

## THE NEWLY CYBERSEAS PROJECT OF THE ROMANIAN ENERGY CENTER ON CYBER SECURITY ACCEPTED FOR FUNDING BY THE EUROPEAN COMMISSION

30<sup>th</sup> of March 2021, Carina Ioana ZIDARU

Romanian Energy Center Association (CRE) expands its portfolio of European Projects with a new one entitled „CyberSEAS” – „Cyber Securing Energy dAta Services” in the field of Cyber Security, together with TRANSELECTRICA. Recently, the Project it has been accepted for funding by the European Commission (EC), within the H2020 Program. Twenty-six european organizations from - IT, DE, EE, ES, SI, RO, EL, HR are part of the Consortia coordinated by ENGINEERING - INGEGNERIA INFORMATICA SPA from Italy.

**CyberSEAS** Project ambition is to improve the resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions and extended involvement models of stakeholders and consumers in complex attack scenarios, characterised by the presence of legacy systems and the increasing connectivity of data feeds. It starts in October this year and will last thirty-six months.

The main strategic objectives of **CyberSEAS** Project are - countering the cyber risks related to highest impact attacks against European Electrical Power Energy Systems (EPES), to increase EPES trust and safety, protecting consumers against personal data breaches and attacks, increasing the security of the Energy Common Data Space. All three objectives are equally important, since cyber-criminals are shifting tactics to favour multi-stage attacks in which stealing sensitive data is a precondition for the real attack and enables them to maximise damage and profits (while traditionally infrastructure cyber-attacks used to be direct attacks to the machinery and typically targeted control systems, not data).

To achieve these objectives, CyberSEAS delivers an open and extendable ecosystem of 30 customisable security solutions providing effective support for key activities, and in particular: risk assessment; interaction with end devices; secure development and deployment; real-time security monitoring; skills improvement and awareness; certification, governance and cooperation. CyberSEAS solutions are validated through experimental campaigns consisting of 100+ attack scenarios, tested in 3 labs before moving out to one of 6 piloting infrastructures across 6 European countries.

**CRE** Association has a key role in this Project and contributes to the following activities: Collaborative assessment of cyber vulnerability and risks in the energy supply chain – WP2, CyberSEAS integrated toolset for cyber-resilient EPES – WP3, Fostering the culture of cyber-resilient Energy supply chain – WP8 and From lab to market – WP9.

CyberSEAS focuses exactly on the attacks, which not only have the highest potential of disrupting the business continuity of critical elements in the energy distribution, but also – and most importantly – result in major safety incidents, with loss of lives and substantial damage to infrastructure (including cascading effects) and critical privacy breaches. This project considers the challenges and the constraints resulting from the increasing use of decentralised Renewable Energy Sources (RES) and the large proportion of legacy systems that will continue to co-exist in extended energy supply chains involving a variety of diverse operators and consumers. CyberSEAS also covers attacks targeting the confidentiality of citizens’ data, as well as on the privacy and the integrity of the Energy data space in general.

After six years of intensive activity of the **Innovation and Development Department**, CRE association is among the top ten Romanian organizations from over three thousand entities that managed to win European funding, with a total exceeding four million euros, according to the statistics of the European Commission ([Link](#))<sup>1</sup>.

CRE Association is constantly preoccupied and interested in the cyber security domain, also in the development of cybersecurity toolkits for critical infrastructure for its members. The association is also very active to find solutions to improve awareness of cyber threats and attacks for the power energy infrastructure. CRE is in constant contact with EU partners to identify new project consortiums that will tackle the cyber-security matter and to actively participate in dedicated conferences and events. CRE already implemented **SUCCESS** Project and is currently implementing other cyber security projects in which the Innovation and Development Department has a significant contribution.

**PHOENIX** Project – „Electrical Power System’s Shield against complex incidents and extensive cyber and privacy attacks”, started in 2019 and it will end in 2022. The main objective of the project is to improve the cyber security of European Electrical Power Energy systems. PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee to minimize cascading effects in infrastructure, the environment, the citizens and the end-users at reasonable cost.

CRE Association is an active and strategic partner together with its members and other potential members in international consortia for deploying energy projects funded by the EC, such as: **CROSSBOW**, **PHOENIX**, **TRINITY**, **EDDIE**, **EDGEFLEX**, **SUCCESS**, **RESERVE**, **NRGS**, **WISEGRID**, **SOGNO** and **CYBERSEAS**.



<sup>1</sup> European Commission H2020 Country Profile [Link](#)