



EUROPEAN NETWORK OF CYBERSECURITY  
CENTRES AND COMPETENCE HUB FOR  
INNOVATION AND OPERATIONS

# Newsletter

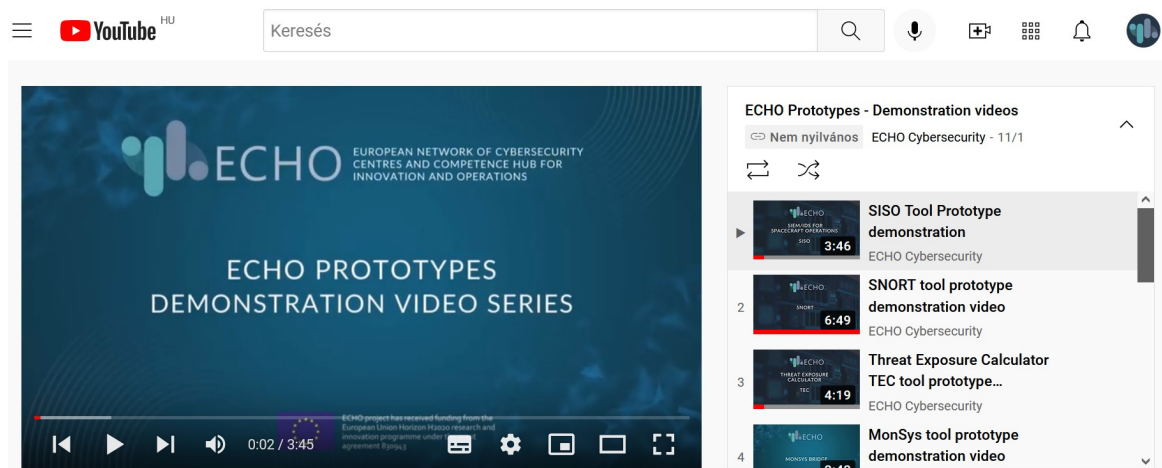
## EARLY PROTOTYPE TOOLS BY ECHO ARE AVAILABLE!

### The vision

In line with the needs of Work Package 4 (Inter-sector Technology Roadmaps) of the ECHO project, Task 4.3 tries to solve the most pressing cybersecurity needs by developing a set of innovative software solutions **addressing a variety of inter-sector and transversal cybersecurity challenges**.

In that frame, task 4.3 “Early prototypes selection, research and development” focuses on the selection and subsequent analysis and development of **early prototype tools** addressing emerging cybersecurity challenges and covering several high priority areas such as healthcare, maritime, energy, space etc. The selected prototypes will not only serve as a source of technology innovation but also as a mean of cybersecurity education and training towards achieving the research goals of the ECHO project in improving the proactive cyber defence of the European Union.

**We are happy to announce that the demonstration videos of the prototype tools are available on ECHO's YouTube channel!**



## UNDERSTANDING EUROPEAN CYBERSECURITY HR RECRUITMENT PROCESSES

**A collaboration between the European Cyber Security Organisation (ECSO) and the European Cybersecurity Competence Network Pilot projects (extract)**

The overall purpose of the survey was to assess how organisations in Europe currently address the recruitment of cybersecurity specialists, given the well-known shortage of cybersecurity specialists.

Based on the data collected and the analysis conducted, the following recommendations are made:

1. The demand for an EU Cyber HR Toolkit is justified
2. Support the creation of an HR cyber knowledge pool
3. There is a need for new approaches to competence building
4. There is a need for European data
5. Integration of synergies and efforts is a must

The data for the “Understanding European Cybersecurity HR Recruitment Processes” report was gathered through an online survey, which took place from April until the end of May 2021.

The challenges and issues faced by stakeholders in hiring and retaining cybersecurity professionals and building strong teams of cyber-defenders are many, complex and interconnected. The expectations and attitudes of the employers sometimes exceed the real qualification and proficiency levels of the graduates and there are very limited options for HR professionals to assess this. In the end, the discrepancy between the expectations and the actual cybersecurity competence landscape along with the capabilities of (candidate) employees challenges the capabilities of the HR department, as it cannot complement the process as professionally and effectively as in the case of other professional domains. A more intensive collaboration between industry and academia, not only in the identification and definition of the requirements and objectives, but also joint investments in internship programs, equipment of practical laboratories, work-based learning, tools for hands-on learning, etc. is very necessary and urgent. These investments shall focus not just on the cybersecurity specific competence building, but also contribute to the HR professionals’ better understanding and cyber workforce related situational awareness. There is an urgent need to overstep the biases of the cybersecurity skills shortage and focus on addressing the challenge by providing overarching solutions. Defining the ecosystem and stakeholders is still an ongoing process and while a lot of work has been done in the domain, the ecosystem and an effective collaboration mechanism still needs to be established.

For the details of results, please find the report here: <https://bit.ly/3ec8dha>

## ECHO EDUCATIONAL PROGRAMMES



### CYBER THREAT INTELLIGENCE IN THE INCIDENT RESPONSE CYCLE ON THE BOARD OF MODERN SHIPS

The ECHO Spring Seminar programme was intended to provide the participants with basic understanding of cyber security concepts and some specific implications in the maritime industry, especially latest technology and operational developments. In addition to the theoretical overview of the methods and tools that support the incident response and analysis, the students could discuss the indicators of compromise of a cyber-attack against a modern ship and processes on the restoring the navigation system after compromising the communications leveraging the ECHO Federated Cyber Range.



The first workshop of ECHO “SERVERS AND CYBER-THREATS” was held on 04/19/2022, which was dedicated to a server protection cybersecurity solution.

The workshop introduced the participants to a combination of tools for secure exchange of information, identification of vulnerabilities in complex systems, and network-based intrusion detection for server applications.

The ECHO team performed a cyber-penetration against one server of a hospital to check its reliability and suggested to the system designer a more secure configuration of the server infrastructure. Moreover, a software that is able to detect cyber intrusions on the network layer was also tested during the demonstration.

More information about the event: <https://echonetwork.eu/echo-workshop-server-and-cyber-threats>

**IF YOU ARE INTERESTED IN DEMONSTRATIONS OF ECHO'S  
PROTOTYPE TOOLS, FOLLOW US AND CHECK OUR WEBSITE  
FOR THE DATES OF THE NEXT WORKSHOPS!**

# ECHO EVENT



## INVITATION

The ECHO project (European network of Cybersecurity centres and competence Hub for innovation and Operations) would like to invite you to attend the

### ***ECHO Early Warning System (E-EWS) use for reference library and in cyber incident coordination response Demonstration workshop.***

**This workshop event will be held online on Wed 18th of May 2022 at 09.00 - 11.30 CET.**

These are the first two of a series of five demonstration cases that are shown in workshops that display through relevant use cases the capabilities of the developed ECHO technology roadmaps. These are the ECHO Early Warning System, ECHO Federated Cyber Range and inter-sector prototypes, in conjunction with other ECHO assets: ECHO Cyber Skills Framework and ECHO Cyber Certification Scheme.

The program of the “*E-EWS use for reference library and for cyber incident coordination response*” Demonstration workshop is:

09.00 Welcome and opening remarks

09.10 Presentation E-EWS use (reference library / cyber incident coordination response)

09.30 Demonstration E-EWS use (reference library / cyber incident coordination r esponse)

10.45 Discussion and feedback

11.30 Closing of event

**Registration for this event is extended to May 4th, 2022 at:**

**<https://zflut9l8ruw.typeform.com/to/dfwGW7pN>**

**Read more about the background of the workshop [HERE](#)**

## MEET ECHO'S EXPERT - EWA KONIECZNA

VisionSpace Technologies GmbH



### **How would you introduce yourself and your role within the ECHO Project?**

I studied international relations at the University of Economics in Prague, worked in finance, currently a project manager at VisionSpace, Quality and Data Management Coordinator for ECHO.

### **Why do you think cybersecurity is important nowadays?**

Already centuries ago, leaders realised that they needed a workforce, resources, capital, and information to grow their power. Nowadays, especially, we can see what effect the overflow of information, inadequate prioritisation of the information, blockage of the information, its manipulation or leakage of information can have. Information holds power, and cybersecurity holds the key to it.

### **What surprised you the most about working in ECHO?**

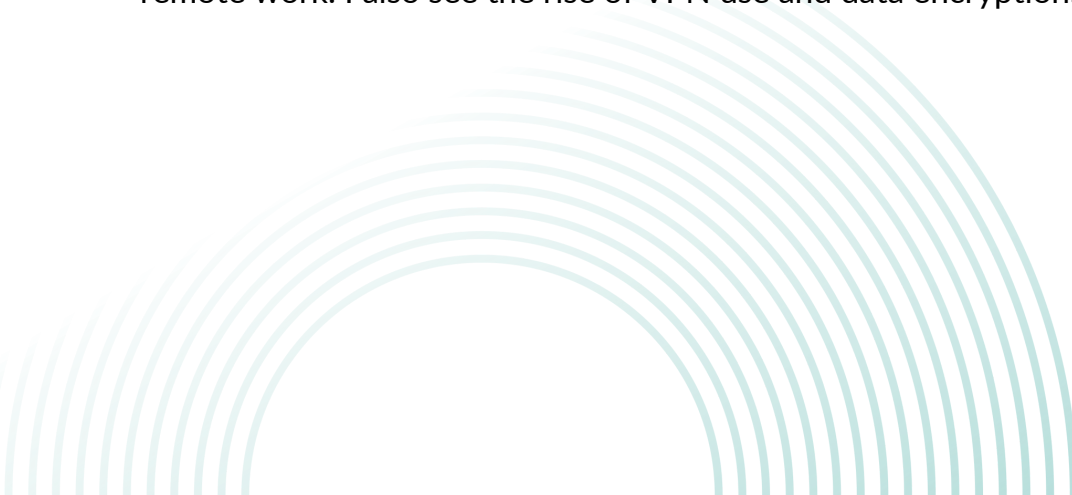
The range of expertise is very wide. I need to admit that I am also quite impressed by the coordination of activities. ECHO is a very complex and ambitious project involving now over forty partners and collaborators. Yet, everything comes together in a very logical manner. Throughout this year we should transition this cooperation from the project-based to collaborative network and I cannot wait to see how it turns out.

### **Is there an achievement or contribution that you are most proud of? Why?**

As a QDMC, I feel responsible for the overall quality of the project's output. I am proud every time our technical solutions, documents or other outputs receive positive feedback.

### **In your opinion, what will be the biggest lesson of the Covid-19 epidemic in terms of cyber security?**

I expect organisations to adapt security policies and update their equipment to allow safe remote work. I also see the rise of VPN use and data encryption.





## ECHO NEWS

### The ECHO Ideathon event on the ECHO-Federated Cyber Range exploitation took place on 10th March 2022.

The ECHO Hackathon event on the ECHO-Federated Cyber Range exploitation took place on 28th March 2022. The aim of this session was to generate innovative ideas for the development of the exploitation strategy of the ECHO – Federated Cyber Range.

A group of 30 participants from the ECHO consortium joined the discussion touching upon the different aspects of the E-FCR's business model and how it shall be governed in order to enter the market. Moreover, participants discussed the prospective use of the E-FCR to offer their services and the potential future collaborations that could be done.

Many diverse and innovative concepts and ideas were shared by the participants, bringing the project closer to the exploitation of its results.

### ABOUT ECHO FEDERATED CYBER RANGE

The main objective of ECHO is to strengthen the proactive cyber defence of the European Union, enhancing Europe's technological sovereignty through effective and efficient multi-sector and multi-domain collaboration.

**The ECHO Federated Cyber Range (E-FCR)** – provides realistic environments for conducting experimentation, exercises, research and prototype testing, enables the combination of multiple scenarios from different content providers, and a focus point for training and expertise.

ECHO intends to raise awareness of the need for cybersecurity amongst EU citizens and better-inform them of potential threats and best practises. The project will also provide innovative solutions to Governmental cyber issues, aid detection of cyberattacks, better combat them and improve response times in order to reduce their impact and ensure the safety of democratic decision-making.

- ECHO targets practical use of outcomes to offer technologies and services having increased cyber-resilience by sector and among inter-dependent partners
- Use of the ECHO Federation of Cyber Ranges (E-FCR) for experimental simulation of cyberattack scenarios, pre-production testing, product evaluations
- Combined use of the ECHO Federation of Cyber Ranges (E-FCR) and E-Cybersecurity Certification Scheme (E-CCS) for certified qualification testing of potential technologies required to meet customer specification
- Use of ECHO Cybersecurity Certification Scheme (E-CCS) as benchmark of cybersecurity certification to be obtained as a market differentiator
- Use of the ECHO Early Warning System (E-EWS) to share early warning of cybersecurity related issues (e.g., vulnerabilities, malware and trends, etc...)
- Promotion of improved cyber skills through leveraging diverse education and training options made available by the E-Cybersecurity Skills Framework, particularly as it relates to security-by-design best practices.

## EVENTS

### CONVERGENCE NEXT - 1-3 JUNE, 2022

CyberSec4Europe, CONCORDIA, ECHO, SPARTA and ECSO are pleased to announce CONVERGENCE NEXT on **1-3 June 2022!**

It follows in the tradition set in the first CONVERGENCE event on 9-11 December 2020 which successfully presented results and demonstrations from the four pilot projects and the collaborative focus groups.

CONVERGENCE NEXT will focus upon the future of the community, the European Cybersecurity Competence Centre (ECCC) and look at the key issues for cybersecurity in the future.

Read more about the event:  
<https://cybercompetencenetwork.eu/convergence-next/>



**Save the date**  
**1-3 June 2022**  
**Brussels**



**CONVERGENCE NEXT**

SAVE THE DATES! 1- 3 JUNE 2022  
 Representation of the State of Hessen to the EU,  
 rue Montoyer 21, Brussels [...]

### Research and Innovation Symposium for European Security and Defence" (RISE-SD)

27 April, 2022 PLOVDIV - BULGARIA

<https://echonetwork.eu/research-and-innovation-symposium-for-european-security-and-defence-rise-sd/>



### 11th Multimedia Communications, Services & Security (MCSS 2022) conference


3-4 November, 2022 KRAKOW/KIELCE - POLAND

Submission: May 23, 2022

<https://echonetwork.eu/11th-international-conference-on-multimedia-communications-services-and-security/>



# The next Laurea Cyber Morning is coming!



## CYBER MORNING

**April 27th 2022 9:00-11:30 hrs CET\***

**Zoom link** (Password = 814505):

<https://laurea.zoom.us/j/66552585760?pwd=SmY3bThxSXhSZCtjRWpKb3RqREdGZz09>

9:00 – 9:10 **Opening / ECHO Cyber security Network**

- Eveliina Hytönen, ECHO / Senior Lecturer, Laurea UAS

09:10 – 10:10 **Fighting Cybercrime / CYCLOPES**

- Peter van de Crommert, CYCLOPES / Manager EU Projects, DITSS

10:15 – 11:15 **Countering hybrid threats / EUHYBNET**

- Päivi Mattila, PhD, EU-HYBNET / Director of Security Research Programme, Laurea UAS

11:15 – 11:25 **Closing**

- Eveliina Hytönen, ECHO / Senior Lecturer, Laurea UAS




**Laurea Cyber Mornings by ECHO**

- Laurea Cyber Mornings are organized as part of Project ECHO as a series of multi-actor events aiming to raise awareness and discussion of various cybersecurity topics.
- This event focuses on European cybercrime prevention and countering hybrid threats.

**By Laurea University of Applied Sciences**

- More information: [harri.ruoslahti@laurea.fi](mailto:harri.ruoslahti@laurea.fi)

\*Note: all times CET (+1 in Finland)

[www.echonetwork.eu](http://www.echonetwork.eu)

Laurea Cyber Mornings are organized as part of Project ECHO as a series of multi-actor events aiming to raise awareness and discussion of various cybersecurity topics. This April 27th event focuses on European cybercrime prevention and countering hybrid threats.

## THE LIGHTER SIDE



VISIT OUR WEBSITE:

<https://www.echonetwork.eu>

ECHO - email: [info@echonetwork.eu](mailto:info@echonetwork.eu)

You received this email because you are registered with ECHO

[You can unsubscribe here](#)

