FEBRUARY 2021 | Issue 4

ECHO

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

Newsletter

Two years of ECHO, and the future ahead

Written by Prof. Wim Mees, Project Coordinator,
Royal Military Academy of Belgium

ECHO is proud to celebrate its two-year anniversary. We have from the start been strongly committed to building the European network of cyber competence centers in close collaboration with the other pilot projects and ECSO. This has resulted in a number of inter-pilot focus groups and joint events.

A lot has happened in those two years. We suffered from the COVID pandemic, that forced organizations to accelerate their digitization process. Whereas before the pandemic digitization mainly focused on increasing the productivity of an organization, now it became a matter of survival, of safeguarding its productivity. An end-to-end paperless digital process, supported by a cyber-resilient IT infrastructure, became key to ensuring business continuity.

As always, criminals were quick to seize the opportunities that a crisis presents to them. They swiftly adapted their modus operandi and engaged in new cybercrime activities. Nation-state threat actors were observed to engage in disruptive activities and launch disinformation campaigns. This once again proved the need for an important investment in cybersecurity in order protect the interests of the European Union, its industry and its citizens.

ECHO was the first pilot to actively undertake initiatives in response to the new and increasing cyberthreats that followed from the COVID crisis. We launched an awareness campaign, published white papers, organized table top exercises and are producing relevant roadmaps, as well as information sharing and training solutions that we validate in our demonstration cases.

At the end of last year it was decided by the member states that Bucharest will host the future European Cybersecurity Competence Center. The governance model for the Center and its interactions with all relevant European stakeholders remains to be determined. As a pilot project we will provide valuable inputs here, just as we will contribute to setting up the Center in the months and years to come.

Indeed, it is now the time to start developing and growing the European cyber competence network, to bring partners on board so we can all together develop the ideas, concepts, and solutions that will enhance Europe’s strategic autonomy in the digital field.

WELCOME TO ECHO

Meet the new ECHO Participants

WELCOME TO ECHO
ВОЕНА АКАДЕМИЈА
1995
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
1918
HUNCERT
European University Cyprus
CYBER CER!DES
COMPETENCE CENTER

WWW.ECHONETWORK.EU/JOIN-ECHO

READ MORE

SPOTLIGHT

Get to know the results of the ECHO project in our new 'ECHO Spotlight' publication series. Follow us on Facebook, Linkedin and Twitter, we keep you updated on the deliverables of ECHO Project.

READ MORE

READ MORE

IMPACT PRODUCT

Transversal technical cybersecurity challenges

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

The bigger picture

In line with the needs of the ECHO project, the **task of the detailed analysis of transversal technical cybersecurity challenges, using a technically focused, comprehensive and holistic approach**, is responsible for setting up the necessary research foundations for developing cybersecurity technology roadmaps. The strategic goal of those roadmaps is to assist in the development of innovative technologies aiming to address contemporary cybersecurity challenges and is thus an important input towards achieving the research goals of the ECHO project in improving the proactive cyber defence of the European Union.

The methodology

This analysis builds on the research outcomes of the multi-sector needs analysis that takes place in WP2 of the project, and takes into account the latest industrial reports and academic publications, covering multiple stakeholders' points of view, and highlighting challenges that span over different and multiple sectors. Subsequently, the threats and concerns identified in these sources were converted to a long and exhaustive list of challenges. To classify these challenges, some of the most widely accepted standards of taxonomies were examined and was concluded that the holistic taxonomy proposed by JRC was the most appropriate and precise to be used as the basis of the conducted analysis, since it provides a more expressive and representative view of the task's given context. **The diverse expertise of more than 20 different contributors was utilised in order to avoid bias and to take into account different perspectives when conducting this analysis.** The result was a classification of 10 categories, aligned with the JRC taxonomy and encapsulating all of the identified challenges.

READ MORE

THE CYBERSECURITY ATLAS

by Dr David Goodman, CyberSec4Europe

European Commission

European Cybersecurity Atlas

Connecting cybersecurity experts across Europe

A digital knowledge management platform to map and categorise cybersecurity competencies across Europe and stimulate collaboration between cybersecurity specialists

Main features

→ An interactive map showing the location of cybersecurity organisations and their area(s) of expertise

→ An EU cybersecurity taxonomy that aligns cybersecurity definitions and terminologies for a common understanding

→ Information about European and national research projects to help identify possible project partners

→ Courses and training offered by participating organisations

The European Cybersecurity Atlas is a European Commission collaborative platform

Register yourself and your organisation:
https://cybersecurity-atlas.ec.europa.eu/

On 9 December 2020 the European Council voted to locate the EU's future cybersecurity research hub in Bucharest. The European Cybersecurity Industrial, Technology and Research Competence Centre, as it is formally known, makes up part of the European proposal for a Cybersecurity Competence Network and Centre, which aims to help the EU continue to build the capacity necessary to secure the Digital Single Market. The Competence Centre will facilitate and coordinate the work of the Cybersecurity Competence Network which in turn will be supported by the European Cybersecurity Atlas, a digital knowledge management and collaborative platform that aims to map, categorise and stimulate collaboration between cybersecurity experts across Europe.

The EC’s initiative will contribute to enhanced networking, visibility of ongoing efforts and coordination of cybersecurity expertise across Europe, that will deliver on the EU’s cybersecurity policy agenda, support the EU’s digital strategy and ultimately ensure a more secure Europe for businesses and citizens.

The **goals of the platform** are to

- facilitate the establishment of a community of practice
- help identify with whom to collaborate on future projects
- map the competencies of Europe in various cybersecurity domains
- act as a knowledge management tool for the European Cybersecurity Competence Centre
- raise the visibility of participants within the cybersecurity community and beyond
- better coordinate European R&D efforts in cybersecurity
- contribute to shaping the strategic orientations of EU programmes funding cybersecurity research, technology and capabilities
- provide relevant input to cybersecurity policymaking in Europe
- provide awareness of the cybersecurity community
- support the European Commission on managing work programmes and allocation of funds
- support diversity and inclusion, aiming to improve gender balance and geographical balance in the cybersecurity sector

READ MORE

IEEE CSR
Cyber Security and Resilience
Virtual Conference, July 2021
IEEE Cyber Security & Resilience
IEEE
Advancing Technology for Humanity
IEEE SMC
Systems, Man, and Cybernetics Society
SMC Technical Committee on Homeland Security
LOG
26-28, JULY 2021
2021 IEEE International Conference on Cyber Security and Resilience

EVENT

International Workshop on Actionable Cyber Threat Intelligence (ACTI) led by ECHO and supported by the 3 other pilot projects (Concordia, Cyber Security for Europe and Sparta)
More information about the ACTI workshop:
https://www.ieee-csr.org/workshops/acti/

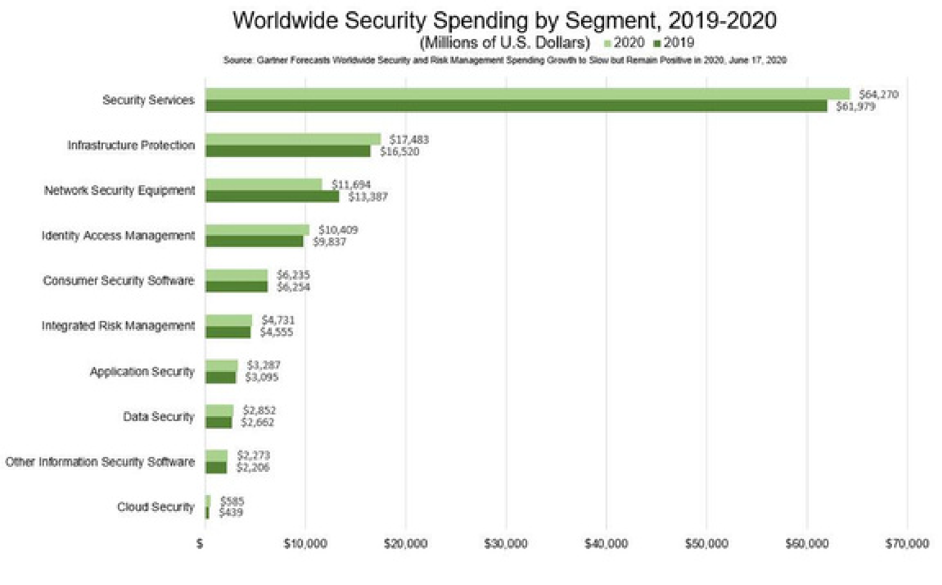
Important dates:
Paper submission deadline: April 19, 2021
Authors' notification: May 3, 2021
Camera-ready submission: May 10, 2021
Early registration deadline: May 31, 2021
Workshop date: July 28, 2021

Organizers are also welcome research on novel designs and design methods to help empowering citizens with tools and literacy and increase their ability in recognizing, reporting and combatting threats.
More information about the 2021 IEEE CSR conference:
https://www.ieee-csr.org/

DID YOU KNOW?

Cybersecurity spending to reach $123B in 2020

CYBERSECURITY BUDGET BEFORE BREACH
CYBERSECURITY BUDGET AFTER BREACH



Source: forbes.com

VISIT OUR WEBSITE:

https://www.echonetwork.eu

ECHO - email: info@echonetwork.eu
You received this email because you are registered with ECHO
You can unsubscribe here