NOVEMBER 2021 | Issue 7

ECHO

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

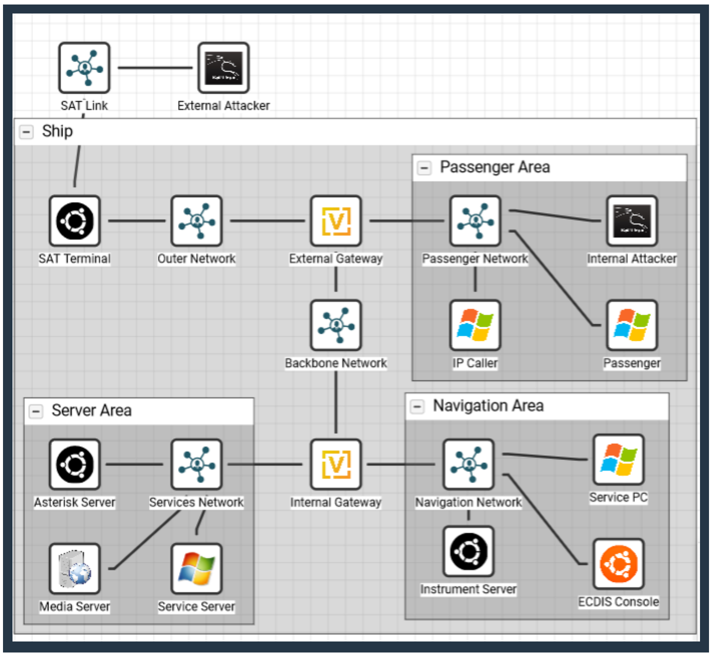
Newsletter

A GLIMPSE ON ECHO CYBER RANGES: A MARITIME SCENARIO

Written by Matteo Merialdo
Project Implementation Coordinator, RHEA Group

As part of the ECHO Demonstration Cases, a wide initiative to validate all ECHO assets via sector-specific and multisector scenarios, the team implemented a Maritime cyber range scenario, a combination of effort from RHEA and Fincantieri.

Leveraging RHEA's cyber range platform (CITEF) the team implemented the emulation of the navigation system of a passenger ship, including an emulated GNSS satellite link providing the positioning data. A set of attack, defense and forensics variations of the scenario have been then developed, in order to teach to small groups of students to identify and react to ongoing cyber attacks targeting the navigation system and with different sources and threat vectors (malware, brute force, configuration files compromission).



See the figure from RHEA's CITEF cyber range management dashboard, the emulated network. It is possible to notice the emulated Sat Link and Sar Terminal, and as well different network areas of the ship.

READ MORE

THE USE OF CYBER RANGES IN THE RISK MANAGEMENT WORLD

Written by Ana Maria Matejic
Security Services Manager, RHEA Group Brussels

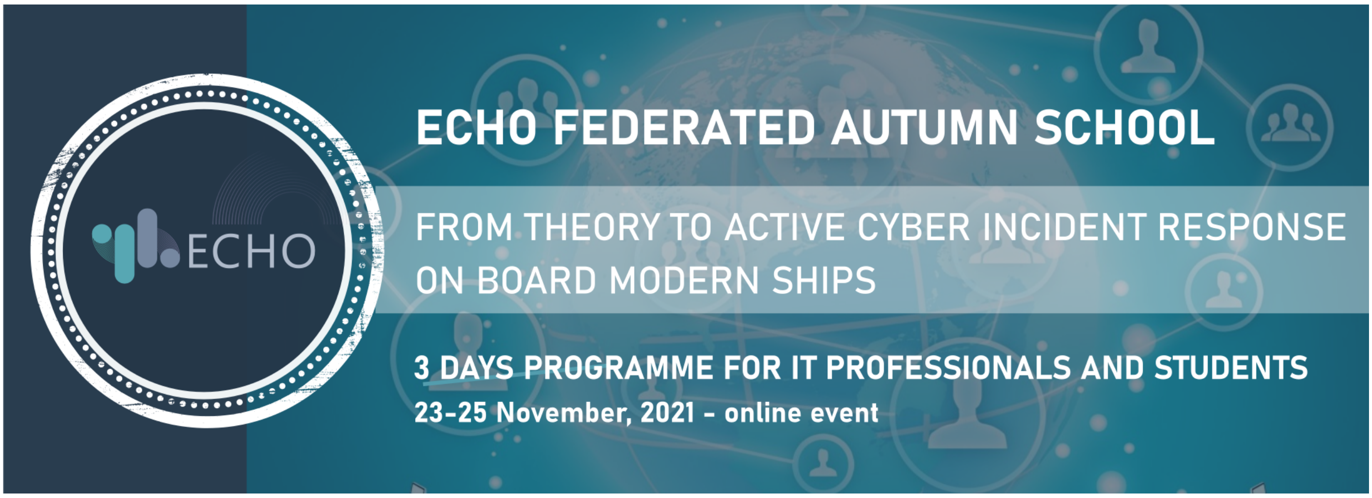
Before connecting the "cyber range" concept with the "risk" world, it is important to start with the basics: why use a cyber range?
Probably the most interesting answer for this question is its ability to provide an environment where new ideas can be tested and fine-tuned. Indeed, assisting at a growing competitive atmosphere within any industry, creativity has taken the lead for those who want to keep their business among the top players. This has created a domino effect and influences the way cyber security and cyber risk teams support the business they serve. In parallel with keeping an organization at the forefront of their specific industry, there are also challenges influencing the way cyber risk is assessed and managed: regulatory landscape changes, new technologies adoption, mergers, and acquisitions or divestitures, compliance maturity, and even cyber security skills limitations.

In these circumstances, cyber ranges have the potential to become an important part of a mature cyber risk management strategy. That gives the opportunity, to the organization supporting this blend, to bring in the same space cyber security teams, risk teams, and executives. They will not only experience cyber threat situations in a controlled environment but also understand how they can cooperate, in daily business, to prevent and contain them. Further, a cyber range offers the possibility to try new ideas on overcoming or treating risks that arise from business practices and that, without simulating specific cyber situations, would not be that facile to uncover.

From a more technical perspective, cyber ranges are a useful tool to uncover internal risks related to operational cyber activities: gaps within the incident response plans or testing certain technologies prior to using them in production environments. This approach helps as a "preventive" control in the risk mitigation domain but also as a "protect the business" mindset for cyber teams that do outstanding efforts to contribute to the organization's growth.
For example, Rhea's CITEF cyber range (widely used in ECHO to support the Federated Cyber Rage solution) is designed to address the aforementioned scenarios and other business-specific ones but also answers to demands from a range of potential users:

- Students – They can test knowledge acquired in classes or develop their future cyber skills
- Instructors/Professors – They can use a cyber range as a classroom "lab" or as a "test environment" for topics they would like to develop for their classes.
- Professionals – Professionals from areas such as cyber security, IT operations, business continuity operations or incident handlers can use for their teams benefit the cyber range to improve communication, knowledge, response methods, and times and to anticipate capacity needs.

Ultimately this will help the respective teams to align with business needs and also to help other teams such as the risk ones.



ECHO

ECHO FEDERATED AUTUMN SCHOOL

FROM THEORY TO ACTIVE CYBER INCIDENT RESPONSE ON BOARD MODERN SHIPS

3 DAYS PROGRAMME FOR IT PROFESSIONALS AND STUDENTS

23-25 November, 2021 - online event

https://echonetwork.eu/echo-federated-autumn-school/

READ MORE ABOUT ECHO FEDERATED AUTUMN SCHOOL
IN THE NEXT NEWSLETTER IN DECEMBER 2021!

2021 IEEE INTERNATIONAL CONFERENCE ON CYBER SECURITY AND RESILIENCE

Written by Notis Mengidis
Cybersecurity Research at Information Technologies Institute (ITI), CERTH

The IEEE International Conference on Cyber Security and Resilience (IEEE CSR) is an annual event sponsored by the IEEE Systems, Man, and Cybernetics (SMC) Society. It focuses on theoretical and practical aspects of security, privacy, trust, and resilience of networks, systems (including complex Cyber-Physical Systems – CPS), applications, and services, as well as, novel ways for dealing with their vulnerabilities and mitigating sophisticated cyber-attacks.

Having been originally planned as a physical event at the island of Rhodes, Greece, the IEEE CSR 2021 conference was unfortunately turned into a fully virtual event due to the pandemic. The technical program included a total of 7 complementary special workshops diving into dedicated areas of high interest to the cyber security community, such as cyber threat intelligence, cyber ranges and security training, artificial intelligence and data science techniques for security applications, power grid and critical infrastructure security, cyber economics, etc., resulting into an intensive three-day event. ECHO partners, both from academia and the industry, had very active participation and submitted high-quality contributions but also provided their expert views during the peer review process as members of the Technical Program Committee.

MEET ECHO'S EXPERT - MÁRTON KIS

Semmelweis University - Budapest, Hungary

How would you introduce yourself and your role within the ECHO Project?
Leading WP9, which is a quite complex work package. While taking care of the dissemination and communication of the important project results the team also focuses on innovation management with introducing an innovative approach to gather inputs for the work (ideathons), exploitation of the assets, products and services developed during the project lifetime, as well as the societal impact of the project

Why do you think cybersecurity is important nowadays?
Digitalization of all aspects of our lives is inevitable. We manage our daily routines mostly online nowadays - should it be governmental affairs, banking, or online learning. If we do not raise awareness, then our digital identity can be easily hacked and misused.

What surprised you the most about working in ECHO?
ECHO is a big consortium. The 100+ partners are coming from all different backgrounds. Yet the focus, and the willingness to work together as a team and contribute towards a greater good, the better and more secure EU level cybersecurity is a really positive surprise.

Is there an achievement or contribution that you are most proud of? Why?
We tried to be proactive during the different maturity levels of the project, and support the development with very successful Ideathons. As the latest addition to this, we are delivering our first ECHO Federated Autumn School (EFAS), where during the 3 days of the event we will aim to show our project results both in theory and then in real-life action.

What was the biggest challenge you were facing?
Of course, we have had difficulties during the peak months of the pandemic, it was not easy to keep the information flow and the motivation levels high at the same time. But we have used all possible digital channels to communicate and share our experience, thus the work did not stop.

In your opinion, what will be the biggest lesson of the Covid-19 epidemic in terms of cyber security?
I'm not sure if there is one single big lesson. Rather would say, that a lot of digital solutions, which were planned for the future (near or distant) became reality during the pandemic. So I see the Covid not only as a problem, but also as opportunity, and I hope, that the spotlight, which was pointed at cybersecurity during these months will not vanish during the normal days.

DIGILIENCE 2021 Conference
by Todor Tagarev

The third international scientific conference “Digital Transformation, Cyber Security and Resilience” (DIGILIENCE 2021), supported by the ECHO project, took place in the old capital of Bulgaria, Veliko Tarnovo, 29 September – 1 October 2021. After rigorous peer-review, the Steering Committee selected 29 papers. The conference agenda (https://digilience.org/content/digilience-2021-program) included another seven invited reports from ENISA, the European Defence Agency, the Software Engineering Institute at Carnegie Mellon University, and the US Pacific Northwest National Laboratory, Bulgaria’s defence ministry and the deputy national cybersecurity coordinator. 65 policy makers and academics from Bulgaria, Finland, Germany, Greece, Italy, Poland, Slovakia, the United Kingdom, the United States and Ukraine participated in the conference – 40 of them onsite, and the rest remotely.

The conference was hosted by Bulgaria’s National Military University. Seventeen of the submitted papers were published prior to the conference in vol. 50 of the open-access Information &amp; Security: An International Journal, https://doi.org/10.11610/isij.v50. AGH, BU, CERTH, IICT, and KhAI reflected ECHO research results in five of these papers. Currently, we are collecting amended version for the post-conference volume, to be submitted to the Springer series “Communications in Computer and Information Science.”

ECHO EVENTS

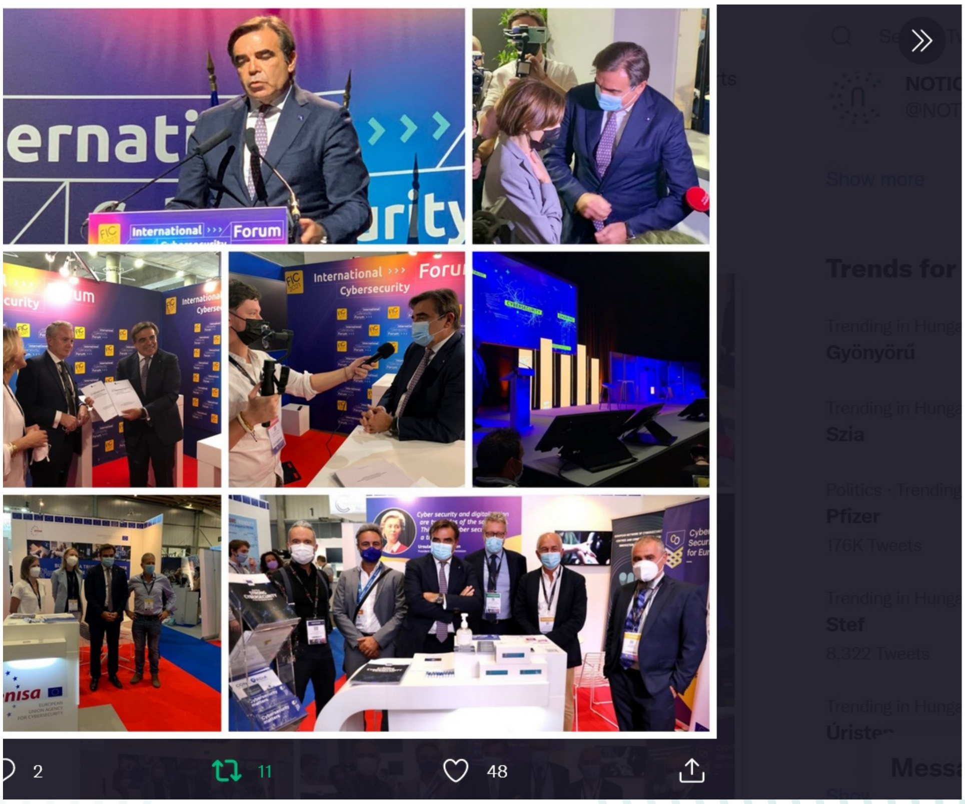
ECHO at FIC Conference in Lille

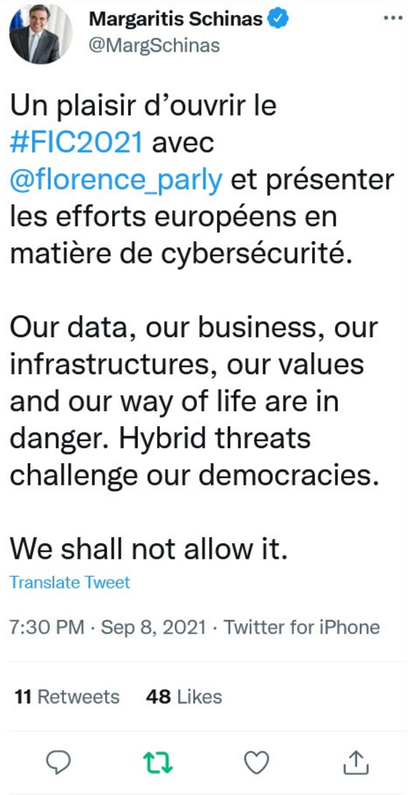
The International Cybersecurity Forum (FIC) is one of the leading European events on Cybersecurity. The event was held in Lille in September. FIC is a TRADE SHOW for buyers and suppliers of cybersecurity solutions to meet and network and a FORUM to foster reflection and exchanges among the European cybersecurity ecosystem.

The theme of this year was: "For a collective and collaborative cybersecurity!"

"When facing systemic risks – whatever their origin – the only valid response is therefore collective and collaborative. Collective, because each stakeholder is responsible not only for its own security but also for the security of every other stakeholder, and therefore of the whole. Collaborative, because cooperation and information sharing are essential to compensate the asymmetry between the «attacker» and the «defender»."

ECHO and the other 3 pilot projects - Concordia, Sparta and Cyber Security for Europe - were excited to be in a live event again. ECHO was present as part of the Cyber Competence Network in Lille and was honored by the visit of *Margaritis Schinas @EU_Commission Vice-President/Promoting our European Way of Life (Migration, Security, Health, Skills, Education, Culture, Sport, fighting Antisemitism, FoRB)*





Margaritis Schinas
@MargSchinas

Un plaisir d'ouvrir le #FIC2021 avec @florence_parly et présenter les efforts européens en matière de cybersécurité.

Our data, our business, our infrastructures, our values and our way of life are in danger. Hybrid threats challenge our democracies.

We shall not allow it.

Translate Tweet

7:30 PM · Sep 8, 2021 · Twitter for iPhone

11 Retweets 48 Likes

ECHO NEWS

AI-ML cybersecurity for aviation/space and maritime autonomous transport ideathon

The ECHO's AI/ML Cybersecurity for Aviation/Space and Maritime Autonomous Transport Ideathon event took place on August, 31st, 2021. The aim of this session was to generate innovative ideas which will inform the development of the ECHO technology roadmap on AI/ML Cybersecurity for Aviation/Space and Maritime Autonomous Transport.

ECHO

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

AI/ML Cybersecurity for Aviation/Space and Maritime Autonomous Transport Roadmap

Oleg Illiashenko
Vyacheslav Kharchenko
KhAI

ECHO project has received funding from the European Union's Horizon H2020 research and innovation programme under the grant agreement no 830943

Ideathon
08-31-2021

READ MORE

New participants at ECHO

By joining ECHO, new project participants help us improve the quality of our inputs, identify new and exciting opportunities, improve the products we create and help Europe in its mission to strengthen its cybersecurity posture.

fhoö UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

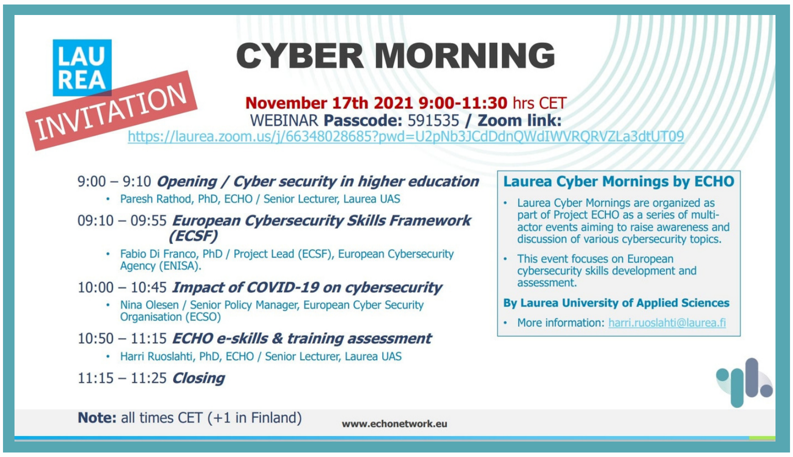
LOGISTIKUM CHALLENGE ACCEPTED

TALGEN

b!nalyze

READ MORE

The ECHO network organized the second Laurea Cyber Morning of 2021



LAU REA

INVITATION

CYBER MORNING

November 17th 2021 9:00-11:30 hrs CET
WEBINAR **Passcode:** 591535 **/ Zoom link:**
https://laurea.zoom.us/j/66348028685?pwd=U2pNb3JCdDdnQWdIWVRQRVZLa3dtUT09

9:00 – 9:10 ***Opening / Cyber security in higher education***
- Paresh Rathod, PhD, ECHO / Senior Lecturer, Laurea UAS

09:10 – 09:55 ***European Cybersecurity Skills Framework (ECSF)***
- Fabio Di Franco, PhD / Project Lead (ECSF), European Cybersecurity Agency (ENISA).

10:00 – 10:45 ***Impact of COVID-19 on cybersecurity***
- Nina Olesen / Senior Policy Manager, European Cyber Security Organisation (ECSO)

10:50 – 11:15 ***ECHO e-skills & training assessment***
- Harri Ruoslahti, PhD, ECHO / Senior Lecturer, Laurea UAS

11:15 – 11:25 ***Closing***

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 cybersecurity skills development and assessment.

By Laurea University of Applied Sciences
- More information: harri.ruoslahti@laurea.fi

Note: all times CET (+1 in Finland)

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 November 17th event focused on European cybersecurity skills development and assessment and there were 45 active participants.

READ MORE

THE LIGHTER SIDE

I CHANGED ALL MY PASSWORDS TO "INCORRECT".
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."
TROLL.ME

VISIT OUR WEBSITE:
https://www.echonetwork.eu