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

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

ENERGYSHIELD WORKSHOP

TRENDS, OPPORTUNITIES AND CHOICES IN DESIGNING A CYBER RESILIENT EPES INFRASTRUCTURE

FOLLOW-UP REPORT

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

1. EXECUTIVE SUMMARY AND AGENDA

EnergyShield Consortium has organized the European workshop **Trends, opportunities and choices in designing a cyber resilient EPES infrastructure** on the 15th 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.

The agenda featured four opening sessions followed by two consecutive panels (Table 1).

Table 1. Agenda

AGENDA – ENERGYSHIELD WORKSHOP 15/04/2021, 10.00 CEST	
Opening sessions	
Welcome and brief introduction of EnergyShield project	Otilia Bularca, SIMAVI
Recent policy developments in cybersecurity for critical infrastructure protection	Christian Wilk, EC
ENISA's activities in the energy sector	Konstantinos Moulinos, ENISA
Bridging the gap between EPES and cybersecurity	Dr. Venizelos Efthymiou, UCY
Combining MAL with safety & functional modelling	Chris Few, Ofgem UK
EnergyShield toolkit demonstration	Iacob Crucianu, SIMAVI; Joar Jacobsson, foreseeti; Anna Georgiadou, NTUA
PANEL 1	**PANEL 2**
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
Moderator: Tommy Wahlman, Swedish Energy Agency **Panellists:** • Daniela Bichir, SIMAVI • Javier Valiño, ATOS • Prof. David Wallom, Oxford e-Research Centre • Dr. Mihai PĂUN, CRE • Loris Piana, IREN Italy	**Moderator**: Monica Florea, SIMAVI **Panellists:** • Sarah Fluchs, admeritia GmbH • Dr. Ing. Matthias Rohr, PSI • Dan Cîmpean, CERT-RO • Massimiliano Masi, Autostrade per l'Italia • Matteo Merialdo, RHEA Group

2. DISSEMINATION & COMMUNICATION STARTEGY

EnergyShield workshop **Trends, opportunities and choices in designing a cyber resilient EPES infrastructure** was announced on the 16th of May via EnergyShield website, promoted via Twitter, via a LinkedIn event and accompanied the message with the video presentation of Energy Shield project. Following the announcement, consortium partners started disseminating the event via own channels (websites or social media account).

Before publishing the full program, the organisers contacted five large H2020 projects and asked them to endorse the event via own channels to reach out all the relevant stakeholders. BRIDGE, CYBERWATCHING.EU, PANTERA, INTEGRIDY and ECHO projects have kindly supported the promotion of the event and increased its overall visibility.

2.1. AUDIENCE TARGETED AND REACHED

Via own website and social media channels of Consortium partners the news about the event reached audience from similar H2020 projects.

The twitter account was used as the main communication channel since EnergyShield already had a good presence on this social media channel. During the promotion of the event, Energy Shield gained over 50 followers and a high number of impressions as seen in the figures below.

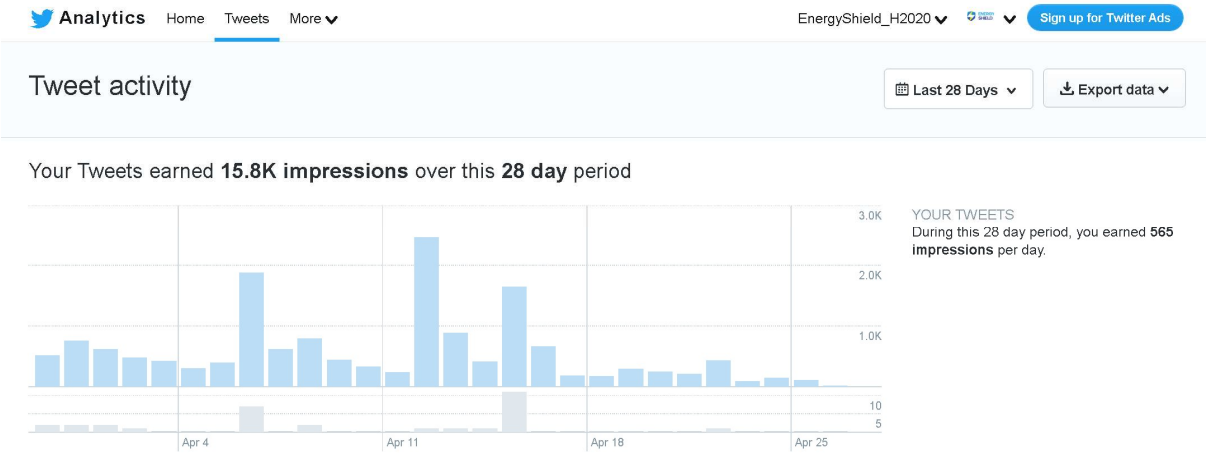


Figure 1. Twitter report from 27th of April 2021

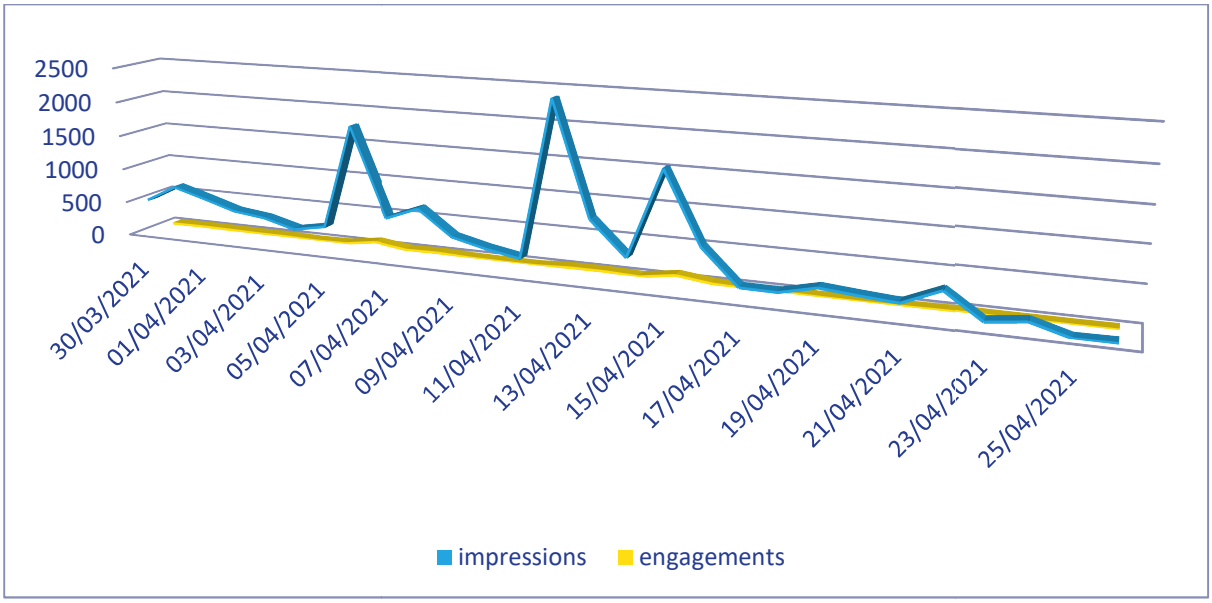


Figure 2. 28 days report. Evolution of impressions as and engagements

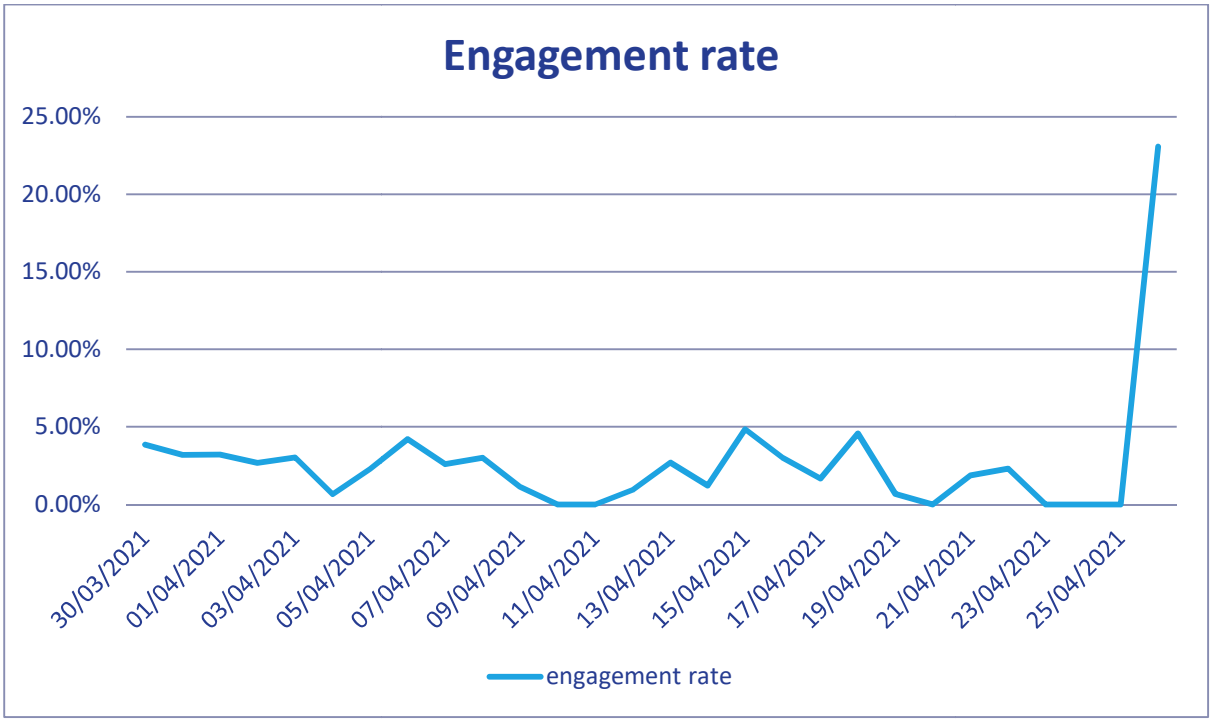


Figure 3. 28 days report. Engagement rate evolution

Another important observation related to twitter that is worth mentioning is that the campaign set a positive trend in terms of engagements.

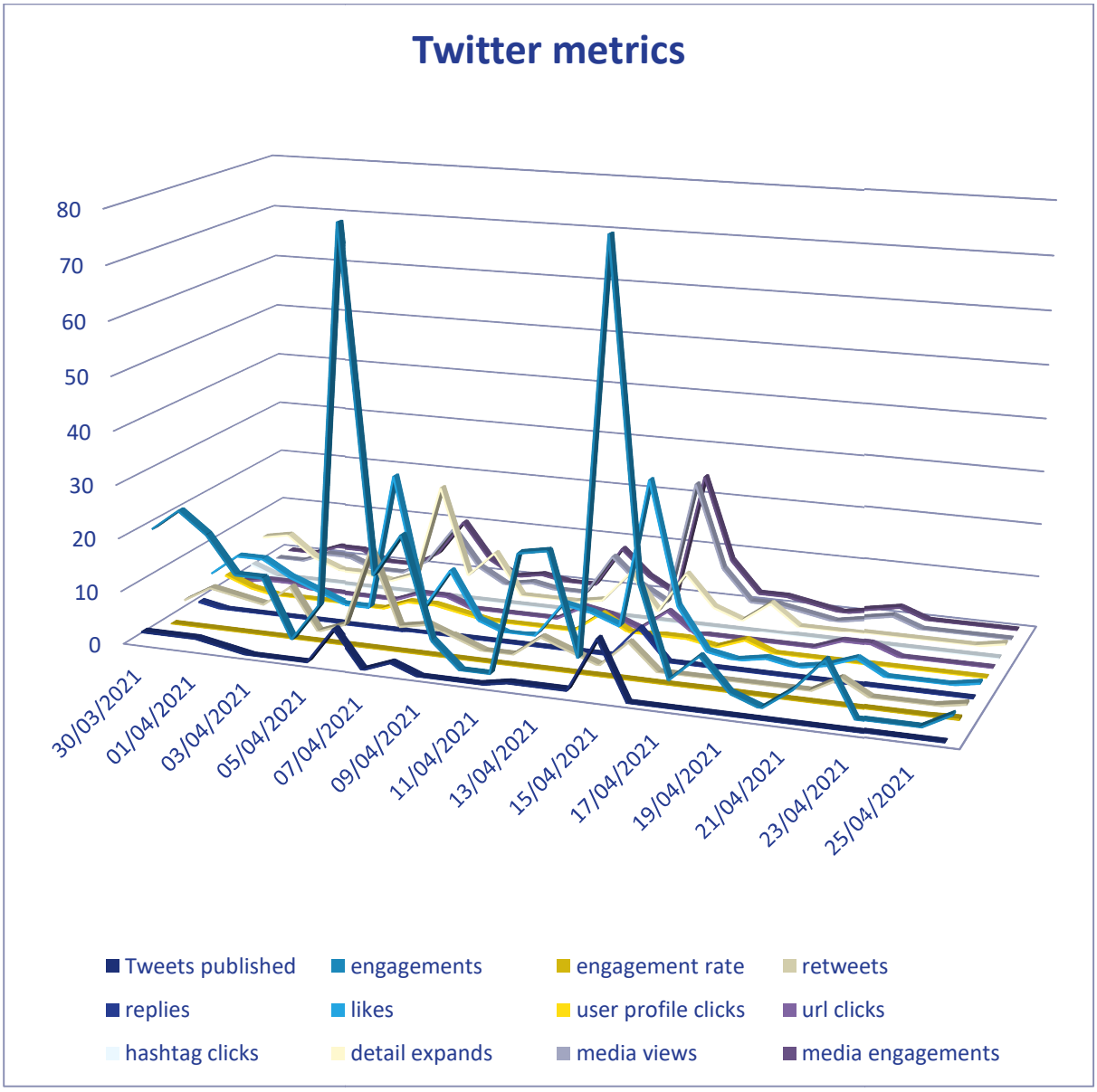


Figure 4. 28 days report. Evolution of twitter metrics

Another way to reach out to a broader audience was by publishing articles on the project's website, on SIMAVI website and social media, and in Romanian newspapers. With these articles details about the event, registration and possibilities to engage and contribute prior to the event were provided (Panel 1 and Panel 2 dedicated surveys that are presented and analysed later on in this report)

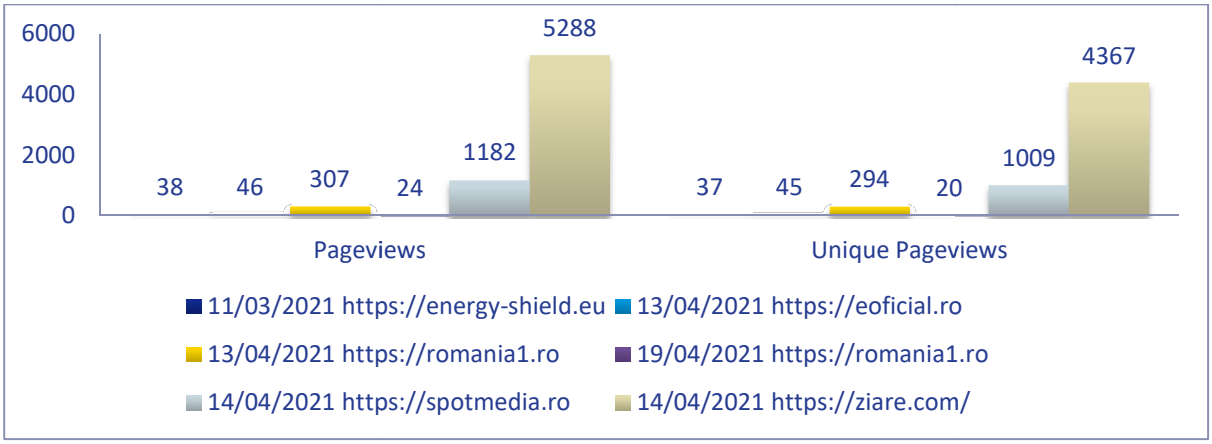


Figure 5. Facebook campaigns impact

Another way of reaching the audience was via Facebook campaigns, both via SIMAVI's account and via local media channels. The audience targeted for these campaigns was higher education, interested in energy and cybersecurity.

The graphs below show the number of persons reached together with related impressions and engagements.

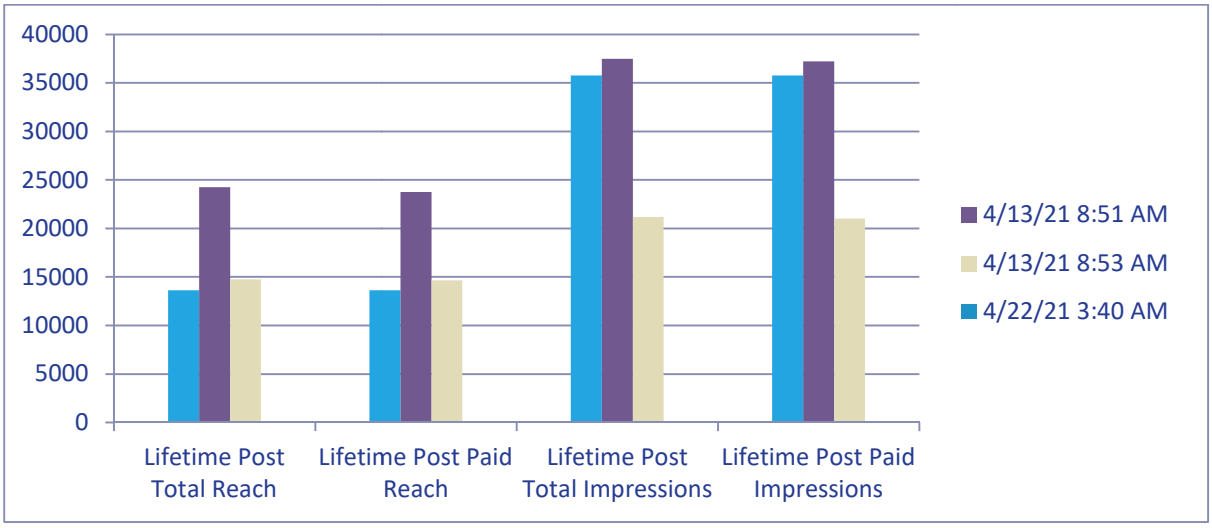


Figure 6. Paid Facebook campaigns outcome

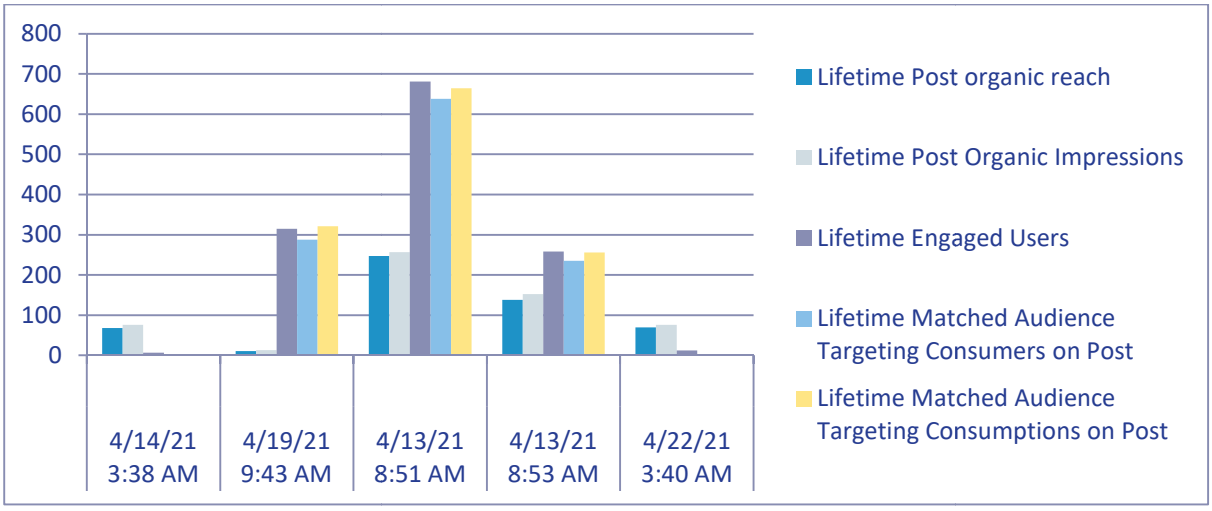
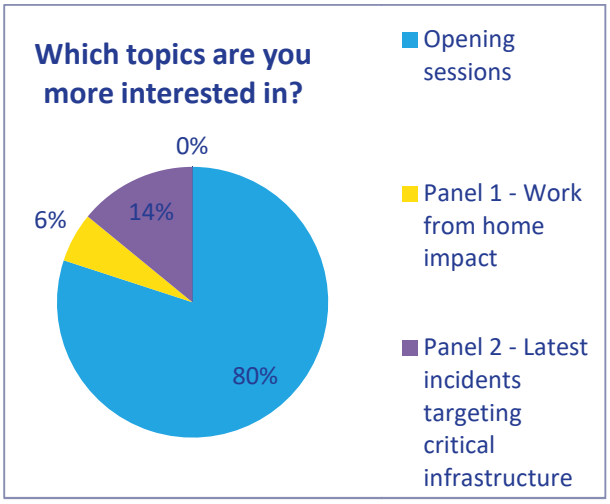
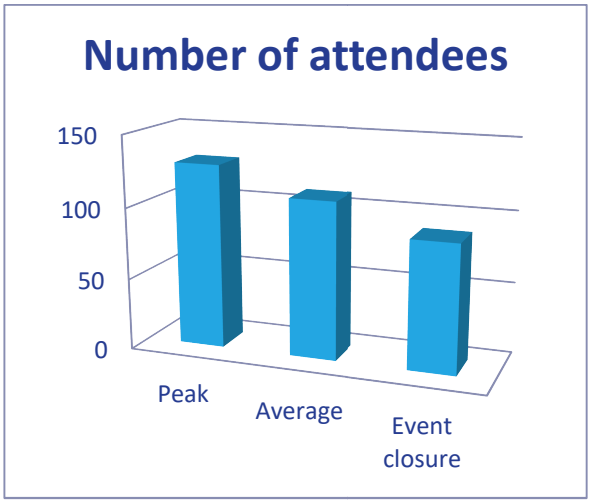


Figure 7. Organic reach via Facebook

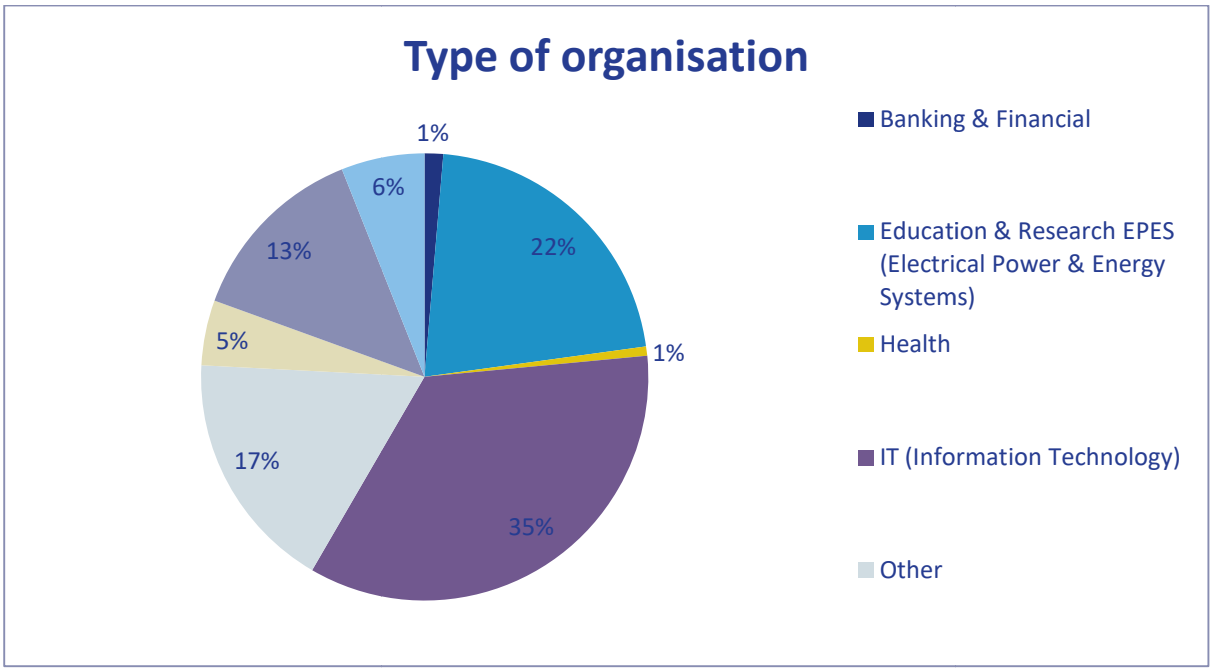
3. WORKSHOP ATTENDEES

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





Considering the type of organisation, most of the attendees came from IT and EPES industry.



4. WORKSHOP OUTCOMES

Different aspects of cyber security in EPES sector including standardization efforts and policy updates were addressed during the opening sessions leaded 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 latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies.

4.1. OPENING SESSIONS

4.1.1. ENERGYSHIELD PROJECT PRESENTATION

Otilia Bularca, Project Manager at SIMAVI shortly presented the objectives of EnergyShield project.

EnergyShield is the short name of the project called - Integrated Cyber security Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures – is an Innovation Action initiative under the topic - cyber security in the Electrical Power and Energy System (EPES).

The goal of the project is to capture the needs of Electrical Power and Energy System (EPES) operators and combine the latest technologies for vulnerability assessment, supervision, and protection to draft a defensive toolkit.

The project started in 2019 on the first of July and is planned to reach its objectives by 2022 – end of June.

This project is implemented by a Consortium of 18 partners from 9 different EU Member States and Associated Countries as follows:

- 2 large industrial partners (SIMAVI and PSI Germany),
- 6 innovative SMEs SIGA and L7Defence from Israel, foreseeti from Sweden, Konnektable form Ireland and Software Company from Bulgaria
- 3 academic research organizations: National Technical University of Athens, City University of London, KTH Royal Institute of Technology Stockholm
- 7 practitioners covering the entire EPES value chain: IREN – DSO in Italy, CEZ – DSO in Bulgaria, ESO – TSO in Bulgaria, Kogen Zagore – gas turbine power plant, VETS hydropower generator MIG23- energy service providers and DIL real estate company.

EnergyShield aims at:

- Adapting and improving available building tools (assessment, monitoring & protection, remediation) in order to support the needs of the Electrical Power and Energy System (EPES) sector
- Integration of the improved cybersecurity tools in a holistic solution with assessment, monitoring/protection and learning/sharing capabilities that work synergistically
- Validating the practical value of the EnergyShield toolkit in demonstrations involving EPES stakeholders
- Developing best practices, guidelines and methodologies supporting the deployment of the solution and encourage widespread adoption of the project results in the EPES sector

Energy Shield toolkit includes 3 categories of tools:

- Assessment tools: Vulnerability Assessment (foreseeti), Security Behaviour Analysis (National Technical University of Athens)
- Monitoring and protection tools Anomaly detection (SIGA) and Distributed Denial of service Mitigation (L7Defecne)
- Learning and management tools (Security Information and Event Management, Konnektable)

These tools will be used to demonstrate:

- scale attacks - Targeting specific organization & Meant to prevent them from conducting business normally
- Large scale attacks - Targeting the entire EPES value chain & Meant to take down the energy supply services at regional or country level

Energy Shield project addressees small-scale and large-scale disruption attack scenarios with an integrated toolkit validated in a live cyber-defence exercise.

End users covering EPES value chain: Generators, DSOs, TSOs, aggregators, prosumers will facilitate two demonstrations in Bulgaria and Italy.

The aim of the BG pilot is to study the cascading effects of cyberattacks throughout the value chain, while the Italian pilot performs the feasibility study (and possible offline trial on a dedicated, simulation area of the networks control systems, if feasible) will be set on Turin DSO network

In terms of innovation the BG pilot proposes mitigation of cyber-attacks and data breaches, while the IT pilot assesses the possibility to test an integrated suite of cyber security tools.

The expected outcomes will be an online, full end-to-end demonstrator in Bulgaria and an offline trial in Italy.

The Energy Shield **toolkit** is organized in several shelves and contains hardware and software components as well as communication ports. Details are presented in the dedicated section.

4.1.2. RECENT POLICY DEVELOPMENTS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION

Christian Wilk, Research Programme Administrator, at European Research Executive Agency of the European Commission briefed the attendees on recent policy developments in cybersecurity for critical infrastructure protection. The European Commission's priorities in cybersecurity were accompanied by a short introduction of two next upcoming directives: NIS 2.0 provision and Critical Infrastructure Protection directive. Under the Directive on the resilience of critical entities, the alignment of those two policies was identified.

European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) that will be located on Bucharest is currently under preparation and it is expected to be operational by the end of 2021. This centre will manage two cybersecurity related Work Programmes: Horizon Europe Cluster 3 Civil Security for Society and Digital Europe Programme

4.1.3. ENISA'S ACTIVITIES IN THE ENERGY SECTOR

Konstantinos Moulinos, expert at ENISA (European Union Agency for Cybersecurity) briefed the audience on the activities ENISA is running within energy sector. ENISA is active in different cybersecurity related topics and collaborated with different EU institutions like DG ENER, ACER (Agency for the Cooperation of Energy Regulators), ENTSO-E, E.DSO.

It has been observed that lately the attacks against power grids have increased and the necessity of having a more harmonized security requirements and incident reporting was identified. This is taken over by the reviewed NISD, CER (Directive on the resilience of critical entities) and the Network code cybersecurity for the electricity and a regulation on Artificial Intelligence will soon be released.

A series of challenges were identified while drafting and reviewing the directives mentioned above. It was also mentioned the collaboration with the private sector, gaps in the governance, crisis coordination gaps, not considered dependencies with other sectors. Another thing that is necessary to be considered in drafting policies is the technological advancement and their capacity of changing the threat landscape.

A comprehensive body of regulations in cybersecurity and energy is available and ENISA is continuously raising awareness, organising exercises and supporting information and knowledge sharing.

4.1.4. BRIDGING THE GAP BETWEEN EPES AND CYBERSECURITY

Dr Venizelos Efthymiou, Chairman of the Research Centre Sustainable Energy of UCY shared challenges related to the digitisation process of EPES.

Starting from the objectives of the EnergyShield project and the special needs of EPES, new factors emerging in the digitalization process of EPES are listed:

- Customer involvements and possible disruptive new business models that could emerge from this involvement

- Greater attention to sector coupling and then correspondingly to the convergence of Smart Energy and Smart Cities and Communities
- New concepts and technologies that are emerging also at the physical layers thanks to a greater role played by electronics in the new digital energy system.

The Distributed Flexibility Marketplace involved all relevant actors and calls for meaningful communication and data exchange. The future of policies in cybersecurity should consider society and energy users awareness, Quantum cryptography, 5G, robotics and autonomous vehicles as they carry a disruptive potential.

4.1.5. COMBINING MAL WITH SAFETY & FUNCTIONAL MODELLING

Then, Chris Few, Head of cyber research and development at the UK Ofgem talked about Combining the Meta Attack Language with safety & functional modelling.

Starting from the capabilities, skills and access to system that is needed to cause a hazardous event, a combination of control signals and control actions is assessed, and potential attacks paths are presented. MAL (Meta Attack Language) enables cyber threat modelling and attack simulations of specific environments – a power grid, a vehicle platform or a particular cloud infrastructure.

4.1.6. ENERGYSHIELD TOOLKIT DEMONSTRATION

This session was completed by the demonstration of EnergyShield toolkit done by Iacob Crucianu, Technical Leader at SIMAVI, while assessment tools were demonstrated by Anna Georgiadou from NTUA and Joar Jacobsson from Foreseeti.

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

The common software platform presented below has five different deployment areas:

- Assessment provides information on most critical attack vectors. It includes Vulnerability Assessment (VA) modules and Security Behaviour Analysis (SBA) tools.
- Monitoring and protection provide early warning on incoming attacks and malware. It includes Anomaly Detection modules and Distributed Denial of Service mitigation modules.
- Learning and sharing collects information from all the other modules and creates plans and instruction which refers to SIEM.
- Framework components are supporting components used by the whole deployment.
- Deployment system. It implements Continuous Integration/Continuous Deployment (CI/CD) mechanism.

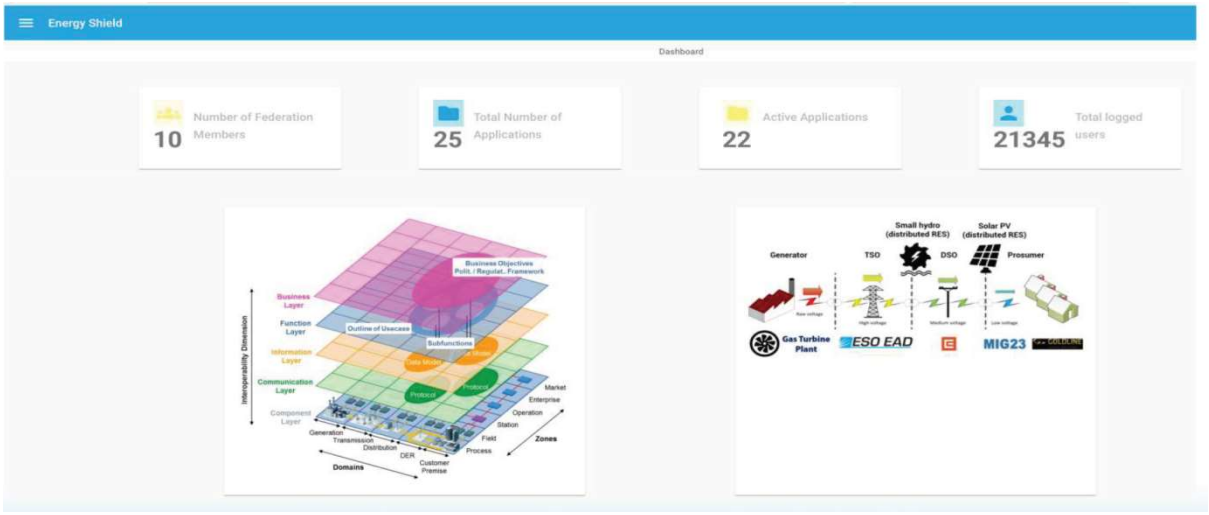


Figure 8. EnergyShield portal

EnergyShield portal is the place where there is a single point of access to the toolkit. It displays the data available from individual components, considering that the components might be deployed in the same place as the portal (common framework) or they are deployed on pilot premises, from where, information is offered via a secured line and according to the security policy implemented by a pilot. The Portal is enabled to take advantage of using the outputs of components running as services (SAAS – Software as a service).

There is no direct interaction between the common platform or the portal with the environment where the Operational System is working.

There are communication links between the technical components of the toolkit deployed on premises, and the common framework and the portal.

Two of the EnergyShield tools were demonstrated following the presentation of the Portal.

The **Vulnerability Assessment tool** is based on foreseeti's securiCAD Enterprise tool which, during the project, has been made to the Electrical Power and Energy Systems (EPES) domain.

This extension is based on the Meta Attack Language (MAL), which is a framework for creating domain-specific threat modelling languages. Older versions of securiCAD had a hard-coded general IT security language that offered low flexibility and little energy domain support. With MAL support in securiCAD, the energy domain can now be represented much more natural and with greater ease.

The newly developed threat modelling and attack simulation language for the energy sector, we call it EPESLang, is designed using the MAL framework. It contains three main parts; i) core IT (coreLang), ii) industrial control systems technology (icsLang), and iii) substation configuration technology (sclLang). All three sub-language have been newly developed during EnergyShield with EnergyShield partners.

In addition to the EPES domain specific analysis capability, a large focus has been placed on the usability, performance and deployment flexibility of the VA tool for a

good fit into the EnergyShield toolkit which may face users of varying skill levels as well as different deployment modes and usage patterns.

The EnergyShield **Security Culture Framework and Tool** developed by NTUA aims to assess and map the socio-cultural behaviour of an organisation's workforce to cyberthreats. The tool is designed and implemented using a holistic approach to easily adapt and adjust to any business domain and, within the context of project, it is adapted to and will be validated by the EPES sector.

The main purpose of the cyber-security culture framework is to assess and evaluate the current security readiness of an organization's workforce. Having conducted a thorough review of the most commonly used security frameworks and pinpointed their gaps, weaknesses and overlaps, NTUA have identified core security human related elements and classified them by constructing a domain agnostic security model. It consists of 10 different security dimensions analysed into 52 domains assessed by more than 500 controls examined under two different pillars: organisational and individual

4.2. PANEL DISCUSSION

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.

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 la address for the follow-up report.

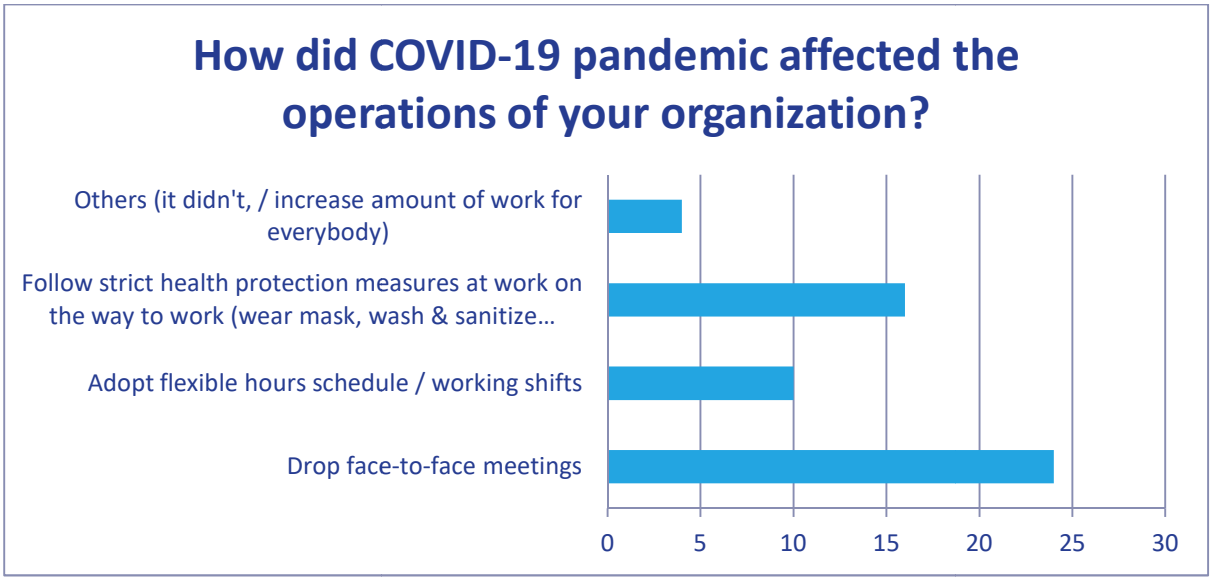
4.2.1. PANEL 1 - WORK FROM HOME IMPACT ON THE ENERGY AND IT INFRASTRUCTURES

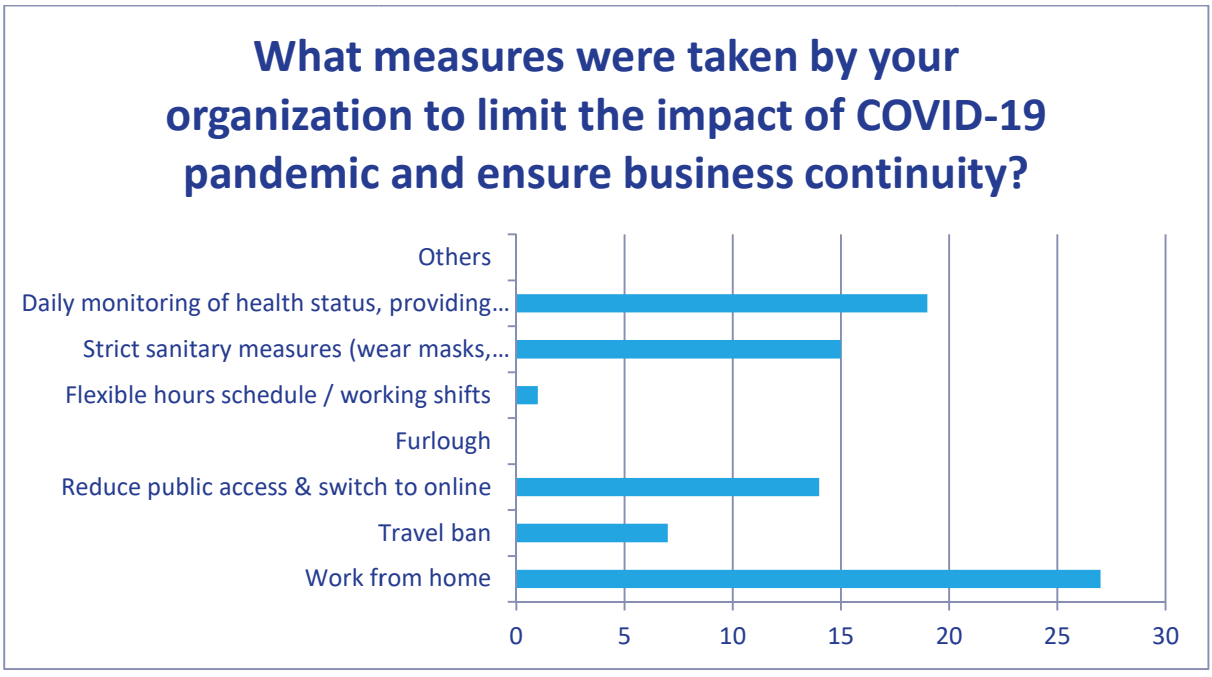
The first panel approaches the effects work from home had on energy and IT infrastructures and is moderated by Tommy Wahlman, Programme Manager, The Swedish Energy Agency.

The panellists were Daniela Bichir, *SIMAVI,* Javier Valiño, *ATOS,* Prof. David Wallom, Oxford e- Research Centre, Dr. Mihai PĂUN, *Romanian Energy Center and* Loris Piana, *IREN Italy*

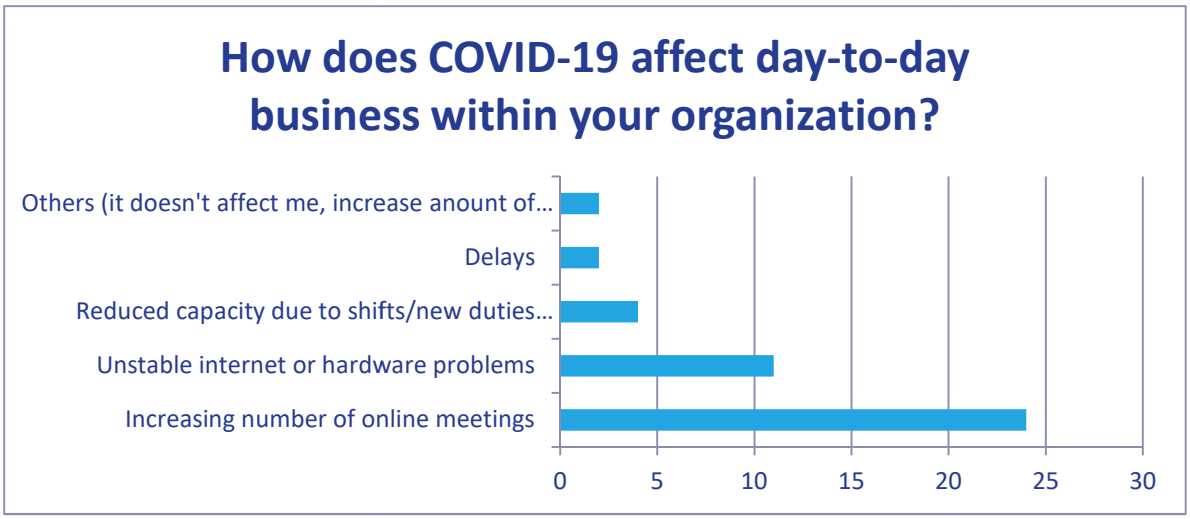
The 4 questions proposed survey for this panel gathered interesting insights. The results show an overwhelming shift to work from home and an increased interest in health monitoring. On top of these the reality of home working brings a high number of online meetings and concerns related to morale and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

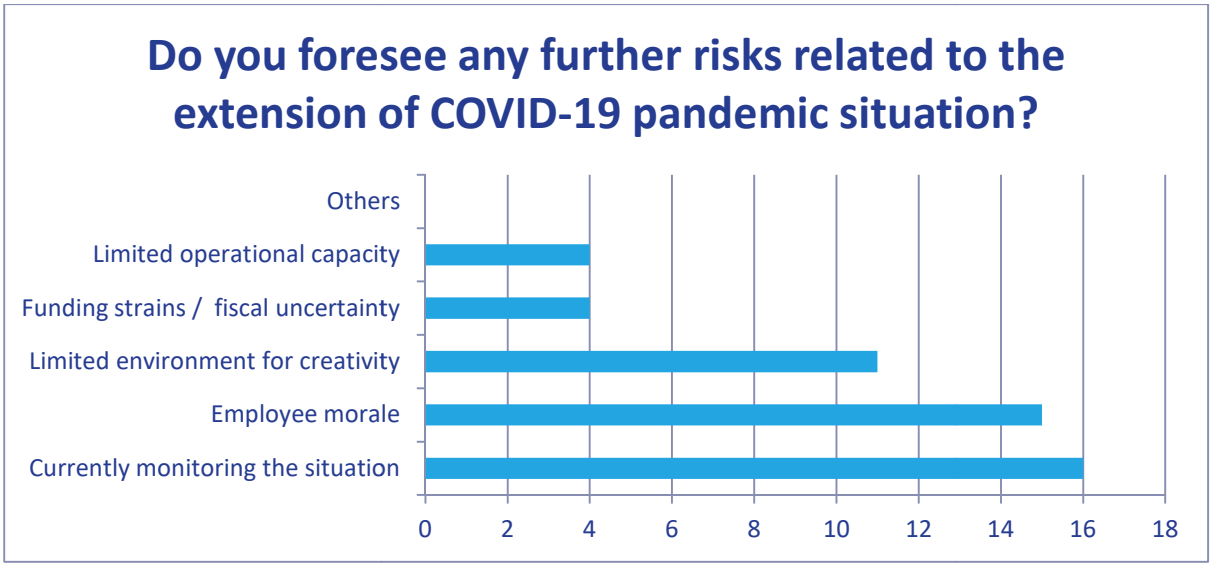
The graphs below show how did COVID-19 reshaped business relationship and which measures were preferred to ensure safety.

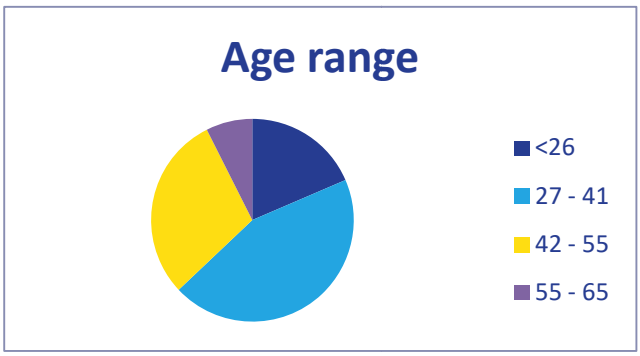


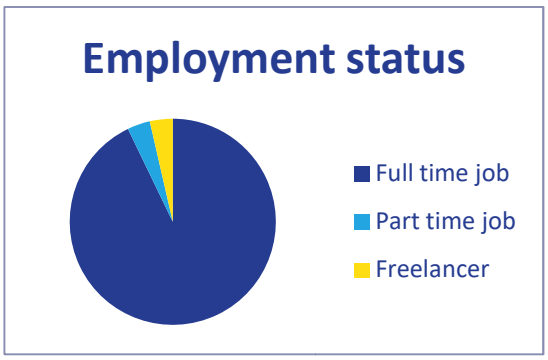


The survey answers show that working from home also has an impact on daily activities. As seen in the following figures the number of the online meeting increased and concerns related to creativity and morale were raised.









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 o 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 also to motivate their employees to be happy.
- Remote working in academia might be difficult for young researchers
- Remote working & large videoconferences mean an increase 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 do 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 definitely 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 asses 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 released I 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

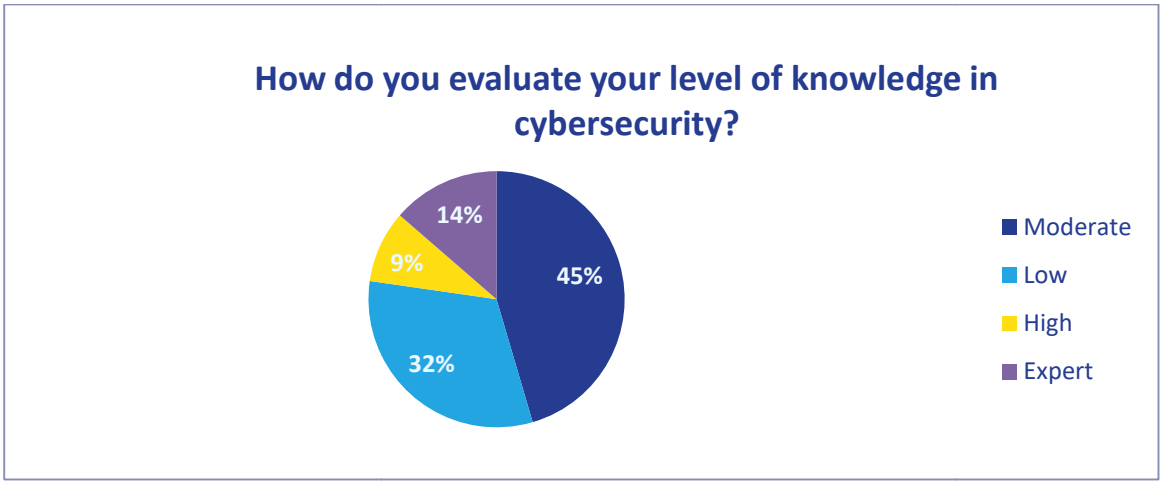
- Opportunities could be connected to happy and productive workers if we could supply them the appropriate devices
- In this case one size does not fit all as not everyone can actually work from home
- Work organisation needs to be redesigned and online fatigue is mentioned and boarding and coaching are challenging perspective

4.2.2. PANEL 2 - LATEST INCIDENTS TARGETING CRITICAL INFRASTRUCTURE AND THEIR IMPACT ON DESIGNING NEW TECHNOLOGIES, BUSINESS MODELS AND POLICIES

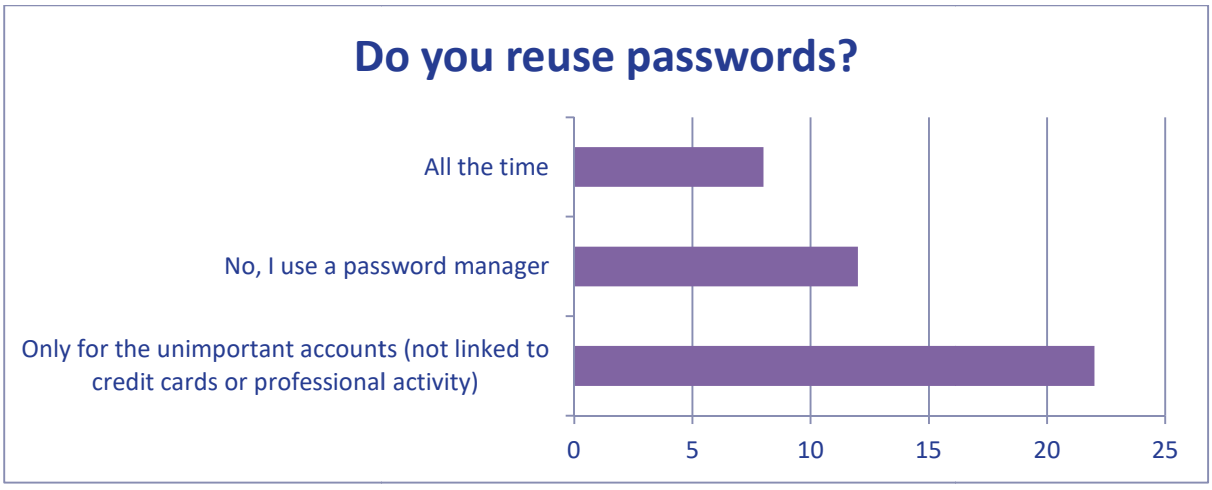
The second one addresses the latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies. This panel is moderated by Dr. Monica Florea, Head of Unit EU projects and SIMAVI. The panellists were Sarah Fluchs, *admeritia GmbH,* Dr. Ing. Matthias Rohr, *PSI,* Dan Cîmpean, *CERT-RO,* Massimiliano Masi, *Autostrade per l'Italia and* Matteo Merialdo, *RHEA Group*

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.

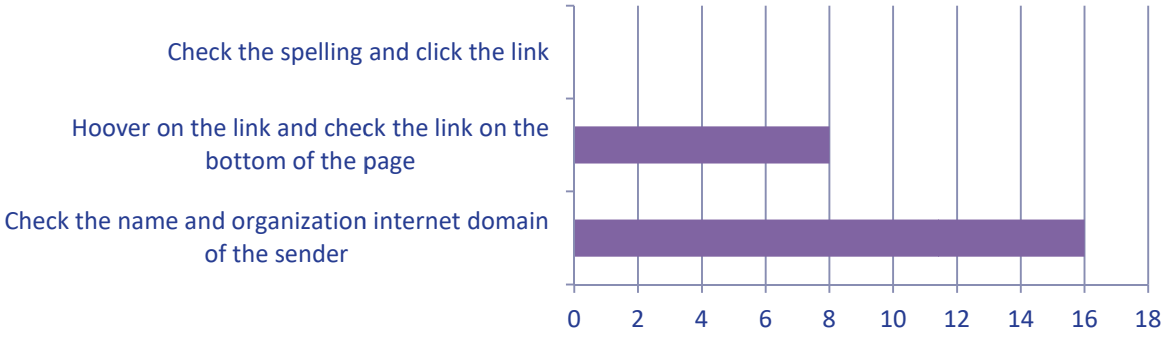
To find out more about user's cyber-awareness the organisers have launched a 5 questions survey. The results show a high degree of cyber-awareness, but also show vulnerabilities and negligence when it comes to having info at hand (e.g. keeping browsing history and using USB drives.


How do you evaluate your level of knowledge in cybersecurity?
14%
9%
45%
32%
Moderate
Low
High
Expert

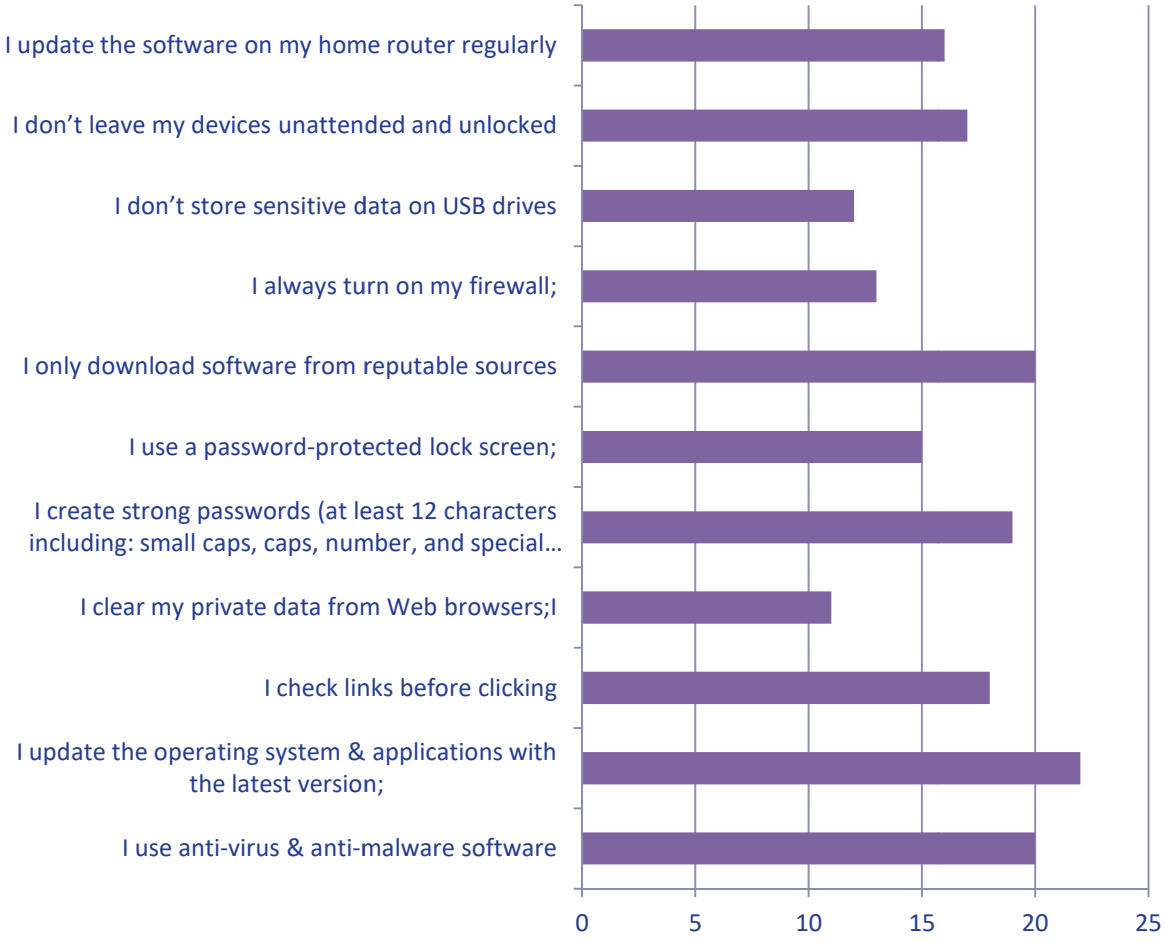

How do you protect your important accounts (e.g. e-mail, social media, bank)
Password manager
Complex password
Second factor authentication;
0
5
10
15
20
25

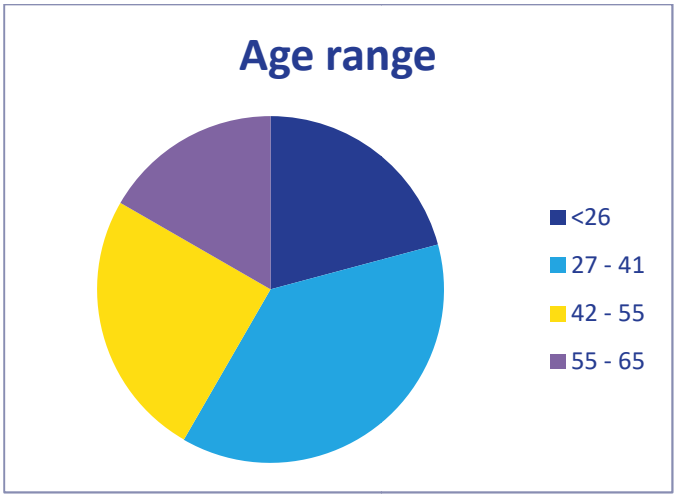

Do you reuse passwords?
All the time
No, I use a password manager
Only for the unimportant accounts (not linked to credit cards or professional activity)
0
5
10
15
20
25

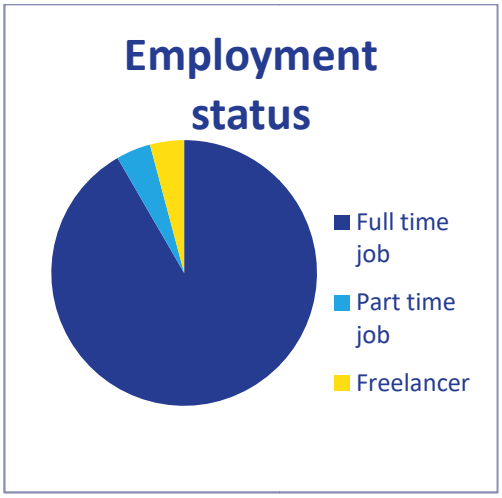
What do you do to identify possible phishing e-mails?



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:

a) Do you consider supply chain as Critical Infrastructure?
b) How to design the systems to avoid spreading the compromise from IT to OT infrastructure?
c) Trends to be considered in designing new technologies and business models that help increasing the security level of CIs
d) 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.

Questions from chat:

Question from participant: How can we make use of the outcomes of this project? in terms of work done but also tools, visualizations etc?

Reply in chat: the scientific output can be found on our website; you could also reach out to us and we can see to whom you need to talk to

Question from participant: Is there anything in the works on the European Level to at least the FOSS-Code Base and make the results public domain?

Reply in chat: I don't know of anything (coordinated) like that, but it would be a great initiative.

5. AKNOWLEDGEMENT

The event is part of the Energy Shield project dissemination and communication activities (a brief introduction of the project will follow) and its organization was leaded by 3 consortium partners: SIMAVI – the coordinator of the project, KTH in Sweden, – leader of the communication and dissemination activities and NTUA leading the collaboration activities within the project.

The persons involved throughout the process of organizing this event are: Otilia Bularca – Project Manager at SIMAVI, Ariadni Michalitsi-Psarrou - a senior research engineer in the Decision Support Systems Laboratory in the School of Electrical and Computer Engineering at the National Technical University of Athens (NTUA), Simon Hacks - Software Systems Architecture and Security group in the Network and Systems Engineering at KTH Royal Institute of Technology and Lavinia Dincă – cybersecurity expert at SIMAVI, Ana-Maria Dumitrescu – senior lecturer at Politehnica University of Bucharest Faculty of Electrical Engineering, and collaborator at SIMAVI.

Special thanks to the speakers, panellists, and moderators and all 135 attendees.

Looking forward to seeing you in other events!

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID

www.energy-shield.eu