....	9
1.2. Structure of the report .....	9
1.3. Task dependencies .....	9
2. EU cybersecurity- from R&I to standardisation .....	10
2.1. EU cybersecurity Policy .....	11
2.1.1. EU Cybersecurity Act.....	11
2.1.2. Cybersecurity Strategy .....	11
2.2. EU cybersecurity legislation .....	12
2.2.1. General Data Protection Regulation (GDPR).....	13
2.2.2. Network and Information Security Directive (NISD) .....	14
2.2.3. EU Cyber defense policy framework .....	15
2.2.4. Cybersecurity Act .....	15
2.3. Emerging EU cybersecurity regulation .....	16
2.3.1. Security Union Strategy 2020-2025 .....	16
2.3.2. NIS2 .....	16
2.3.3. EU RCE directive .....	17
2.3.4. DORA regulation .....	17
2.4. EU cybersecurity Standardization bodies .....	18
2.5. EU cyber-ecosystem.....	21
3. Energyshield project touchpoints .....	23
3.1. Standards & policy paths .....	23
3.1.1. Coding standards .....	24
3.1.2. Security and privacy .....	27
3.2. Awareness raising & communication paths .....	28
3.2.1. Energyshield policy workshop .....	28
3.2.2. Clustering & Collaborating .....	39
3.2.3. Scientific publications .....	39

3.2.4. Whitepapers Publication .....	40
4. Conclusion .....	43
References.....	44

## LIST OF FIGURES

Figure 1. EU Cybersecurity governance and decision-making [ECA22] .....	10
Figure 2. ENISA's general concept general concept for the role of standards in the evaluation and certification process .....	11
Figure 3. Objectives of the Cybersecurity strategies (2013 vs 2020) [JOI13],[JOI20] .....	12
Figure 4. Complementary aspects of GDPR and NIDS [ECA22] .....	15
Figure 5. Representation of the Digital Operational Resilience Act, available at <a href="https://www.pacemakers.io/dora-1">https://www.pacemakers.io/dora-1</a> .....	18
Figure 6. Main standardisation bodies at EU level .....	20
Figure 7. Proposed pathway to reach standardization and policy bodies .....	23
Figure 8. EnergyShield policy workshop agenda and speakers .....	30
Figure 9. Dashboard of Energy Shield project in OpenAIRE .....	40

## LIST OF TABLES

Table 1. Whitepaper template sections and guidelines .....	40
Table 2. List of published whitepapers .....	41

## ACRONYMS

ACRONYM	DESCRIPTION
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT	Registered in the U.S Patent and Trademark Office by Carnegie Mellon University
CNI	Critical National Infrastructure
CSIRTs	Computer Security Incidents Response Teams
CSDP	Common Security and Defence Policy
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CWA	CEN Workshop Agreement
CVSS	Common Vulnerability Scoring System
DORA	Digital Operational Resilience Act
DISA STIG	DISA — (Defense Information Systems Agency) that provides technical guides (STIG — Security Technical Implementation Guide).
EU	European Union
EUIBA	European Union Institutions, Bodies and Agencies
EN	European Standard
ENISA	European Union Agency for Cybersecurity
EPES	Electrical Power and Energy Systems
ETSI	European Telecommunications Standards Institute
ESO	European Standards Organization
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ICT	Information and communications technology
NVD	National Vulnerability Database
Ofgem	Office of Gas and Electricity Markets
OWASP	Open Web Application Security Project
RCE	Resilience of Critical Entities
PSD2	Second Payments Services Directive



## 1. INTRODUCTION

### 1.1. SCOPE AND OBJECTIVES

The current report presents the efforts done by the EnergyShield Consortium to promote the results of EnergyShield project to standardisation and policy bodies. The groups targeted are at both at European level (CEN/CENELEC/ETSI) and ISO/IEC level.

### 1.2. STRUCTURE OF THE REPORT

The report is structured on two main parts: the first one briefing the EU cybersecurity ecosystem together with its standard and policy frameworks, while the second one focuses on the concrete steps taken by consortium partners to promote the results of EnergyShield project.

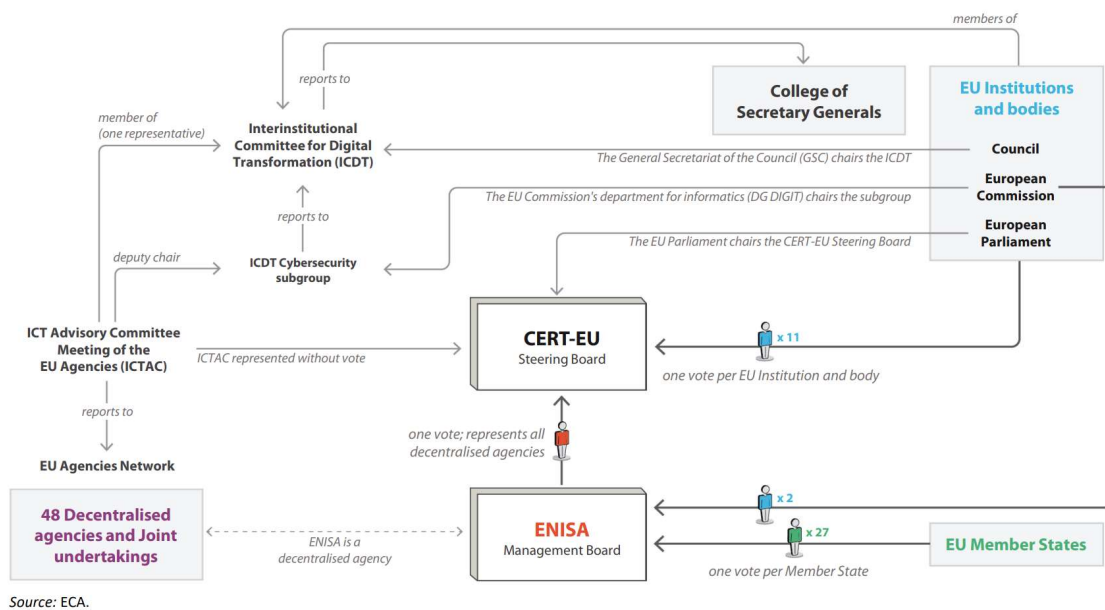
### 1.3. TASK DEPENDENCIES

This document builds upon a series of documents released in the first year of the project implementation: technical requirements [ESH11], commercial requirements [ESH12], regulatory requirements [ESH13], ethics requirements [ESH10], system architecture [ESH14] and data management [ESH93] and is closely related to some ones like the collaboration report [ESH78].

## 2. EU CYBERSECURITY- FROM R&I TO STANDARDISATION

Standardization is identified in Horizon 2020 as one of the innovation-support measures. Standardization can help bridge the gap between research and the market, by enabling the fast and easy transfer of research results to the European and international market.

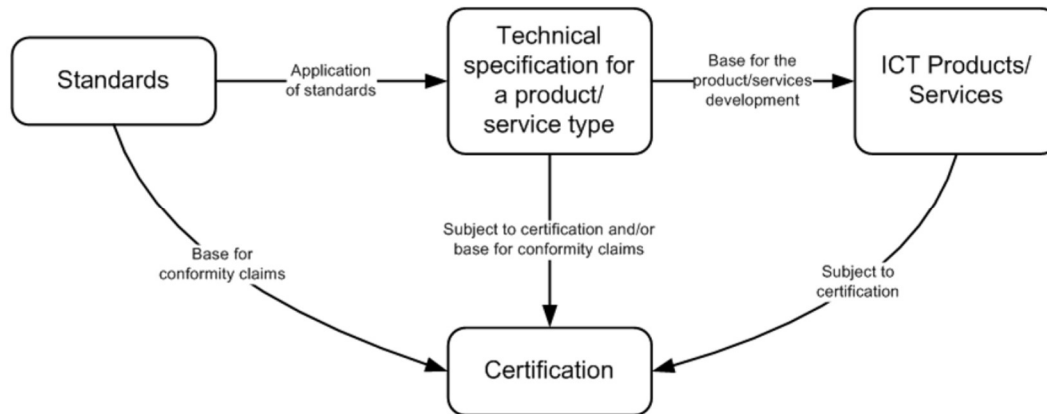
The history of the European cybersecurity network begins with adopting the Budapest Convention on Cyber Crime in 2001 [COE01], the Common Framework on Electronic Communications Networks and services in 2002 [ECD02], and subsequent establishing of European Network and Information Security Agency (ENISA), an independent EU Agency for cybersecurity, by Regulation (EC) No. 460/2004 of the European Parliament and of the Council in 2004 [ECR04]. It stated the mains tasks of ENISA i.e., developing a culture of network and information security for the benefit of citizens, consumers, businesses, and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market.



Source: ECA.

**Figure 1. EU Cybersecurity governance and decision-making [ECA22]**

ENISA is a key player supporting European Union Institutions, Bodies and Agencies (EUIBA) and its activity is dedicated to achieving a high common level of cybersecurity across the EU (Figure 1). ENISA's mission is to enhance the trustworthiness of information and communications technology (ICT) products, processes, and services with cybersecurity certification schemes, to cooperate with EUIBAs and Member States, and to help them prepare against cyber threats.



**Figure 2. ENISA's general concept for the role of standards in the evaluation and certification process**

## 2.1. EU CYBERSECURITY POLICY

### 2.1.1. EU CYBERSECURITY ACT

Until May 2019 there was no EU certification framework for IT products being developed and sold. The EU Cybersecurity Act [EPC19], intends to change that by establishing a European cybersecurity certification framework for ICT products, services, and processes. Standardisation will play an important role in the new framework. ENISA takes the leadership of sole reference point for a new cybersecurity certification scheme to avoid certification scheme fragmentation within the European Union (EU). The Cybersecurity Act strengthens ENISA and establishes a cybersecurity certification framework for products and services.

ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises [ECA22]. Also, this task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive) [NIS16].

### 2.1.2. CYBERSECURITY STRATEGY

The building block of EU's policy is represented by the Cybersecurity Strategy [JOI13] and cuts across internal policy areas, like justice and home affairs, digital single market and research policies while aiming at making EU's digital environment the safest in the world.

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy [JOI20].

Figure 3 shows the objectives of the Cybersecurity strategies (2013 vs 2020 version). Technological advancement has called for major updates in the EU cybersecurity strategy, the latest strategy focusing on creating a safe digital space, building operational capacity, and advancing to a global and open cyberspace.



**Figure 3. Objectives of the Cybersecurity strategies (2013 vs 2020) [JOI13],[JOI20]**

## 2.2. EU CYBERSECURITY LEGISLATION

Since 2002 legislation with varying degrees of relevance to cybersecurity has been adopted.

In December 2015, the EU legislation issued two pieces of legislation that will have a profound impact on all industry sectors. The General Data Protection Regulation (GDPR) represents a profound reform of data protection law in Europe, shifting the balance of power towards the citizen to whom the personal data belongs, away from organisations that collect, analyse, and use such data.

The change in international conditions has also led to an evolution of the European Cybersecurity legislation. After several legislative pieces targeting specific cybercrime issues, such as payment frauds and electronic communication systems, The Directive on Security of Network, and Information Systems across the EU (the NIS Directive) from 2016 is an example of general EU-wide legislative piece focusing on cybersecurity. The Network and Information Security Directive (NISD) can be regarded as a complementary law to GDPR, designed to create a focus on the protection of IT systems in European critical national infrastructure (CNI) such as the energy, transport, banking, and healthcare sectors.

Both GDPR and NISD came into force in 2016 but there will be a period of up to 2 years during which organisations will be allowed to prepare for the new regulations and for the directive to be transposed into country law.

### 2.2.1. GENERAL DATA PROTECTION REGULATION (GDPR)

Building on the Article 94 – EU General Data Protection Regulation [**GDPR**] it establishes one set of data protection law across all 28 European states and requires organisations to demonstrate the effectiveness of their data security measures. As the scale and sophistication of attacks grow, critical infrastructures have to remain vigilant and try to put in place sufficient processes and policies to best protect their data. Dramatically increased maximum penalties for mishandling data are now 4% of global revenue or 20M Euros, whichever is greater. To illustrate the impact of this new regulation, the Talk cyberbreach of October 2015 (affecting nearly 157,000 customers) generated a fine of £400k by the UK national authority, whereas it would cost nearly €17M to the company under the new GDPR. Additionally, responsibility for protecting personal information under GDPR will extend to data processing as well as data controllers. Further changes to be introduced include:

- Data breaches must be reported as soon as possible and, where feasible, no later than 72 hours after discovery of a breach.
- Personal data now extending to location, IP address, RFID identifiers, as well as whole new swathes of medical data, including genetic information.
- The “right to be forgotten” is enshrined in law, allowing people to request of search engines to delete links to the data in question.

Regulation will apply to companies headquartered outside of Europe if they have operations in Europe.

- Organizations are required to measure the effectiveness of their security measures/controls
- New requirements to carry out Privacy Impact Assessments (PIAs) to ensure that personal data is sufficiently protected, and privacy of the individual maintained.

The replacement of the classical meters with their smart variants has advantages for both the consumer and industry. Some of the key benefits include giving consumers the information to gain control over their energy consumption, lowering the cost for managing the supply of energy across industry, and producing detailed consumption information data from these smart meters which in turn enable a wide range of services. It is expected that the meters have an update rate of every 15 minutes at least. When generating such a large amount of consumer data a lot of privacy sensitive information is being disclosed. There are various initiatives to date which stress and outline the importance of having solutions for the smart grid where privacy protecting mechanisms are already built-in by design. The energy suppliers need to forecast to buy energy generation contracts that cover their clients. Moreover, to

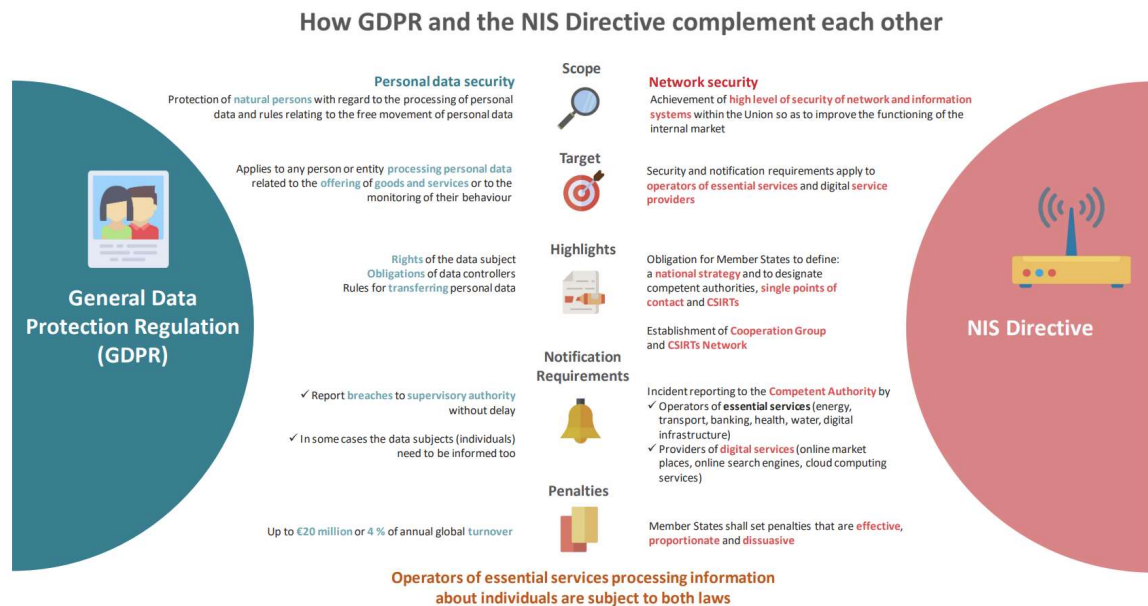
ensure network capacity the network operators require longer term forecasting. This forecasting is typically done by taking as input the (aggregated) data from several households. Based on this consumption data together with other variables such as the date and the current temperature and weather, a forecast is computed to predict the short, medium, or long-term consumption. The energy providers or network operators only need to know the desired forecast information based on their (potentially proprietary) forecasting algorithm and model. There is no need to observe the individual consumer data. To protect the consumer privacy and also to provide better service, the project will use homomorphic encryption-based algorithms to allow data smart meter data to be encrypted and passed onto a third-party cloud service where it can be securely shared for operational and business intelligence without compromising the privacy and identity of the consumers. The developed techniques will help the energy provider to comply with GDPR requirements and at the same time gather business intelligence. The developed algorithm will also allow the user to have total control of their smart meter data and how they share with their energy provider. The consumer can also search in the encrypted data to identify their energy utilisation patterns and their billing information.

### 2.2.2. NETWORK AND INFORMATION SECURITY DIRECTIVE (NISD)

NISD [NIS16] can be regarded as complementary to GDPR, designed to create a focus on the protection of IT systems in European critical national infrastructure (CNI). Member States will be required to adopt a national cyber strategy which defines objectives, policy, and regulatory measures to protect that nation. The UK has a well-established National Cyber Security Strategy. The directive also identifies that the providers of some digital services have also become part of the CNI, so providers of search engines and cloud services will also be covered by in country legislation. Other key measures that will be introduced by NISD include:

- Member States must adopt a NIS strategy and designate a national NIS competent authority with adequate financial and human resources to prevent, handle and respond to NIS risks and incidents;
- Member States and the Commission will create a cooperation mechanism among to share early warnings on risks and incidents through a secure infrastructure, cooperate and organise regular peer reviews;
- Operators of critical infrastructures must adopt risk management practices and report major security incidents on their core services.





Source: ECA.

**Figure 4. Complementary aspects of GDPR and NIDS [ECA22]**

### 2.2.3. EU CYBER DEFENSE POLICY FRAMEWORK

The EU Cyber defence policy framework, adopted in 2014 [CON14], was updated in 2018 to better correspond to the new cybersecurity challenges. Attention is paid to conflict prevention and cooperation in cyber space, as well as to the availability of information; the updated priorities list includes development of cyber defence capabilities, training and exercises, research and technology, civil-military cooperation and international cooperation. The “cyber diplomacy toolbox” from 2017 provides framework for the joint foreign policy responses to cyberattacks against the EU, with the idea to “influence the behaviour of potential aggressors in the long term” [TRE19].

### 2.2.4. CYBERSECURITY ACT

On the 11<sup>th</sup> of December, 2018, the European Parliament, the Council and the European Commission reached an agreement on the Cybersecurity Act [EPC19], which, next to establishing an EU framework for cybersecurity certification, granted ENISA additional resources, thus reaffirming ENISA role in practical support of the Member states for cyberattacks management and prevention, as well as in the area of cyber-security policy-making.

## 2.3. EMERGING EU CYBERSECURITY REGULATION

Security is one of the major concerns of citizens and the recent spate of terrorist attacks on European soil have underlined still further the need for EU action. Critical Infrastructure protection and resilience.

The daily lives of citizens rely on an ever more interconnected and interdependent physical and digital infrastructure. This infrastructure is vital for the functioning of the economy and of society. Without reliable supplies of energy, predictable transportation, comprehensive health systems or a digitally driven financial network, our current way of life would not be possible. The COVID-19 pandemic has shown it even more clearly.

### 2.3.1. SECURITY UNION STRATEGY 2020-2025

On 24 July 2020, the Commission adopted an EU Security Union Strategy 2020-2025 [COM20] to target action on priority areas where the EU can bring added value to national efforts. It builds upon progress achieved previously under the European Agenda on Security 2015-2020 [COM15] and provides a new focus, to ensure that EU security policy reflects the changing threat landscape; that it builds long-term, sustainable resilience; that it engages the EU institutions and agencies, governments, the private sector and individuals in a whole-of society approach; and that it brings together the many policy areas with a direct impact on security

### 2.3.2. NIS2

The threat landscape has changed considerably since the NIS Directive was adopted in 2016, and the scope of the directive needs updating and expanding to meet current risks and future challenges, one such challenge being to ensure that 5G technology is secure.

The pandemic has more than confirmed the importance of preparing the EU for the digital decade as well as the need to continually improve cyber-resilience, particularly for those who operate essential services such as healthcare and energy

As a result of the review process, the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was presented by the Commission on 16 December 2020 [NIS20].

During the autumn of 2021, the European Parliament adopted a draft cybersecurity directive, the revised 'Directive on security of network and information systems' (commonly referred to as 'NIS2'). When it moved to the Council, additional changes were made; one was to extend the time for Member States to transpose it into national law from 18 months to two years.

Overall, the NIS2 proposal sets itself three general objectives:

- Increase the level of cyber-resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors



- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive
- Improve the level of joint situational awareness and the collective capability to prepare and respond [EUP21]

To ensure consistency and coherence with related EU legislation, the NIS Directive review in particular takes into account the following three Commission initiatives:

- the review of the Resilience of Critical Entities (CER) Directive, which was proposed alongside the NIS2 proposal, with the objective of improving the resilience of critical entities against physical threats in a large number of sectors.
- the initiative on a digital operational resilience act for the financial sector (DORA);
- the initiative on a network code on cybersecurity with sector-specific rules for cross border electricity flows (see snapshot analysis from the SPEAR project).

### 2.3.3. EU RCE DIRECTIVE

The RCE Directive [RCE20] is launched in parallel with the NIS2 review. As recognised in the proposal it is necessary to achieve a coherent approach between the two instruments. The proposal for a Directive on the resilience of critical entities (RCE Directive) [RCE20] expands both the scope and depth of the 2008 European Critical Infrastructure (ECI) Directive. [ECI08]

### 2.3.4. DORA REGULATION

In the last few years two major pieces of regulation have shaped the digital transformation of Financial Services. These are the Second Payments Services Directive (PSD2) [PSD15] and General Data Protection Regulation (GDPR) [GDP16].

A new wave of regulation is about to start from Brussels and will eventually reach all global markets. It's called DORA (Digital Operational Resilience Act) [DOR20]. It was presented by the EU Commission on 24 September 2020.

The European Commission has published a legislative proposal for a regulation on Digital Operational Resilience in the EU financial services sector ("DORA"). It is designed to consolidate and upgrade Information and Communications Technology (ICT) risk requirements throughout the financial sector to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations. DORA aims to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require firms to ensure that they can withstand all types of ICT-related disruptions and threats. The proposal also introduces an oversight framework for critical third-party providers, such as cloud service providers.

DORA is a proposal for Regulation of digital operational resilience for the financial sector that aims to harmonize how ICT risks are regulated in the EU financial services ecosystem. This regulation is not yet active, but we can expect it to go live in some form after 2023.

## Digital Operational Resilience Act

Four Strategic Objectives of the European Central Bank

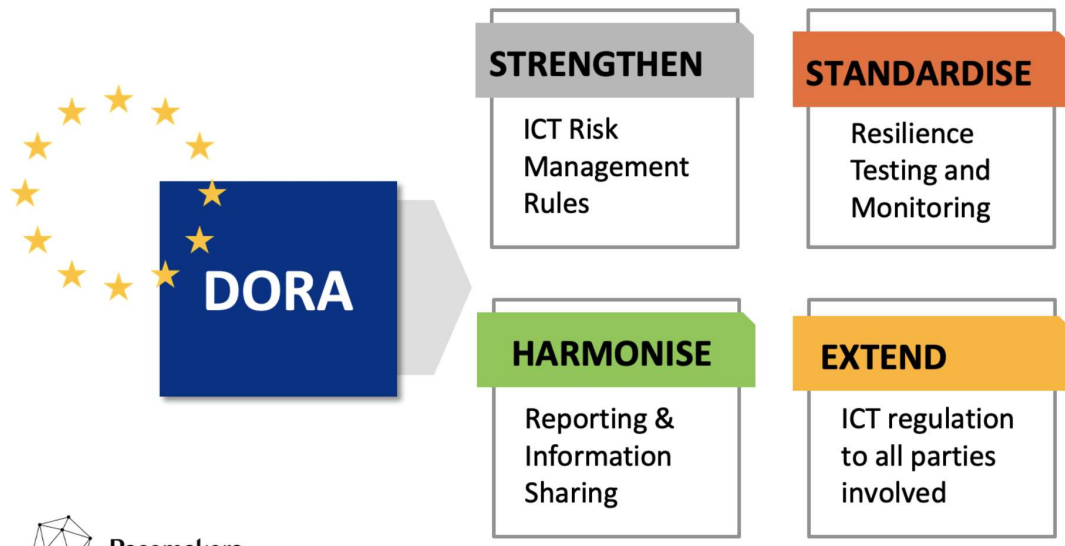


Figure 5. Representation of the Digital Operational Resilience Act, available at <https://www.pacemakers.io/dora-1>

### 2.4. EU CYBERSECURITY STANDARDIZATION BODIES

There is a plethora of bodies involved in cybersecurity standardisation. A comprehensive list is included in [ENI19] and summarized below

- **ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection.** This standardisation committee develops international standards for information security, cybersecurity and privacy protection. They have produced over 150 standards, including generic methods, techniques, and guidelines to address both, security and privacy aspects, such as:
  - security requirements capture methodology;
  - management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services: ISO/IEC 270XX family;
  - cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information, ISO/IEC 18033, ISO/IEC 29192, ISO/IEC 10118, ISO/IEC 15946;
  - security management support documentation including terminology, guidelines as well as procedures for the registration of security components;

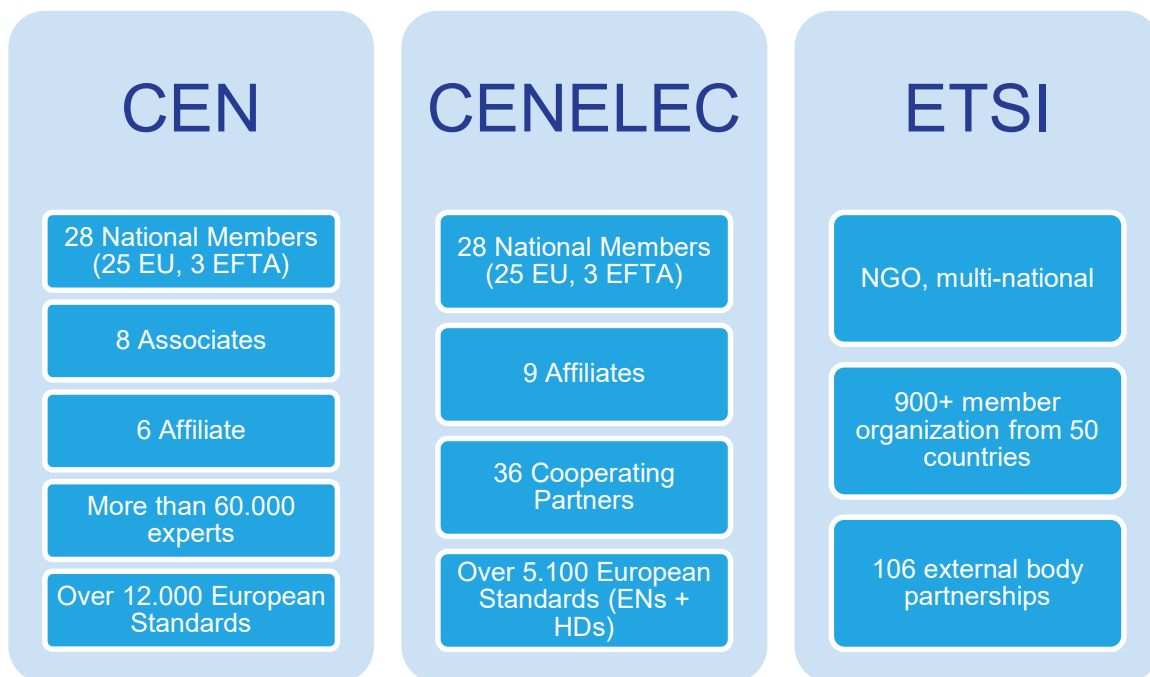
- security aspects of identity management, biometrics and privacy like ISO/IEC 24761, ISO/IEC 24745, ISO/IEC 24760, ISO/IEC 29100/29101, ISO/IEC 27101;
  - conformance assessment, accreditation and auditing requirements in the area of information security;
  - security evaluation criteria and methodology ISO/IEC 15408/18045 known as Common Criteria, and also ISO/IEC 19790/24759 Security module evaluation.
- **CEN CENELEC JTC13 Cybersecurity and Data Protection.** This committee develops standards for data protection, information protection and security techniques with specific focus on cybersecurity covering all concurrent aspects of the evolving information society, including:
  - Organizational frameworks and methodologies, including IT management systems
  - Data protection and privacy guidelines
  - Processes and products evaluation schemes
  - ICT security and physical security technical guidelines
  - Smart technology, objects, distributed computing devices, data servicesCEN CENELEC JTC13 is also organizing in coordination with ETSI TC Cyber dedicated events on cybersecurity standardisation, with the support of CCMC (CEN CENELEC management centre) and ENISA
- **ETSI TC CYBER.** The ETSI TC CYBER (Cybersecurity) intends to cover:
  - Cyber Security Standardization from a generic point of view
  - Security of infrastructures, devices, services and protocols
  - Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators
  - Security tools and techniques to ensure security
  - Creation of security specifications and alignment with work done in other Technical Committees and International Study GroupsIt coordinates work with external groups such as the CEN/CENELEC JTC13, the NIS Platform and ENISA. It collaborates with other SDOs (ISO, ITU, NIST, ANSI etc.). The committee answers to policy requests on cybersecurity and ICT security in broad sense.

For security evaluation, ETSI has published the TR 103-645 – Cybersecurity for consumer IoT, which will become the basis for a future EN.
- **Other relevant committees of standardization bodies:**
  - ISO/IEC JTC 1/SC 41 Internet of Things and related technologies
  - ISO/IEC JTC1/SC 38 Cloud Computing and Distributed Platforms
  - ISO/IEC JTC 1/SC 42 Artificial intelligence
  - ISO TC22/SC32/WG11 Automotive cybersecurity.
- **Industrial Forum of interest:**
  - 3GPP/GSMA, for 4G/5G concerns
  - CSA, Cloud security has a liaison with ISO/IEC JTC1/SC27WG4

- Fido Alliance,
- Eurosmart
- Global platform, has a liaison with IOS/IEC JTC1/SC27/WG3
- IEEE,
- IETF,
- AIOTI,
- one M2M,
- TCG, has a liaison with ETSI TC CYBER
- Oasis, has a liaison with ETSI TC CYBER

The main standards used currently for cybersecurity evaluation are:

- ISO/IEC 15408/18045 – Common criteria and evaluation methods. These standards are under important revision at ISO/IEC JTC1/SC27 level
- IEC 62443-4-2 – Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components
- EN 303-645 – Cybersecurity for consumer IoT, which is a standard originally developed by ETSI and now managed under a joint agreement by ETSI CEN CENELEC. This a good example of future collaboration



**Figure 6. Main standardisation bodies at EU level**

European standardization has led to the cooperation and agreements among countries. The benefits of standards for European industry are extensive helping manufacturers reduce costs, anticipate technical requirements, and increase productive and innovative efficiency. The European Commission recognises the positive effects of standards in areas such as trade, the creation of Single Market for products and services, and innovation.

The basic principles that are in the same time strengths of the European standardization are:

- identical standards throughout all countries
- removes barriers to trade
- complete the Single Market
- larger markets create wealth
- competitiveness and technical innovation
- guarantees State of the Art
- regional influence in the global economy
- exports European know-how
- access to the Single Market
- self-development' for Accession countries
- alternative to formal regulation
- 'self-regulation' by the user and industry [KEL10]

## 2.5. EU CYBER-ECOSYSTEM

Research into digital security is essential to building innovative solutions that can protect us against the latest, most advanced cyber threats. That is why cybersecurity is an important part Horizon 2020 and its successor Horizon Europe.

In Horizon Europe, for the period 2021-2027, cybersecurity is part of the 'Civil Security for Society' cluster.

As part of Horizon 2020, the Commission co-funded research and innovation into topics such as cybersecurity preparedness through cyber ranges and simulation, cybersecurity for small and medium-sized enterprises, cybersecurity in the electrical power and energy system, and cybersecurity and data protection in critical sectors. These topics fall under the cluster 'Secure societies — Protecting the freedom and security of Europe and its citizens.'

**ENISA** – the EU cybersecurity agency. ENISA is the EU's agency that deals with cybersecurity. It provides support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

**ISACs.** Information Sharing and Analysis Centres (ISACs) foster collaboration between the cybersecurity community in different sectors of the economy. Further developing ISACs at both EU and national level is a priority for the Commission. In collaboration with ENISA, the Commission also promotes the establishment of new ISACs in sectors that are not covered. The "empowering EU ISACs consortium", supervised by the Commission, provides legal, technical, and organisational support for ISACs.

**JRC.** The Joint Research Center (JRC) of the Commission is actively contributing to Cybersecurity in the EU. For example, the JRC has developed a Cybersecurity Taxonomy. This aligns the terminology used in cybersecurity so that we can have a clearer overview of cybersecurity capabilities in the EU. The JRC also recently published a report that provides insights into the current EU cybersecurity landscape and its history, entitled “Cybersecurity – our digital anchor”.

**CSIRTs/CERTs.** Under the NIS Directive, EU Member States are required to ensure that they have well-functioning Computer Security Incident Response Teams ('CSIRTs'), also known as Computer Emergency Response Teams ('CERTs'). These teams provide deal with cybersecurity incidents and risks in practice. They cooperate with each other at EU level, and work together with the private sector. All types of operators of essential services and digital service providers must be covered by designated CSIRTs.

The main tasks of CSIRTs are:

- monitoring incidents at a national level;
- providing early warning, alerts, announcements and other information about risks and incidents to relevant stakeholders;
- responding to incidents;
- providing dynamic risk and incident analysis and situational awareness;
- participating in the CSIRTs network [[NIS16](#)].

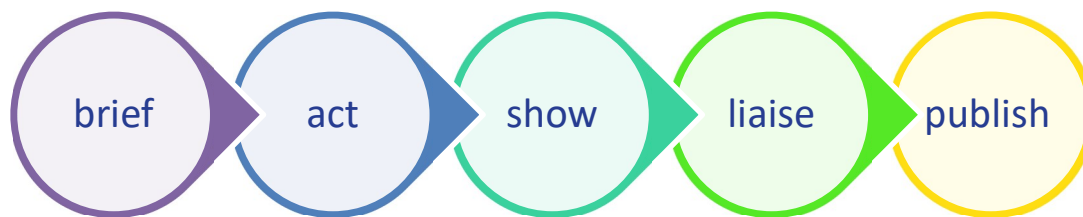
**ECSO.** The European Cybersecurity Organisation (ECSO) was created in 2016 to act as the Commission's counterpart in a contractual public-private partnership covering Horizon 2020 in the years 2016 to 2020. The majority of ECSO's 250 members belong either to the cybersecurity industry or to research and academic institutions in the field. To a lesser degree, ECSO's members also comprise public sector actors and demand-side industries. Besides making recommendations on Horizon 2020, ECSO carries out various activities aiming at community building and industrial development at European level.

**Women4Cyber.** It is important to highlight the role of women in the cybersecurity community, who are underrepresented. That is why the Commission has set up the Women4Cyber Registry, in cooperation with ECSO's Women4Cyber initiative. It makes it easier for the media, event organisers and others to find the many talented women working in cybersecurity, so these women become more visible and prominent in the cyber community and the public debate.



### 3. ENERGYSHIELD PROJECT TOUCHPOINTS

Within EnergyShield project follows five step conceptual pathway (Figure 7) to identify the most suitable ways to contribute to standardization and policies related to cybersecurity and EPES.



**Figure 7. Proposed pathway to reach standardization and policy bodies**

The journey started with briefing the EU cybersecurity regulation and policy framework. These documents were assessed in depth in the first year of the project as part of technical requirements [ESH11], commercial requirements [ESH12], regulatory requirements [ESH13], ethics requirements [ESH10], system architecture [ESH14] and data management [ESH93] reports. Next, Consortium members started working on improving, adapting the proposed tools to the EPES and developing new concepts. As the first iteration of tools development was closed, technical partners have promoted the tools in different events and workshops, while the academic partners started drafting scientific articles, liaise with similar H2020 initiatives (12) and publish scientific articles (31).

#### 3.1. STANDARDS & POLICY PATHS

The EnergyShield project contributes to the standardization of metrics able to provide a more holistic “system of systems” picture of the vulnerabilities of a complex infrastructure.

The EnergyShield toolkit is organized in several “shelves” or “drawers” and contains hardware components, software components, and communication ports. The toolkit is accessible via a Portal through an authentication mechanism:

- ASSESSMENT tools add focus on the critical infrastructure components and leverages the security behaviour to improve the vulnerability analysis.
- MONITORING & PROTECTION tools focus on allowing rapid attack response (e.g., heat maps of intrusion).

- LEARNING & SHARING tools gradually automate the security information and event management process and integrate vulnerability assessment tools to create security metamodels.

EnergyShield deploys an open source SIEM tool compatible with the most widely used network security tools using the IDMEF (Intrusion Detection Message Exchange Format) standard format, making sure that incident reports can be shared seamlessly with EU CERTs and EPES operators.

For SOC/CSIRTs, the vulnerability assessment tool can continuously monitor an infrastructure, following and considering changes to the technical infrastructure, human users and IAM, vulnerabilities and cyber threat intelligence. Its usage extends from adversary emulation, red teaming, behavioural analytics development to a defensive gap and SOC (Security Operations Centre) maturity assessment.

The components of EnergyShield toolkit exposes a set of REST API that enables the interoperability between them and the possible integration with other tools.

The EnergyShield toolkit offers asynchronous message exchange using queues, inter module asynchronous communication, and allowing external system to subscribe to the topics.

The global view of each tool results using a data fusion mechanism combined with a machine learning system able to continuously improve the outputs of the fused model.

The whole architecture is federated. There is a central federation Coordinator and there are locally deployed federation members. The central component is responsible for maintaining the rules and standards, for common processing. The federation members are responsible for local data collection and processing.

One way to manage cybersecurity, often tightly coupled with expert investigations, is to implement the guidelines prescribed by standards or frameworks such as the ISO/IEC 27000 and ISO/IEC9000 series and SO/IEC/IEEE 12207. However, these guidelines are by design very general and do not provide any readily available means to measure and improve security. As a consequence, application of them can be vague and troublesome. Another issue is the standardization of vulnerability descriptions.

### 3.1.1. CODING STANDARDS

EnergyShield project proposes standardized approaches supporting the NIS directive [NIS16], both at system/process level (vulnerability assessment tool based on Bayesian networks) and component level (cybersecurity supply chain risk management). EnergyShield deploys an open source SIEM tool compatible with the most widely used network security tools using the IDMEF (Intrusion Detection Message Exchange Format) standard format, making sure that incident reports can be shared seamlessly with EU CERTs and EPES operators.

The key coding standards to help ensure secure software development include:



- CERT - registered in the U.S Patent and Trademark Office by Carnegie Mellon University
- CWE - Common Weakness Enumeration
- CVE - Common Vulnerabilities and Exposures
- OWASP - Open Web Application Security Project
- DISA STIG - (DISA — Defense Information Systems Agency) that provides technical guides (STIG — Security Technical Implementation Guide).
- NVD - National Vulnerability Database
- CVSS - Common Vulnerability Scoring System

There are many **knowledge databases** that describe modus operandi of attackers as well as exploits of vulnerabilities, such as Common Vulnerabilities and Exposures (CVE) databases. A CVE is composed of an identifier and a general summary. A CVE belong to an abstracted class called Common Weakness Enumeration (CWE), a formal list or dictionary of common software weaknesses that can occur in software architecture, design, code or implementation that can lead to exploitable security vulnerabilities. The CWE was created to serve as a common language for describing software security weaknesses, to serve as a standard measuring stick for software security tools targeting these weaknesses, and to provide a common baseline standard for weakness identification, mitigation, and prevention efforts. The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. The CVSS assessment measures three areas of concern: base metrics for qualities intrinsic to a vulnerability, temporal metrics for characteristics that evolve over the lifetime of vulnerability and environmental metrics for vulnerabilities that depend on a particular implementation or environment. A numerical score is generated for each of these metric groups. A vector string represents the values of all the metrics as a block of text. However, as discussed earlier, these metrics generate a long list of vulnerabilities for every software component/application in the architecture, ranked by CVSS score, but do not provide an aggregate “system of systems” picture.

Energy Shield tools provide information on most critical attack vectors and probable paths, focus on allowing rapid attack response and gradually automate the security information and event management process and integrate vulnerability assessment tools to create security metamodels.

- The **Vulnerability Assessment** (VA) tool integrates a threat model (attack vectors and probabilities) and is built into securiCAD Enterprise; supports MAL based threat modelling languages that allows a more adequate representation of EPES systems. The Risk Matrix - Confidentiality, Integrity and Availability - scores are the sum of the probabilities for the attacker to have succeeded with

compromising C, I and/or A related operations (like read, write and deny) for the selected high value assets. It is extended to inform other modules of the identified vulnerabilities and priorities in real time. Uses CVSS scoring of vulnerabilities. It is non-intrusive, meaning it will not interfere with the actual systems

- The **Security Behaviour Analysis (SBA)** tool evaluates the current security readiness of an organization's workforce. The identification of specific cyber-threats based on the achieved socio-cultural behaviour assessment results exploiting a) a hybrid MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Model for an OT Environment, consisted of a combination of the Enterprise and the ICS threat models and b) an enriched version of the MERIT (Management and Education of the Risk of Insider Threat) model.
- The **Anomaly Detection (AD)** tool rather than analysing limited data available only in the network (top) levels of the ICS layers (e.g., communication protocols, access & control software, or HMI), the tool integrates into the actual physical layer of the ICS (Level 0), monitoring and analysing EPES asset operations by duplicating unidirectionally electrical signals that run between sensors and actuators to the PLC. These duplicated electrical signals are used by the tool in an out-of-band, separate, independent, and autonomous network, and are analysed by our unique and powerful smart AI engine? Data from legacy systems can be accessible via online batch processing of different formats, including CSV, JSON, XML Online data from legacy systems can also be achieved by using MQTT protocol, or by accessing APIs where available.
- EnergyShield's **Security Information and Event Management (SIEM)** tool supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources, including other Energy Shield tools such as the DDoS mitigation tool and the anomaly detection tool. The SIEM tool supports compliance reporting and incident investigation as well as sharing with CERTs and other operators
- The **Automated Forensic Tool (AFT)** enrich events identified and reported by the SIEM tool with information deriving from different security databases, such as CWE, CVE, CAPEC, MITRE ATT&CK, OVAL, WASC, OWASP.
- EnergyShield **toolkit** exposes a set of REST API that enables the interoperability between them and the possible integration with other tool, offers asynchronous message exchange using queues, inter module asynchronous communication, and allowing external system to subscribe to the topics. Also. the toolkit is accessible via a Portal through an authentication mechanism. EnergyShield toolkit includes container engine (Docker), Authentication and Authorization (Keycloak), Communication system (Kafka), REST, and Process management (Kubernetes). The whole architecture is federated. There is a central federation Coordinator where federation members

are locally deployed: the central component is responsible for maintaining the rules and standards, for common processing, while the federation members are responsible for local data collection and processing.

### 3.1.2. SECURITY AND PRIVACY

Energy Shield project has worked on two concepts approaching security and privacy:

- Cybersecurity supply chain risk analysis (chain of software and hardware components that are part of tools such as control systems that are used to operate critical energy infrastructures.),
- Searchable Encryption and Homomorphic Encryption (anonymise and search data in the encrypted domain using the state-of-the-art homomorphic encryption techniques)

Thus, EnergyShield toolkit will support NIS and GDPR compliance as follows:

- Enable critical infrastructure operators to share early warning on cybersecurity risks and incidents as well as to report major security incidents on their core services.
- Provide this standard of measurement against which security effectiveness can be demonstrated, decrease the risk and occurrence of major data breaches
- Enable EPES operators to check both their understanding of the regulations and the technical challenge to test preparedness
- Define business recovery and resilience planning in the case of a cyber-attack
- Provide an intelligence-led responds to certain events by triggering types of training targeted at the weak points in the organisation
- Identify services that look for evidence of interest by attackers, whether bedroom hackers, hacktivists, cyber criminals, or state attackers after company secrets
- Provide managed security services which take away the need to invest in security teams, introduced that is increasingly hard to do because of the global cyber skills shortages
- Offer advanced managed security services that 'hunt' for hidden presences, attackers interested in siphoning out sensitive data without the client organisation's knowledge
- In addition, all data collected from pilot deployments will be sent through secure, encrypted channels and stored on controlled, secured servers. Access to data will be carefully restricted to authorized users and for authorized purposes only. All data will be physically stored in Europe.

## 3.2. AWARENESS RAISING & COMMUNICATION PATHS

Awareness raising and skills development remain relevant Strategy objectives, for which continuous efforts at both national and EU level are needed. A report issued by ENISA at the end of 2021 [ENI21] proposes recommendations to increase the effectiveness of national awareness raising activities, based on the research of existing NCSS, and from information provided by identified stakeholders who were interviewed for this study

- building capacities for cybersecurity awareness,
- regular assessments of cybersecurity trends and challenges,
- measuring cybersecurity behaviour, and
- planning for cybersecurity awareness campaigns

Moreover, a report published by ENISA [SKL19] European Skills Agenda for sustainable competitiveness, social fairness, and resilience [SKL20] approaches the shortfall of a cybersecurity workforce capable of handling cybersecurity tasks represents an issue for both economic development and national security. The rapidly growing demand for digital experts cannot be met. For example, (ISC)<sup>2</sup> cybersecurity workforce study [ICS19] suggested there is a gap of 291,000 professionals in cybersecurity in Europe up from the previous estimate of 142 000 professionals that had been given in the 2018 report.

### 3.2.1. ENERGYSHIELD POLICY WORKSHOP

EnergyShield Consortium has organized the European workshop Trends, opportunities, and choices in designing a cyber resilient EPES infrastructure on the 15<sup>th</sup> of April 2021, 10.00 CET.

The event was initiated and organized by three EnergyShield partners: Software Imagination & Vision (Coordinator), KTH Royal Institute of Technology in Stockholm (Dissemination & Communication Leader) and National Technical University of Athens (Collaboration Leader).

The event gathered Critical infrastructure stakeholders, business, academia, and industry professionals from 8 European countries around cross-domain topics.

A total of 135 persons attended the online EnergyShield workshop and the majority were interested in the opening session topics.

Different aspects of cyber security in EPES sector including standardization efforts and policy updates were addressed during the opening sessions led by representatives from European Commission, ENISA and energy standardization and regulatory bodies. Also, a brief introduction of Energy Shield project and a demonstration of the toolkit developed completed this session.

The second part of the workshop focused on two topics that will be addressed in two consecutive panels equipped with high profiled experts from the field. The first one


elaborated on the effect of work from home on energy and IT infrastructures, while the second one addressed the latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies.

In the first part of the workshop, representatives from the EU agencies and H2020 projects have provided insights on recent policy developments in cybersecurity for critical infrastructure protection, on the activities run by ENISA and on ways of brooding the gap between EPES and cybersecurity. All these presentations were followed by a demonstration of the EnergyShield tools and toolkit.

The second part of the workshop focused on two topics that will be addressed in two consecutive panels gathering experts and professionals from the various domains.

The organisers of the event alongside with the speakers and panellists draw the attention on the lifestyle imposed by COVID-19 pandemics, on the associated cyber vulnerabilities and windows opened to attackers. How did work from home impact us? Are we prepared to continue working from home as the number of cyber-attacks increases? The answers to these questions will reshape the future technologies and business models.





DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID!

## Trends, opportunities and choices in designing a cyber resilient EPES infrastructure

**ENERGYSHIELD (WORKSHOP) TOOLKIT**

**YOU'RE INVITED** EPES value chain stakeholder, critical infrastructure and/or cyber security expert, researcher, scientist or domain enthusiast

**ATTEND** Virtual event engaging different stakeholders in cross-domain topics. Speeches about standardization efforts and policy updates. 2 panels with high profile experts

**ENGAGE** Fill a survey and add questions for PANEL 1 <https://bit.ly/3R2H4XK>. Fill a survey and add questions for PANEL 2 <https://bit.ly/3JdMS5H>


**SHARE** Use #EnergyShield\_Event2021 to promote the event via Twitter. Check out the latest news on project website [www.energy-shield.eu](http://www.energy-shield.eu). Join EnergyShield group and event on LinkedIn

**While deciding...** Watch the EnergyShield project video <https://youtu.be/ASU5hmkp1Dw>

**About EnergyShield project**

EnergyShield project follows an integrative approach to assess, monitor, protect and manage security threats and insights. Several tools are combined in a toolkit that provides an unique perspective and supports the needs of Electrical Power and Energy System (EPES) value chain in predicting cyber and physical attacks, learning from previous attacks and preventing future attacks. The assessment tools add focus on the critical infrastructure components and leverages the security behaviour to improve the vulnerability analysis, monitoring & protection tools focus on allowing rapid attack response, while tools gradually automate the security information and event management process and integrate vulnerability assessment tools to create security metamodels.


**Vulnerability Assessment Tool**



**Anomaly Detection Tool**



**Security Behaviour Analysis Tool**




**EnergyShield toolkit**

**WORKSHOP AGENDA | 15-04-2021**



OPENING SESSIONS		10.00 CET - 11.30 CET
Welcome and brief introduction of EnergyShield project (10')		Otilia Bularca, SIMAVI
Recent policy developments in cybersecurity for critical infrastructure protection (10')		Christian Wilk, EC
ENISA's activities in the energy sector (15')		Konstantinos Moulinos, ENISA
Bridging the gap between EPES and cybersecurity (10')		Dr. Venizelos Eftymiou, UCY
Combining MAL with safety & functional modelling (10')		Chris Few, Ofgem UK
EnergyShield toolkit demonstration (15')		Iacob Ciucanu, SIMAVI
Q & A (10')		Coffee break (10')

PANEL 1   11.30 CET - 12.00 CET	PANEL 2   12.00 CET - 12.30 CET
Work from home impact on the energy and IT infrastructures	Latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies
<p><b>Moderator:</b> Tommy Wahlman, Swedish Energy Agency</p> <p><b>Panelists:</b> Daniela Bichir, SIMAVI Javier Valillo, ATOS Prof. David Wallom, Oxford e-Research Centre Dr. Mihai PAUN, CRE Loris Piana, IREN Italy</p>	<p><b>Moderator:</b> Monica Flores, SIMAVI</p> <p><b>Panelists:</b> Sarah Fluchs, admertitia GmbH Dr. Ing. Matthias Rohr, PSI Dan Cimpean, CERT-RO Maximiliano Masi, Autostade per l'Italia Matteo Merlardo, RHEA Group</p>

**CO-ORGANISERS**





**FACILITATORS**




**HOST**




**ENDORSERS**







**CO-ORGANISERS**





**CO-ORGANISERS**





This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement 832907

**Figure 8. EnergyShield policy workshop agenda and speakers**

Two short surveys have been submitted to general audience to collect insights for the panels announced within the EnergyShield workshop:

- A) Panel 1 – Work from home impact on the energy and IT infrastructures
- B) Panel 2 – Latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies

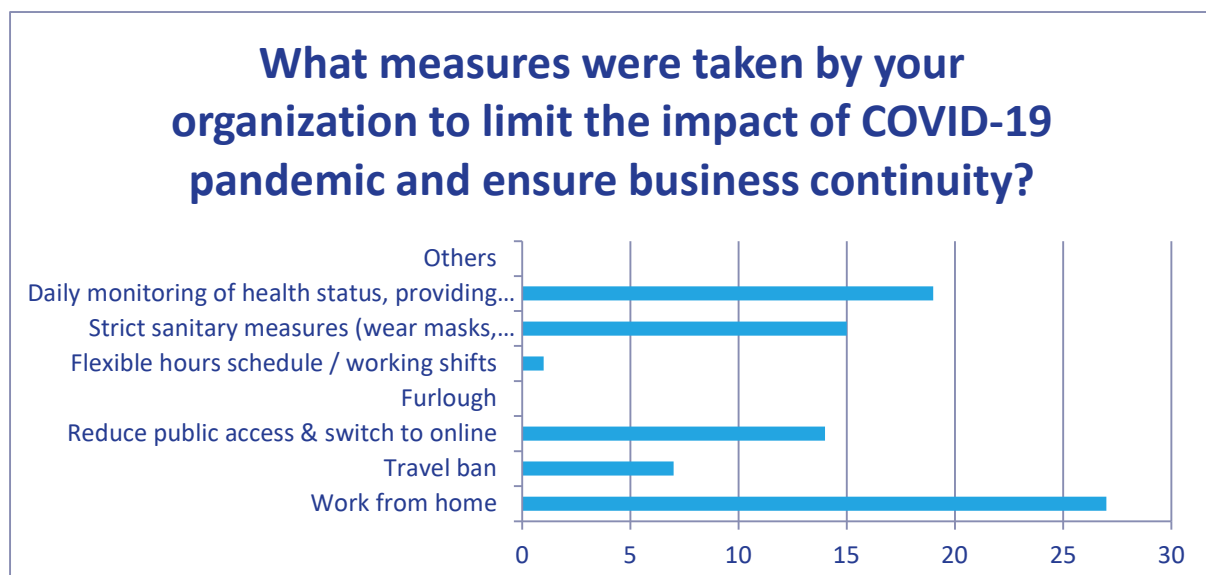
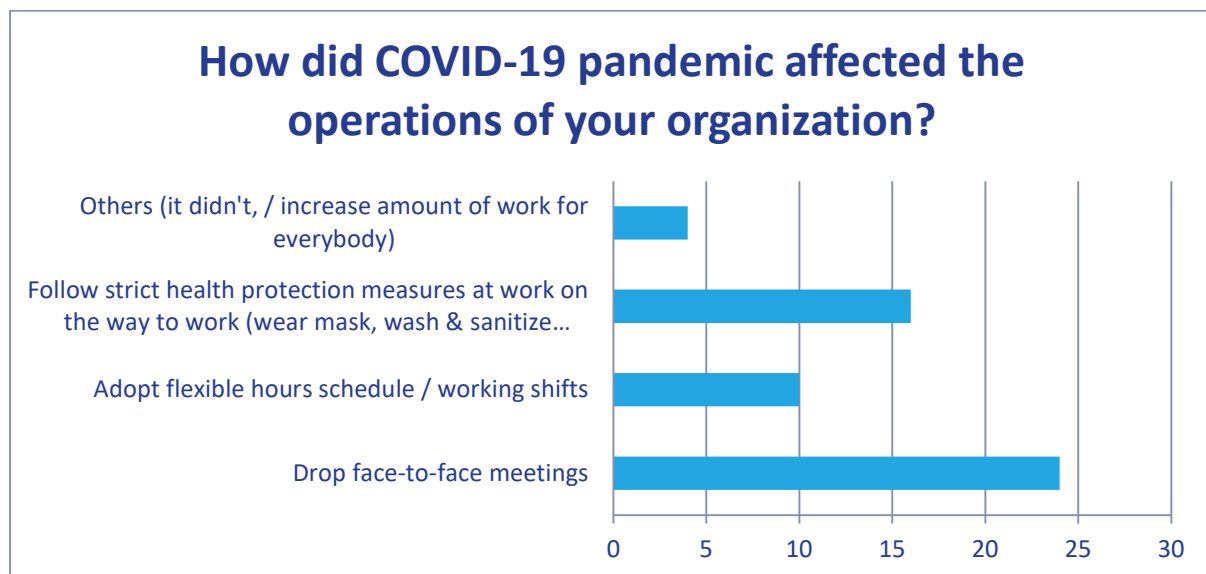
All the information collected via these surveys is presented in the sections below. Anyone reaching the surveys could have filled them in anonymously and alternatively could provide an e-mail address for the follow-up report.

- Panel 1 – Work from home impact on the energy and IT infrastructures

The first panel approaches the effects work from home had on energy and IT infrastructures.

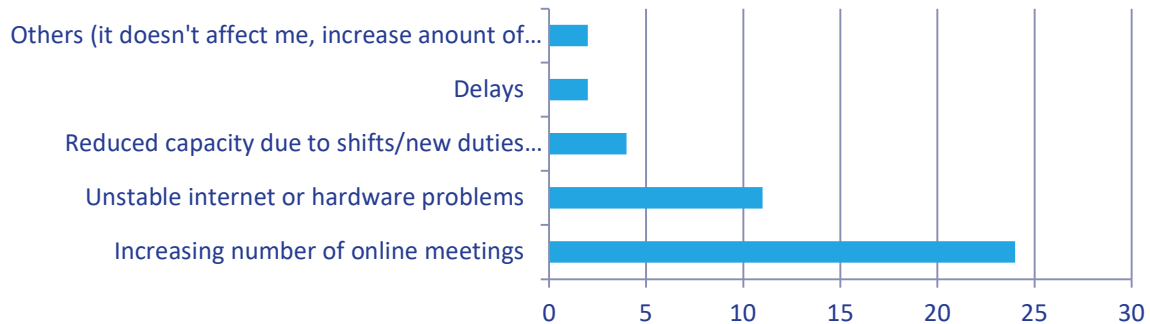
The 4 questions proposed survey for this panel gathered interesting insights prior the event. The results show an overwhelming shift to work from home and an increased interest in health monitoring. On top of these the reality of home working brings a high number of online meetings and concerns related to morale and creativity.

The graphs below show how did COVID-19 reshaped business relationship and which measures were preferred to ensure safety.

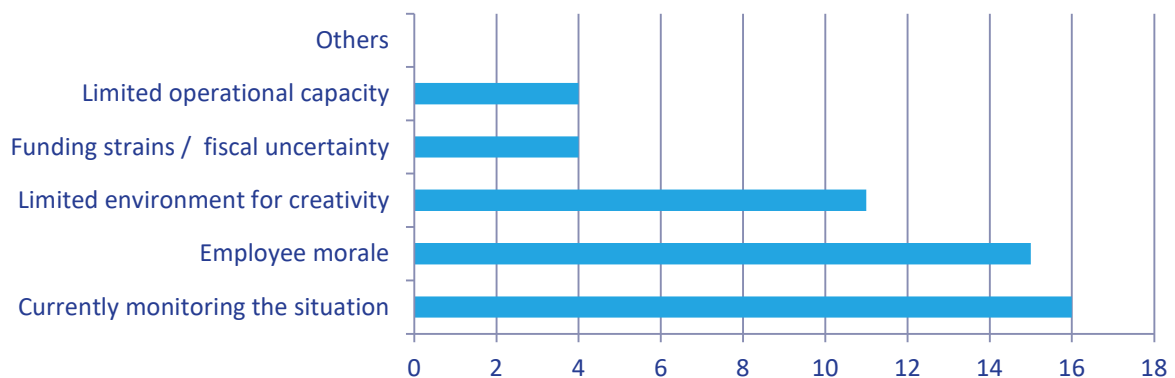


The survey answers show that working from home also has an impact on daily activities. As seen in the following figures the number of the online meeting increased and concerns related to creativity and morale were raised.

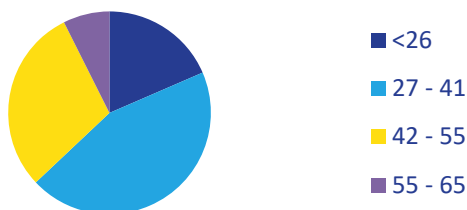
## How does COVID-19 affect day-to-day business within your organization?



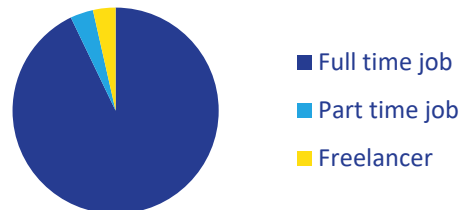
## Do you foresee any further risks related to the extension of COVID-19 pandemic situation?



### Age range



### Employment status



Tommy Wahlman, Programme Manager, The Swedish Energy Agency took the lead of the panel and invited all participants to answer the following questions:

**Below you may find some the things mentioned by the panellists:**



**a) What is your opinion on this topic? Please share thoughts on the results of the survey**

- Shifting to work from home was a challenge for the organizations as the change had to happen fast and all control systems and management approach adapted to the new context
- Remote working is the future (at least in IT)
- Companies need to give workers the necessary IT infrastructure (hardware and software) and to motivate their employees to be happy.
- Remote working in academia might be difficult for young researchers
- Remote working & large videoconferences mean an increased use of resources
- A hybrid solution could suit more categories of professionals as in some cases physical presence is needed (e.g., OT environments).
- Induction and mentoring in case of remote working is difficult
- The infrastructure still needs to be adapted for remote working as users face difficulties with internet connection
- New skills are needed for remote working

**b) Are we aware on how we create value in the organization when we're sitting at home? Has that value creation changed for the companies when we're sitting at home? How do we collaborate to create value in innovation?**

- An Agile approach & empowering more the project manager
- On boarding, induction and coaching is difficult
- Keeping innovation alive is still possible? It depends on the happiness of the employee, their state of mind.
- Alternatives for people that are not able to work from home due to personal reasons
- Beyond regular meetings (that should be kept short) a one-to-one engagement is necessary to substitute human interaction
- Available tools cannot replicate face-to-face communication & interaction for a brainstorming session for instance
- To boost creativity among employees' leisure & hobby virtual meetings could be considered
- How is working from home for the Energy industry? The ICT infrastructure needs to be re-designed to cope with remote working
- Protecting devices from attacks in remote scenario is not easy as the environment itself might not be secure enough

**Questions from audience (survey or chat)**

- Increased pressure on the IT infrastructure that needed to be upgraded

As a huge part of employees shifted to online working, family service packages/solutions became business packages/solutions. To face this transition both service and technology providers need to adapt their business models to the new reality, i.e., high speed internet connection from everywhere and maybe back-up solutions for remote workers.

- Shouldn't the employers and/or government provide every employee who works from home – some on their own devices, as teachers do – with a package of antivirus programs?

Implementing security standards for home/remote working is difficult but expectations are that technology providers will come up with built-in solutions.

- How do you see the future of work in IT companies after the pandemic (work from home will remain valid)?

After the pandemic remote work will remain an option for a lot of workers. However, some still prefer home working, and this is why a hybrid approach is most likely to be deployed during the next period.

- Do you think thing will revert to 100% face to face work after the pandemic?

A clear and definitive answer is difficult to provide. All companies will assess and prioritize the needs and define how future business engagements will look like. The need of physical presence is a fact, and it has been proved that ensures better communication and collaboration and boosts creativity.

- Will work from home reshape the definition of productivity?

During the panel it has been mentioned that productivity was similar in 2020 and 2019. However, individual assessments are needed as the work context and environment is different for each employee.

- Did organizations increase remote accessibility for critical infrastructure controls?

The COVID-19 pandemic has produced remarkable and unique social and economic circumstances and changes that can be exploited by cyber criminals. The changes are far-reaching, from work practices and socialization, meaning people are now spending more time online, to unemployment rates, which have also increased, meaning more people are sitting at home online – it is likely that some of these people will turn to cybercrime to make a living. As a result, many cyber-attacks take advantage of these events by starting with a phishing campaign that asks victims to download a file or access a URL. The file or URL acts as a carrier for malware that, when installed, acts as a vehicle for financial fraud. To increase the likelihood of success, the phishing campaign uses media and government announcements. What is the experience in this area and what counterstrategies are taken against such campaigns within internal corporate structures?

- During COVID-19 crisis the amount of energy consumed increased or decreased?

The pandemic disrupted and reduced energy consumption, creating significant uncertainty in terms of energy demand and supply. An IEA report [IEA20] released 1 January 2021 shows that Electricity demand dropped to Sunday levels under lockdown, with dramatic reductions in services and industry only partially offset by higher residential use. Also, in EU countries the share of variable renewables in the electricity mix depends on many factors: wind and solar parks in operation, weather conditions, and total demand.

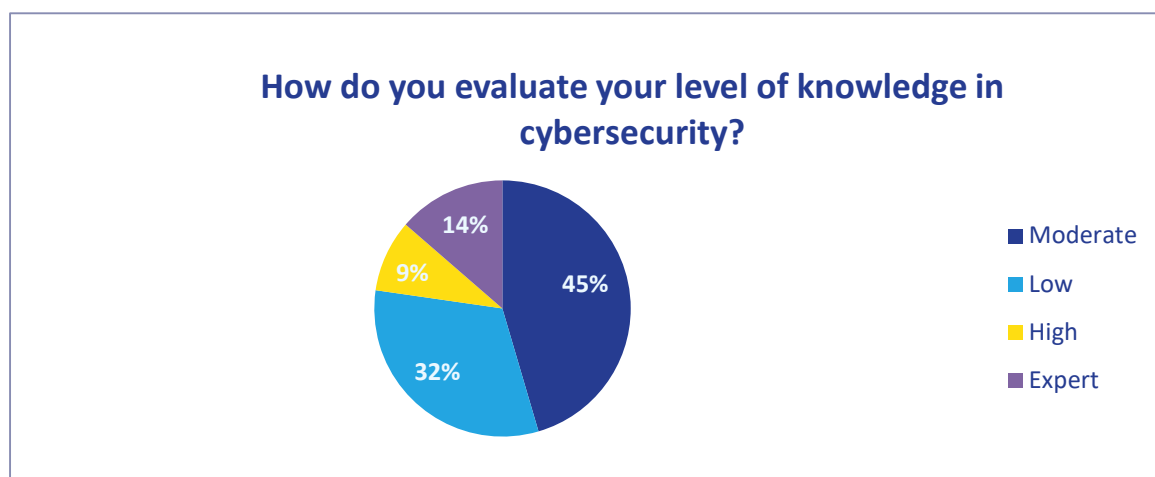
### Conclusions

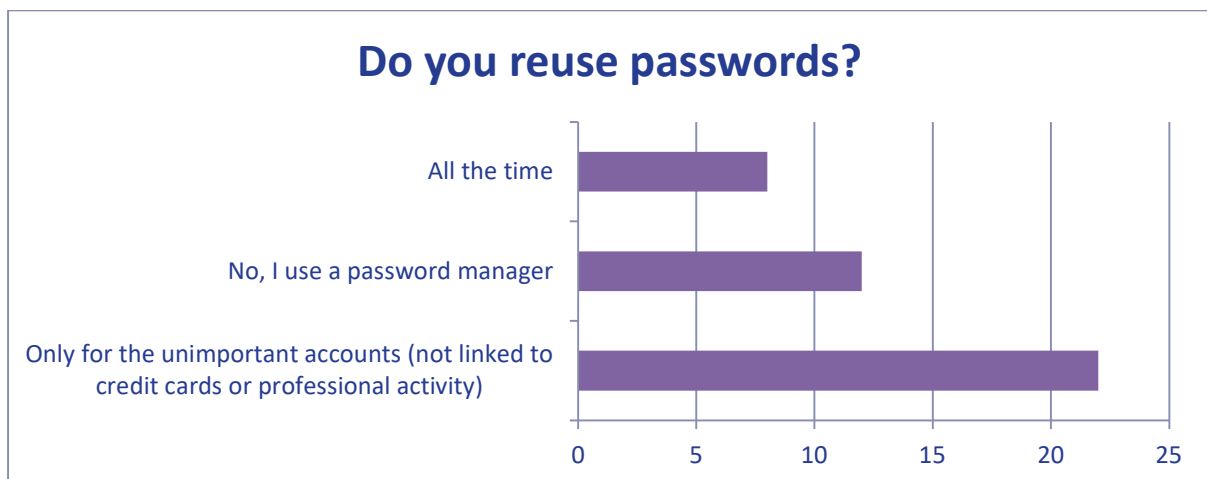
- Opportunities could be connected to happy and productive workers if we could supply them the appropriate devices
- In this case one size does not fit all as not everyone can actually work from home
- Work organisation needs to be redesigned and online fatigue is mentioned and boarding, and coaching are challenging perspective
- **Panel 2 – Latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies**

The second one addresses the latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies.

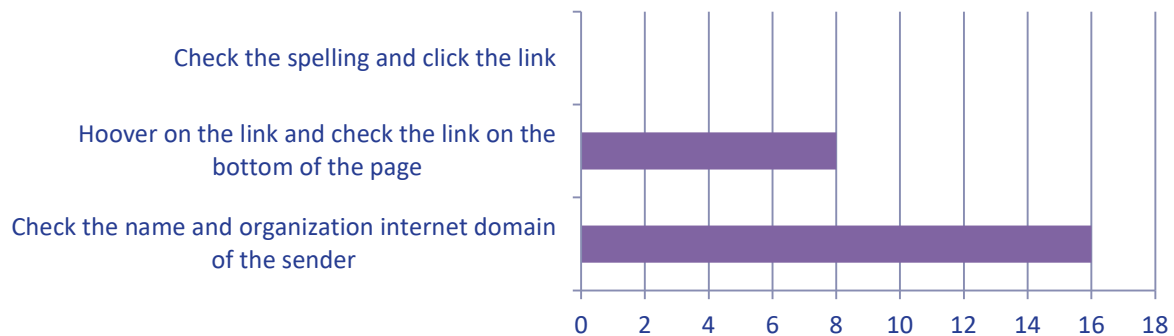
The role of experts in defining measures, policies and incident response plans is crucial, but we could all contribute to maintaining a high level of security within the companies we work acting vigilant.

To find out more about user's cyber-awareness the organisers have launched a 5 questions survey. The results show a high degree of cyber-awareness, but also show vulnerabilities and negligence when it comes to having info at hand (e.g. keeping browsing history and using USB drives).

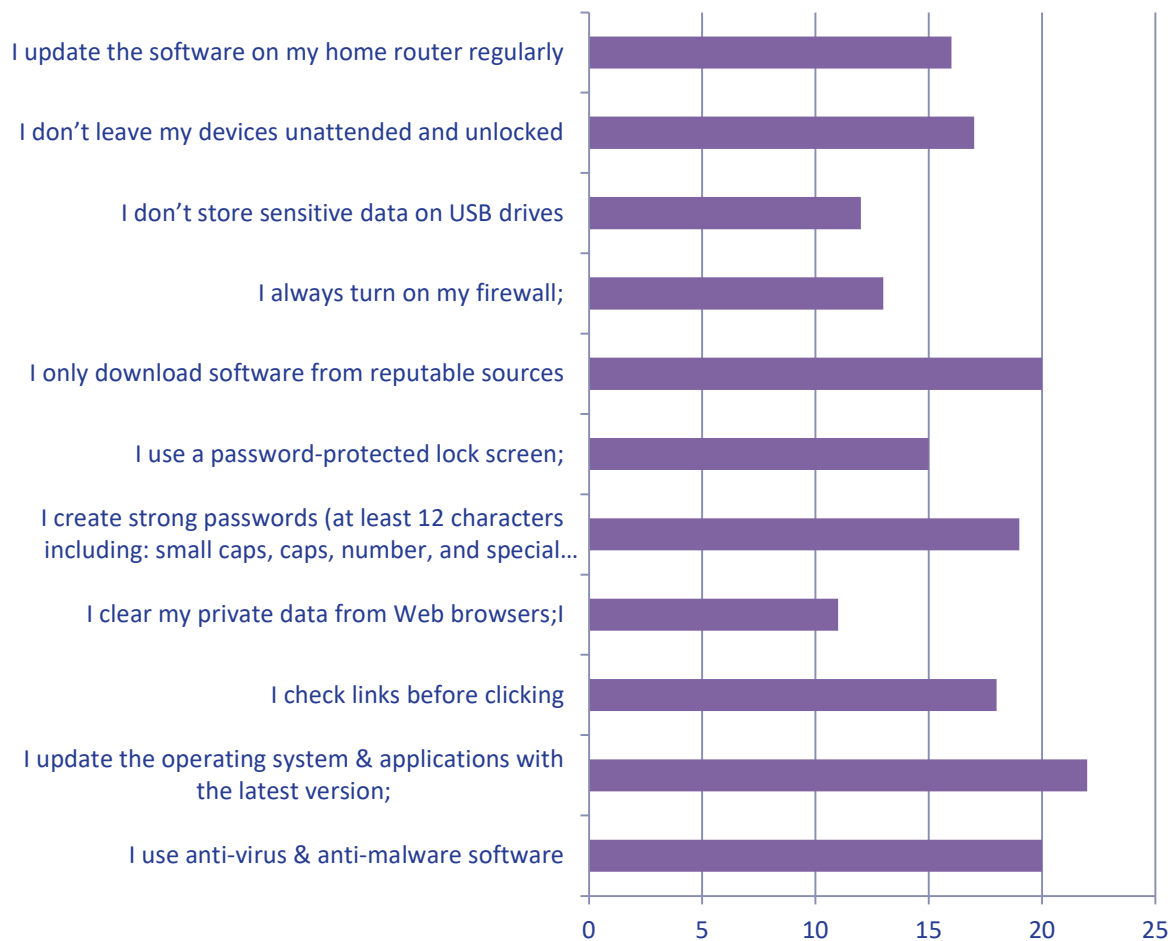


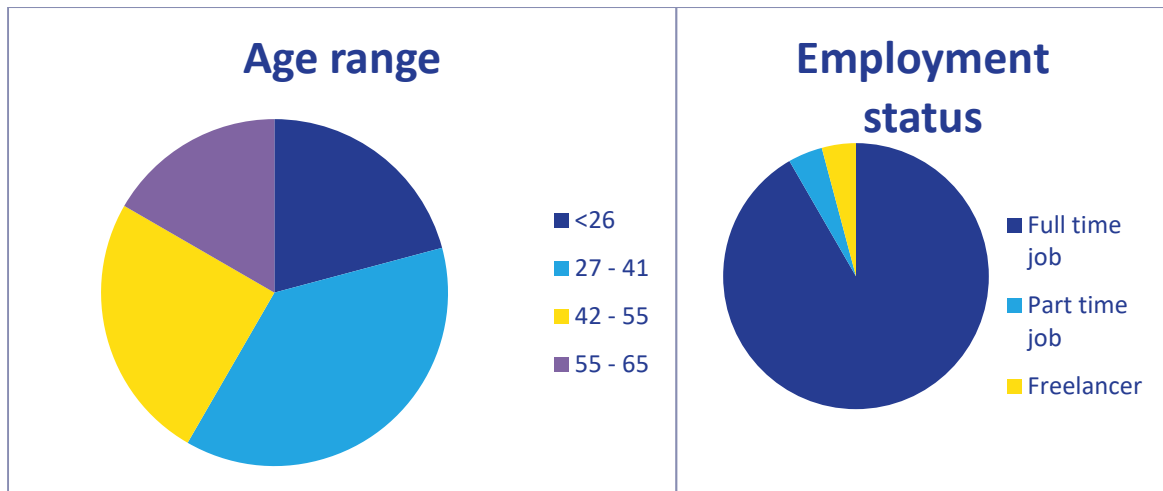


## What do you do to identify possible phishing e-mails?



## Below it's a comprehensive check list of the best practices for securing yourself against malicious actors. Which one of these applies to you?





During this panel, the panellists were clanged to identify the sector/domains that are triggering change during this period, and which are ne necessary means to adjust and to adapt the technology and the business models via the following questions:

- Do you consider supply chain as Critical Infrastructure?
- How to design the systems to avoid spreading the compromise from IT to OT infrastructure?
- Trends to be considered in designing new technologies and business models that help increasing the security level of CIs
- Cybersecurity expertise & training needs; the competences gap

### Insights from panellists

- Supply chain is already critical infrastructure, but it's important to define the critical vendors and plan accordingly
- We need to pay for security; we need more security requirements for CI vendors. A vendor needs to prove that a new product is secure by using strict standards.
- Agile poses risks for CI because most testing is automatic and can introduce threats
- The solution for a security problem is never one product: we should make a risk assessment and threat modelling, and implement secure by design from system inception
- We need to adopt new technologies, but we need to make sure that the security is sustainable across the board
- Change management is very important because it can affect security
- Clear lack of cyber security professionals is obvious, but universities are catching up by increasing the security curriculum.

The organization of this policy workshop with speakers from standardization and policy bodies was a successful initiative (even though online) attracting 135 attendees and many mentions in online newspapers and of course, reaching out to standardization bodies.

It is worth mentioning the fact that EnergyShield project is mentioned in Ofgem report on Analyzing the cyber-security of industrial control systems [OFG21]. This report was published in July 2021, after a representative of the British Office of Gas and Electricity Markets attended and delivered a presentation on MAL standard and its ability to model energy sector specific elements in this official publication.

This report is citing Energy Shield when approaching way of building the attacks graphs: “If the ICS has been built, a vulnerability scanner or network monitoring tool can reveal whether there are publicly known vulnerabilities and if so, a level of difficulty can be assigned to applicable attack steps. The Common Vulnerability Scoring System provides a means of translating vulnerability data into attacker skill levels required to exploit them. If an attack graph is produced in a machine-readable format it is feasible to automate the import of system security data. This can be done through parsers which receive data from sources such as network monitoring tools and write data into the attack graph format. An example of this in development is an EU Horizon 2020 project, Energy Shield” [OFG21].

The MAL language and its extension with energy-sector-specific elements is also mentioned in the Ofgem document. This proves that some EnergyShield content reached standardization bodies. Ofgem also attended one of Foreseeti’s online Energy Shield workshops.

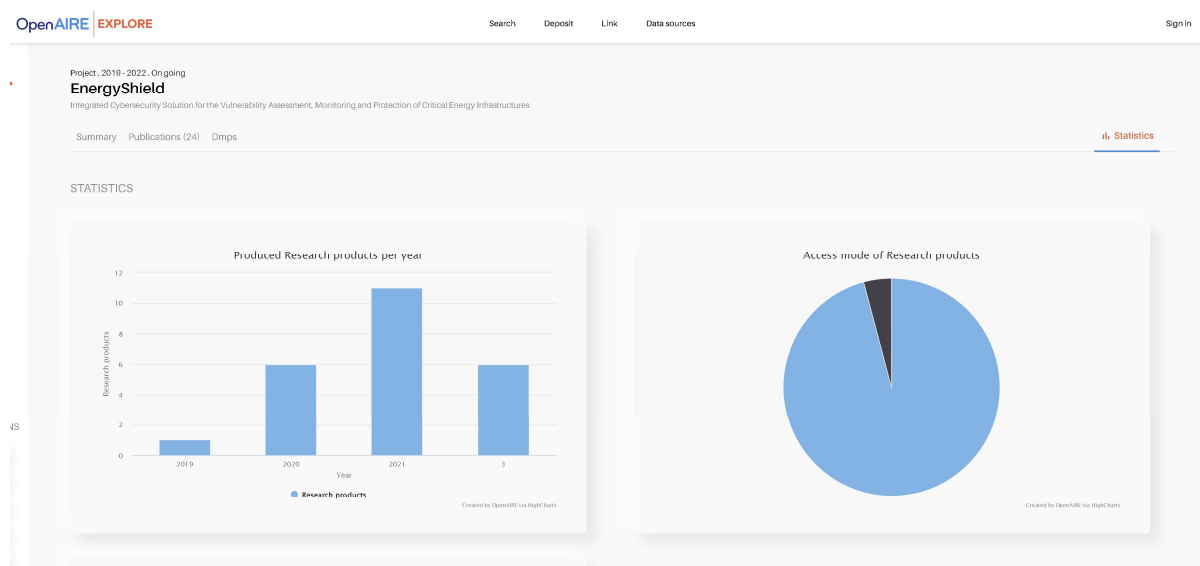
### 3.2.2. CLUSTERING & COLLABORATING

To communicate about the progress and results achieved, EnergyShield consortium partners supported other H2020 projects initiatives, called for endorsement of own events and actions and participated in cluster activities; for two of them being also a founding member: ECSCI (<https://www.finsec-project.eu/ecsci>) and CyberEPES (<https://cyberseas.eu/cyberepes>). All the details are included in D7.8 Collaboration report [ESH78].

### 3.2.3. SCIENTIFIC PUBLICATIONS

EnergyShield follows the open access policy of Horizon 2020 by providing on-line access to scientific information that is free of charge to the end-user and that is reusable. In the context of this project, scientific information refers to peer-reviewed scientific research articles (published in scholarly journals) and research data (data underlying publications, curated data and/or raw data).

The EnergyShield consortium published in open access journals and used OpenAIRE repository [OPR22] for peer-reviewed articles published by the consortium to ensure the largest possible impact among researchers, policymakers, and businesses representatives. 26 of the scientific articles are already available in OpenAIRE repository.



**Figure 9. Dashboard of Energy Shield project in OpenAIRE**

Overall, during project implementation 31 scientific peer reviewed articles were published. These were disseminated via project website [ESH22] where they are available in camera ready versions and have been disseminated via social media channels (Twitter and LinkedIn).

Partners also ensured access to the bibliographic metadata that identify the deposited publication. However, they retained their copyright and grant adequate licences to publishers, based on Creative Commons licenses.

### 3.2.4. WHITEPAPERS PUBLICATION

Ten whitepapers presenting EnergyShield's tools, concept tools, pilots and toolkit were elaborated, published on project website and disseminated via Twitter and LinkedIn to inform the readers and the scientific community about the results and challenges faced by the Consortium during project implementation.

A common structure (Table 1) was defined and guidelines shared for similar approaches and contents.

**Table 1. Whitepaper template sections and guidelines**

Section	Guidelines
<b>In a nutshell</b>	<ul style="list-style-type: none"> <li>section dedicated to a short summary of the whitepaper.</li> </ul>
<b>Context</b>	<ul style="list-style-type: none"> <li>Please use this section to shortly introduce the tool or the pilot concept and the role within Energy Shield project (context and objectives).</li> <li>Please add details about the need and opportunity to deploy this (tool, toolkit, use case) in EPES</li> </ul>



<b>Technical details</b>	<ul style="list-style-type: none"> <li>• Please use this section to introduce the architecture of the tool and the deployed methodology to develop new capabilities (design and methodologies)</li> <li>• Please use this section to add details about the features developed within Energy Shield, the technologies used, etc.(capabilities)</li> <li>• For the Pilots, please use this section to summarize the use cases deployed in Energy Shield project.</li> </ul>
<b>EnergyShield demonstrator</b>	<ul style="list-style-type: none"> <li>• Please describe the set-up &amp; configuration for demonstrating the tool/ pilot</li> <li>• Please include early results</li> <li>• Please assess the implementation process and summarize all the difficulties encountered / ways to overcome the risks and challenges</li> </ul>
<b>Best practices and lessons learned</b>	<ul style="list-style-type: none"> <li>• Plans to use/exploit the results</li> <li>• Please add relevant details/recommendations that you would like to share with the Energy Shield stakeholders</li> </ul>
<b>Dissemination and communication</b>	<ul style="list-style-type: none"> <li>• Add a list of published papers</li> <li>• Add a list of events where the tool/pilot was disseminated/demonstrated</li> </ul>
<b>About the company</b>	<ul style="list-style-type: none"> <li>• Please add a short description of the company: name, contact, business purpose, main relevant achievements</li> </ul>

**Table 2. List of published whitepapers**

Year	Author(s)	Title of the Whitepaper	Company
<b>2021</b>	Joar Jacobsson	<a href="#">Threat Modeling and Attack Simulations in the Energy Sector Analysis Process</a>	Foreseeti AB
<b>2022</b>	Anna Georgiadou	<a href="#">Security Behaviour Analysis</a>	National Technical University of Athens
<b>2022</b>	Joar Jacobsson, Ismail Butun, Robert	<a href="#">securiCAD Vulnerability Assessment Tool</a>	FORESEETI, KTH Royal

	Lagerström, Jose Cabus		Institute of Technology
<b>2022</b>	Anna Georgiadou	<a href="#">Automated Forensic Tool</a>	National Technical University of Athens
<b>2022</b>	Aras Arasilango	<a href="#">Homomorphic Encryption</a>	Tech Inspire Ltd
<b>2022</b>	Gianluca Serale, Giuseppe Carnevale, Stefania Sella, Alessandro Armellin, Emiliano Roggero	<a href="#">EnergyShield pilot at the electrical energy distribution grid of Turin</a>	IREN, IRETI, CSP
<b>2022</b>	Nikolay Palov, Magda Zafeiropoulou, Maria Atanasova	<a href="#">Implement the online field trials in Bulgaria</a>	Software Company Limited
<b>2022</b>	Christos Angelidis	<a href="#">Security Information and Event Management tool</a>	Konnektable Technologies
<b>2022</b>	Yisrael Gross, Rajarajan Muttukrishnan	<a href="#">Ammune DDoSM Tool for Anomaly Detection &amp; DDoS Mitigation</a>	L7 Defense, City University of London
<b>2022</b>	Hagai Galili	<a href="#">Anomaly Detection tool</a>	SIGA
<b>2022</b>	Iacob Crucianu, Lavinia Dincă, Ana- Maria Dumitrescu	<a href="#">EnergyShield toolkit</a>	SIMAVI

## 4. CONCLUSION

This deliverable presents the steps taken by EnergyShield Consortium partners to promote the results of EnergyShield project.

From setting up a strategy to reaching out standardization and policy bodies by direct (invitations to workshops) or indirect means (scientific articles, whitepapers) the consortium partners have contributed to increasing the visibility of EnergyShield project and to promoting the tools and concepts developed within the 3 years of implementation.

Organizing a Workshop with large audience, having the project and MAL mentioned in a Ofgem report are among the most remarkable results of this task.

Also, the number of events organized in collaboration with other H2020 project (12), the publication of 31 peer-reviewed articles and active participation in 4 clusters are worth mentioning.

## REFERENCES

- [COE01]** Convention on Cybercrime (ETS No. 185)  
<https://rm.coe.int/1680081561>
- [COM15]** Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee And The Committee of the Regions, The European Agenda on Security  
[https://ec.europa.eu/home-affairs/system/files/2020-09/eu\\_agenda\\_on\\_security\\_en\\_0.pdf](https://ec.europa.eu/home-affairs/system/files/2020-09/eu_agenda_on_security_en_0.pdf)
- [COM20]** Communication from the Commission to the European Parliament, The European Council, the Council, the European Economic and Social Committee and the Committee Of The Regions on the EU Security Union Strategy  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605>
- [CON14]** Council of the European Union (2014) EU Cyber Defence Policy Framework  
<https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf>
- [DOR20]** REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014  
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN>
- [ECA22]** European Court of Auditors (2002) Cybersecurity of EU institutions, bodies and agencies, Level of preparedness overall not commensurate with the threats,  
[https://www.eca.europa.eu/Lists/ECADocuments/SR22\\_05/SR\\_cyber\\_security-EU-institutions\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cyber_security-EU-institutions_EN.pdf)
- [ECD02]** Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) –  
<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021>
- [ECI08]** Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection  
<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114>
- [ECR04]** Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency,  
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

- [ENI19]** ENISA (2019) Standardisation in Support of the Cybersecurity Certification, Recommendations for European standardisation in relation to the Cybersecurity Act
- [ENI21]** ENISA (2021) Raising Awareness of Cybersecurity, A Key Element of National Cybersecurity Strategies, NOVEMBER 2021 <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>
- [EPC19]** Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881>
- [ESH11]** EnergyShield Consortium (2019) D1.1 Technical requirement specification
- [ESH12]** EnergyShield Consortium (2019), D1.2 Commercial requirement specification
- [ESH13]** EnergyShield Consortium (2019), D1.3 Regulatory requirement specification
- [ESH14]** EnergyShield Consortium (2019), D1.4 System architecture v1
- [ESH93]** EnergyShield Consortium (2019), D9.3 Data Management Plan v1
- [ESH10]** EnergyShield Consortium (2019), D10.1 H – Requirement No. 1
- [ESH22]** EnergyShield project website, resources page – <https://energy-shield.eu/resources/#1590131410501-e61fcba5-36aa>
- [ESH78]** EnergyShield Consortium (2022) D7.8 Collaboration report
- [EUP21]** European Parliament (2021) BRIEFING EU Legislation in Progress – The NIS2 Directive A high common level of cybersecurity in the EU [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
- [GDP16]** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [ICS19]** (ISC)<sup>2</sup>. (2019). Strategies for Building and Growing Strong Cybersecurity Teams – (ISC)<sup>2</sup>, Cybersecurity Workforce Study 2019. <https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study->

[2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482](https://www.iea.org/reports/covid-19-impact-on-electricity)

- [IEA20]** IEA (2020) Covid-19 impact on electricity, <https://www.iea.org/reports/covid-19-impact-on-electricity>
- [JOI13]** Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001>
- [JOI20]** Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN>
- [KEL10]** Michael Kelly , CEN/CENELEC/ETSI Joint Presidents' Group (2010) Standardization and the New Approach
- [NIS16]** Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>
- [NIS20]** Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN>
- [OPR22]** OpenAIRE repository, EnergyShieldporject, [https://explore.openaire.eu/search/project?projectId=corda\\_h2020::0e0cc382a8372db14444dc9b2137a050](https://explore.openaire.eu/search/project?projectId=corda_h2020::0e0cc382a8372db14444dc9b2137a050)
- [OFG21]** Ofgem (2021) Report on Analysing the cyber-security of industrial control systems, [https://www.ofgem.gov.uk/sites/default/files/2021-07/ICS\\_Attack\\_Graph%20trial%20report%20v1.0.pdf](https://www.ofgem.gov.uk/sites/default/files/2021-07/ICS_Attack_Graph%20trial%20report%20v1.0.pdf)
- [PSD15]** Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>
- [RCE20]** DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities, COM(2020) 829 final [https://ec.europa.eu/home-affairs/system/files/2020-12/15122020\\_proposal\\_directive\\_resilience\\_critical\\_entities\\_com-2020-829\\_en.pdf](https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf)

- [SKL19]** ENISA (2019) Cybersecurity Skills Development In The EU, The certification of cybersecurity degrees and ENISA's Higher Education Database - <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union>
- [SKL20]** COM(2020) 274, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, European Skills Agenda for sustainable competitiveness, social fairness and resilience <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0274&from=en>
- [TRE19]** University of Trento (2019) Governance Challenges for European CyberSecurity Policy: Stakeholders Views, EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe



## DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

---



[www.energy-shield.eu](http://www.energy-shield.eu)

