

ACADEMIC FOCUS

Erasmus+ Mobility Projects at “Mihai Viteazul” National Intelligence Academy

In July 2025, “Mihai Viteazul” National Intelligence Academy (ANIMV) completed its 5th academic mobility project (KA131_2023) dedicated to the countries participating in the ERASMUS+ programme. Through the Erasmus KA_131 mobility project won in 2023, ANIMV set out to continue the efforts started in 2018 towards institutional internationalization and the development of the key competencies and skills of teaching/administrative staff and students from our academic study programs, through all 4 types of mobilities – study, practice, teaching and training. Additionally, we considered increasing and expanding university partnerships with universities from participating countries. Upon finishing the 26 months of implementation, ANIMV has managed to consolidate its status as a trusted European partner and higher education institution focused on the development of students and staff, evidenced by the following academic milestones derived from the set objectives:

1. supporting four participants in order to develop key competencies and promote lifelong learning;
2. increasing ANIMV’s visibility among the European university community and facilitating the exchange of good academic practices with higher education institutions with similar profiles and training centers with a tradition in the area of training courses for professionals;
3. promoting diversity, inclusion and equal opportunities by organizing four outgoing mobilities, one for each of the four categories;
4. developing the capacity to offer study programs better oriented towards the European community – introducing new subjects taught in English, rethinking a Master’s degree program in order to increase its attractiveness – creating synergies with other Erasmus projects carried out within ANIMV (INSET – Erasmus Mundus Design Measures);

5. intensifying the digitalization process by transposing courses and support materials used in the traditional setting to the digital classroom;

6. mapping new possible funding opportunities offered within the framework of the Erasmus program and preparing project proposals with partners to create additional academic synergies.

In conclusion, the KA131_2023 project represented another essential step in consolidating ANIMV's internationalization process, with direct effects on the quality and relevance of the educational databases offered within the academic study programs. During the implementation period the Academy reconfirmed its capacity to capitalize on opportunities for training, exchange and European cooperation, generating a visible impact on the development of the skills of teaching/ administrative staff and students, and at the same time contributing to the consolidation of its position as a trusted partner and learning/ research hub. As a result, due to this solid foundation, the Academy will be able to build and expand future university partnerships, both in the area of classic university mobilities and in the area of broader projects.

Collectively, the five ERASMUS+ projects that have been implemented so far have encompassed a number of 18 beneficiaries, students and professors alike, who took part in different types of mobilities, as follows:

- 7 training mobilities;
- 5 traineeships;
- 3 teaching mobilities;
- 3 study mobilities.

ANIMV is currently implementing two more Erasmus+ KA131 mobility projects for which it has received funding under the 2024 and 2025 calls, respectively.



**Prevention of Weaponization and Enhancing Resilience against
Security-related Disinformation on Clean Energy - POWER
Grant agreement no. 2024-1-RO01-KA220-HED-000245038
(2024 - 2027)**

POWER Project addresses the fight against climate change by mitigating the effects of clean-energy-related disinformation on public policy adoption and implementation among both the target group and the general public. The project directly tackles two crucial societal challenges: climate change and the pervasive issue of disinformation, particularly around renewable energy. By engaging students, educators, and professionals across Romania, Malta, Spain, and Moldova, it aims to elevate media and clean energy literacy, foster a comprehensive understanding of environmental issues, thus enhancing resilience against disinformation.

The project consortium is headed by “Mihai Viteazul” National Intelligence Academy and the partners are University Rey Juan Carlos, Spain, the University of Malta, Eurocomunicare Association. The project also has an associated partner The Center for Strategic Communication and Countering Disinformation, in the Republic of Moldova.

The project’s first general objective is to facilitate transition to clean energy by fostering an informed fact-based public discussion on clean energy sources. In correlation, the second general objective is to strengthen societal resilience against the weaponisation of clean energy conversations by disinformation actors, and to contribute to the EU’s policy objectives to reduce net greenhouse gas emissions by 55% by 2030 and to generate at least 42.5% of the EU’s energy from renewable sources.

These objectives have been broken down into six specific objectives: (1) to develop a lexicon related to clean energy and associated

concepts in Romania, Spain, Malta and the Republic of Moldova in the target languages; (2) to map online disinformation modus operandi, techniques, and narratives in the four participating countries. The project will collect and analyse automatically and manually clean-energy-related disinformation narratives on three social media platforms. The results of both these research activities will represent the basis of the clean-energy lexicon; (3) to neutralize clean energy disinformation through dynamic science communication in Romania, Spain, and Malta; (4) to enhance clean energy and media literacy among students, teaching staff and employees of the partner organizations. These results will be achieved through organizing three, five-day, face-to-face Clean Energy Cafes as learning events which bring together students in the fields of security, intelligence, communication, social sciences, and sciences with teaching staff and employees in the same areas and are designed as experiential, learning-by-doing activities; (5) to foster a collaborative empowered community of practice among students in the partner organizations and local universities by organizing four three-day face-to-face Clean Energy Living Labs dissemination activities in each partner country. In these labs, participants will work together to design innovative, artistic, digital productions to increase clean energy literacy and preempt disinformation; (6) to create and populate digital educational content and tools addressed to stakeholders in the four partner countries. This e-learning hub will include a Practitioner's Digital Briefcase, an Educator's Digital Briefcase, digital storylines, online learning modules. These will foster the development of new teaching and learning practices through digital content and interactive learning resources.

At the heart of this initiative is the development of innovative educational content and digital tools. This includes a clean energy lexicon, immersive learning scenarios, and digital storylines, all designed to debunk myths perpetuated by disinformation campaigns about renewable energy. The approach integrates cutting-edge research, participatory teaching methodologies, and broad dissemination activities, such as Clean Energy Living Labs and Clean Energy Cafés.

Key to the strategy is the cross-sectoral collaboration that leverages the expertise of the partner organizations with a proven track record in digital education, fighting against disinformation and environmental projects. By creating synergies between media literacy, environmental education, and digital pedagogy, POWER not only addresses the selected priorities head-on but also pioneers a holistic model for tackling complex global challenges.



EU Knowledge Hub on Prevention of Radicalisation (EUKH)

The EU Knowledge Hub on the Prevention of Radicalisation takes up the legacy of the Radicalisation Awareness Network and aims to provide a set of resources and activities such as trainings, workshops and study visits, as well as mentoring and job shadowing for young professionals in the field of preventing and combating radicalisation. Further, selected experts will conduct research on specific topics in line with the project's general objectives. Two communities of experts will support the project: The Knowledge Hub Research Committee, composed of 15 internationally recognised researchers in the field and the EU Research Community on Radicalisation (ERCOR), a database of experts which will be called upon when their expertise is required.

The activities of EUKH will be grouped according to several thematic panels, which will represent the main directions of the projects and will be aligned with the priorities set out in the Strategic Orientations. The thematic panels will be composed of leaders and co-leaders, selected from the expert database, as well as invited researchers. The results of the activities of thematic panels will be summarized in annual reports.

Further, EUKH will offer tailor-made support services, requested by a member state, with the aim for addressing specific challenges in the field of combatting radicalisation. These tailor-made support services will assist Member States to implement EUKH results to their specific conditions.

The project was selected through a competitive tender organized by the European Commission. The project will be conducted over four years and has a total budget of 60 million Euros. The winning consortium is led by NTU Denmark and is composed of "Mihai Viteazul" National Intelligence Academy (MVNIA), IPS Innovative Prison Systems (Portugal),

Polish Platform for Homeland Security, Fundación Euroárabe (Spain), Center for Security Studies (KEMEA – Hellenic Ministry of Citizen Protection), Hellenic Foundation for European and Foreign Policy, European Research and Project Office (EURICE, Greece), Deep Blue, European Centre of Studies and Initiatives (CESIE, Italy).

Romania is represented by the “Mihai Viteazul” National Intelligence Academy, which will support training and research activities on the process and factors supporting radicalisation. It will also incorporate research findings in its B.A., M.A. and PhD curricula, as well as support the development of a common culture among practitioners dedicated to combating radicalisation.



Co-funded by
the European Union

INTERSOC
INTERCONNECTED SECURITY
OPERATION CENTRES

**INTERconnected Security Operation Centres – INTERSOC
Strengthening Europe's cybersecurity infrastructure through
innovative machine learning solutions and collaborative
intelligence¹**

(January 2024-January 2027)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a grant for the implementation of the **project INTERconnected Security Operation Centres – INTERSOC**, under financing contract no. 101145853. The project is funded by the Directorate-General for Communications Networks, Content and Technology CNECT.H – Digital Society, Trust and Cybersecurity, H.1 – Cybersecurity Technology and Capacity Building, under the call for projects DIGITAL-ECCC-2022-CYBER-B-03, type of action: DIGITAL-JU-SIMPLE.

Cyber threats have a global impact, often going beyond sectorial borders and producing far broader effects than the targets initially settled. In a context where digital systems are becoming increasingly complex, total prevention of cyber-attacks is no longer possible. However, through robust, integrated and coordinated defence mechanisms, risks can be significantly reduced, ensuring critical infrastructure protection

¹ We thank PhD Claudia Lascateu for the presentation. The INTERSOC project received funding from the Directorate-General for Communications Networks, Content and Technology CNECT.H – Digital Society, Trust and Cybersecurity, H.1 – Cybersecurity Technology and Capacity Building, under grant contract No 101145853. However, the opinions expressed belong exclusively to the author(s) and do not necessarily reflect the views of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

and business continuity. Currently, cybersecurity efforts in the European Union are often fragmented, while cyber-attackers are increasingly coordinated and sophisticated. This reality calls for a new approach to the protection of critical infrastructures. Monitoring the tactics, techniques and procedures used by malicious actors, together with analysing their motivations and targets, can help improve incident detection and response capabilities.

The INTERSOC project was designed to strengthen the level of cybersecurity across the European Union. The initiative aims to increase preparedness at national and European level, facilitate advanced threat forecasts, strengthen cyber incident detection and response capabilities and develop skills in the security of digital infrastructures, while respecting privacy principles and fundamental rights.

Coordinator: Eximprod Engineering S.A. – EPG – Romania.
Partners: Aristotelio Panepistimio Thessalonikis (AUTH) – Greece; Asm Terni Spa (ASM) – Italy; Caixabank SA (CAIXA) – Spain; Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (CERTH) – Greece; Clone Systems Cy Ltd (CLONE) – Cyprus; Cyberethics Lab Srls (CEL) – Italy; Diethnes Panepistimio Ellados (IHU) – Greece; SQS Business Services SRL – Romania; Southeast Electricity Network Coordination Centre Selene Cc Anonymi Etaireia (SELENE) –Greece; Sphynx Hellas Anonymi Etaireia (SPH) – Greece; National Cyber Security Directorate (DNSC) – Romania.
Affiliated entity: Frontiere – Italy.

As cyber-attacks become increasingly sophisticated, multidimensional and difficult to detect by traditional means, these threaten not only the continuity of essential services, but also the economic and social security of the European Union. In this context, it is essential to develop innovative solutions capable of providing advanced threat forecasting, improved detection and response capabilities, as well as tools for secure collaboration between institutional and private actors in the field of cybersecurity. The INTERSOC project responds to these challenges through an integrated and user-centred approach, combining state-of-the-art technologies with advanced information sharing mechanisms.

The overall objective of the INTERSOC project is to *strengthen cybersecurity incident response and increase the resilience of digital infrastructures* by developing advanced threat forecasting, detection and incident response capabilities at national and European levels. In parallel, the project aims to strengthen skills through dedicated training sessions on the security of digital infrastructures. The INTERSOC project also aims to strengthen a resilient, safe and sustainable European cybersecurity ecosystem based on trust, cooperation and compliance with the evolving European regulatory framework.

The specific objectives of the project relate to:

- **Monitoring of complex network and information systems.** The project will develop advanced monitoring mechanisms for complex network and information systems capable of identifying anomalies caused by advanced, multidimensional cyber-attacks. This will be achieved by extending traditional SIEM (Security Information and Event Management) and IDS (Intrusion Detection Systems) functionalities with behavioural and decision-making artificial intelligence algorithms, enabling faster and more accurate incident detection.
- **Low-code approach to security and automation of cyber incident management.** INTERSOC will implement a low-code/no-code approach that will enable a flexible and scalable approach to security processes and incident management automation. This will reduce human intervention, speed up response times and improve the resilience of Security Operation Centers (SOCs).
- **Decentralised and Confidential Sharing of Cyber Threat Information (CTI).** The project will develop a decentralised and confidential mechanism for cyber threat information sharing based on peer-to-peer networks aligned with the European regulatory framework (NIS2, GDPR and related regulations). This will strengthen cross-border and inter-institutional cooperation, enabling a secure and reliable exchange of information.
- **Reliable solutions and technologies for information exchange.** INTERSOC will design and refine trusted solutions and technologies

to address challenges related to establishing and maintaining trust between partners during online information sharing. They will create a secure and transparent collaboration framework, reducing the risks of data manipulation or compromising information flows.

- **Risk and threat analysis, impact assessment and mitigation.** An important objective of the project is to identify, analyse and mitigate vulnerabilities in pilot systems through specific activities. This integrated approach will ensure a high level of security and help strengthen the resilience of the pilot infrastructures tested.
- **Advanced Penetration Test Tools and Methodologies.** Advanced tools and methodologies on penetration testing for new vulnerabilities will be developed and tested. They will be actively tested in SOCs (Security Operation Centres) as part of pilot tests, simulating real cyber-attacks and testing the ability to defend infrastructures.
- **Reliable artificial intelligence algorithms.** The project will develop trustworthy AI algorithms in line with European AI regulations (e.g. proposed AI Act), aligned with relevant standards and working groups (e.g. CEN/CLC JTC21 WG4). These algorithms will comply with transparency, ethics and traceability requirements, while ensuring enhanced performance.
- **Cyber Range Platform for Advanced Exercise.** INTERSOC will use a virtualization platform to host and conduct advanced red team/blue team exercises. These cyber exercises will strengthen institutional capacities, provide realistic training environments and increase users' awareness and preparedness.
- **Validation in three pilot sectors (banking, energy, CSIRT-Cyber Security Incident Response Teams training)**

The project results will be validated through case studies and practical scenarios in three representative sectors:

- the banking sector, where customer security and trust are essential;
- the energy sector, which is essential for economic stability and the functioning of society;

- training and training of CSIRTs, for which knowledge transfer and practical training are fundamental for rapid response to cybersecurity incidents.

Through its approach, the INTERSOC project aims to manage the most important challenges of cybersecurity at European level, including threat forecasting and the development of response capacities:

- **Prediction of threats.** Implement advanced machine learning models, capable of predicting with high precision the evolution of cyber threats, supporting the adoption of proactive defence measures and increasing the resilience of European critical infrastructures.
- **Integration of SOC.** Creating an interconnected network of Security Operations Centres (SOCs), capable of sharing threat intelligence, coordinating responses and providing mutual support in real time.
- **Automated response.** Implement automated incident response systems capable of responding to threats in a shorter time than human operators, minimising the impact, damage and length of the recovery process.
- **Information sharing** (Knowledge exchange). Establish standardised protocols to facilitate the exchange of information on cyber threats and best practices between participating organisations and states, helping to increase trust and build collective resilience.
- **Capacity building.** Increase European cybersecurity capabilities through training programmes, knowledge transfer and the development of a new generation of security professionals.

Through these strategic directions, INTERSOC project aims to strengthen a safer, more resilient and better prepared European cybersecurity ecosystem for the challenges of the future. The integrated approach – from threat prediction and automated response to information exchange and human resources development – reflects the shared commitment to improve European cooperation to a competitive and security advantage in the face of an increasingly complex digital environment.



Co-funded by
the European Union



EU-INSPIRE

**INnovative multi-diSciPlinary Industry-focused
cybersecurity education for upskilling
and Reskilling the EU workforce – EU-INSPIRE²**

(January 2025-January 2028)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of **INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce** – EU-INSPIRE project, under the grant agreement no. 101190054. The project is financed through Digital Europe Programme by the granting authority: European Health and Digital Executive Agency (HaDEA), under the call DIGITAL-2023-SKILLS-05-SPECIALEDU – Specialised Education Programmes in Key Capacity Areas topic, type of action: DIGITAL Lump Sum Grants.

The EU-INSPIRE project responds to the urgent need to bridge the cybersecurity skills gap across the European Union and to train a new generation of professionals with advanced expertise in the political, organisational and technological dimensions of cybersecurity and artificial intelligence (AI). As the cyber threat landscape evolves, specialised training programmes capable of up skilling and reskilling

² We thank PhD Claudia Lascateu for the presentation. EU-INSPIRE project has received funding from the European Union’s Digital Europe Programme, DIGITAL-2023-SKILLS-05 call, under the Grant Agreement no.101190054. Views and opinions expressed are however those of the author(s) only, and the European Union or the granting authority is not responsible for any use that may be made of the information it contains.

the workforce are essential to ensure the resilience of Europe's digital infrastructures and services.

Launched in January 2025 with a funding of 19,477,569.31 euro of which non-reimbursable financial assistance of 9,638,686.15 euro, the project will be implemented over a period of 48 months and will aim to develop a sustainable and multidisciplinary cybersecurity education ecosystem. Accredited and certified training programmes will also be developed, a cybersecurity campus will be created, and the foundations of the EU-INSPIRE Academy will be laid.

The Consortium, consisting of 24 partners from 14 European countries, is coordinated by the University of Piraeus Research Center (Greece) and includes top academic institutions, research organisations, private companies and national authorities: Mib Developpement Ecole des Ponts Business School – France; Universitetet I Oslo – Norway; Technische Universitaet Muenchen – Germany; Universidad De Malaga – Spain; Anoikto Panepistimio Kyprou (Open University of Cyprus) – Cyprus; Consiglio Nazionale Delle Ricerche – Italy; Euroopan Hybridiuhkien Torjunnan Osaamiskeskus – Finland; United Nations Interregional Crime And Justice Research Institute – Italy; Bitdefender SRL – Romania; Obrela Security Industries – Ypireseies Asfaleias Pliroforion Anonymos Etaireia- Greece; Sphynx Hellas Anonymi Etaireia – Greece; Cyberalytics Limited – Cyprus; Insuretics Limited – Cyprus; Karavias Mesites Asfaliseon Kai Symvouloi Asfaliseon Anonymi Etairia – Karavia Insurance Brokers And Insurance Advisors Societe Anonyme – Greece; Asfalys SRL – Belgium; Eunomia Limited – Ireland; AEGIS IT Research GMBH – Germany; Cardet Centre For The Advancement Of Research & Development In Educational Technology Limited – Cyprus; Circular Economy Foundation – Belgium; Cyprus Organisation For Standardisation – Cyprus; Balgarska Organizatsia Po Kibersigurnost Sdruzhenie – Bulgaria; Directoratul National De Securitate Cibernetica – Romania.

The overall objective of the EU-INSPIRE project is to revolutionize the landscape of higher education within the cybersecurity domain by cultivating new group of specialists, equipped with master-level expertise across the political, organizational, and technological dimensions of

cybersecurity, artificial intelligence (AI), and cyber insurance. Its goal is to shape an advanced educational ecosystem that not only fosters the development of specialized skills but also supports the continuous upskilling and reskilling of professionals in response to evolving industry demands and challenges. During its lifetime, the project will deliver three distinct master's programs (MSc, MBA, and MSc by research) and will engage over 1,000 students in master's programmes and award 5,000 certifications, creating a lasting European education program that trains cybersecurity experts, keeps their skills current, and makes sure everyone has access to quality training that matches what employers need.

EU-INSPIRE's mission is to respond to the need for addressing the multifaceted educational and vocational training needs critical to support the future EU Cyber Resilience ecosystem through an innovative three-fold approach:

- nurturing ICT personnel adept in leveraging AI-driven cybersecurity technologies to enhance the resilience of processes, systems, and digital infrastructures,
- cultivating cyber insurance specialists who possess a deep understanding of how cybersecurity and AI converge to protect cyber insurance policies, alongside expertise in deploying mechanisms for the assessment of cyber risks and threats, and
- empowering domain experts with sector-specific insights into digital transformation, who are proficient in applying cutting-edge AI solutions to cybersecurity conformity assessments. EU-INSPIRE is set to implement strategic mechanisms aimed at engaging a diverse array of industrial and research-driven communities ensuring the sustainability of the ecosystem beyond the end of the project through the development of a financially viable and cost-effective roadmap for establishing the EU-INSPIRE Academy. This institution is envisioned to serve as a cornerstone of the next-generation EU Cybersecurity Foundation, fostering synergies and integration with existing EU commitments aimed at mitigating the cybersecurity skills gap.

As partner in the EU-INSPIRE project, DNSC will ensure the coverage of the curricula with respect to policies and the compliance of the certifications to proposed policy recommendations. Highlights: (i) expertise in cybersecurity standards, regulations, and best practices; (ii) guidance on curriculum alignment, certification pathways, and industry accreditation, facilitating students' seamless transition into the workforce; (iii) hubs for technological innovation and entrepreneurship; (iv) expose students to emerging technologies, research collaborations, and industry partnerships; (v) access to state-of-the-art facilities, mentorship programs, and networking opportunities, fostering a culture of innovation and entrepreneurship among students.

The project directly contributes to achieving the Digital Decade targets and Europe's Digital & Green Transition by enhancing the security level of data and e-services operated by EU organisations, boosting economic growth for EU companies, facilitating the swift transition to digital transformation, expanding opportunities for students and professionals seeking careers in cybersecurity, providing top-notch training opportunities for students from various sectors and cultural backgrounds, and ensuring inclusiveness through Educational Mobility Grants that prioritize students with disabilities and those from low socio-economic backgrounds.



Funded by the
European Union



ENDURANCE

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe – ENDURANCE

Grant agreement no. 101168007

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of the **Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe – ENDURANCE** project, under the grant agreement no. 101168007. The project is financed through Horizon Europe Programme, by the granting authority: European Research Executive Agency (REA), under the call HORIZON-CL3-2023-INFRA-01 topic, type of action: HORIZON Innovation Actions³.

Amidst an increasingly interconnected and complex world, the provision of essential services remains crucial for the well-being of European citizens and the smooth functioning of the internal market. Yet, the ever-evolving landscape of risks, ranging from cyber threats, physical attacks, and human errors to natural disasters, demands a proactive and collaborative, pan-European approach to ensure disruption resilience. ENDURANCE is driven by the critical need to fortify Europe's essential services against potential disruptions, transcending the sole focus on the underlying critical assets.

Recognizing the significance of the Critical Entity Resilience (CER) and NIS2 Directives in setting the groundwork for resilience and, in

³ We thank PhD Claudia Lascateu for the presentation. The ENDURANCE project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement no. 101168007. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

parallel, the current silo approach to the Critical Infrastructure (CI) resilience and business continuity of essential services they provide, the project will assist the CI authorities across Europe in fully grasping and harmoniously implementing both directives.

To maximize the impact of our developments and projects' results, the Pan-European Working Group on Disruption Resilience (WGDR) will be created. The main direction of this expert networking is an information exchange ecosystem to feed the Critical Infrastructure Stakeholders' community with relevant best practices and new knowledge on improving the resiliency of their infrastructure. The ENDURANCE project responds to this need by bringing together a consortium of 23 partners from 7 European countries, which includes 7 authorities, 5 critical infrastructure operators from 6 key sectors and 11 entities with expertise in different domains. With a 36 months duration, launched in October 2024, this 5-million-euro EU-funded initiative is committed to developing interoperable solutions aimed at strengthening Europe's defences. The project will deliver robust methodologies, cutting-edge technologies, and strategic frameworks to build the resilience of critical infrastructures and ensure their capacity to recover from both physical and cyber incidents.

The Consortium is coordinated by EVIDEN TECHNOLOGIES SRL - Romania, having as partners: Engineering – Ingegneria Informatica Spa – Italy; Synelixis Lyseis Pliroforikis Automatismou & Tilepikoinonion Anonimi Etairia – Greece; SBT Poslovne Resitve Doo – Slovenia; Erevnitiko Panepistimiako Institouto Systimatou Epikoinonion Kai Ypologiston – Greece; Institut Za Korporativne Varnostne Studije Ljubljana – Slovenia; Agencija Za Komunikacijska Omrezja in Storitve Republike Slovenije – Slovenia; Urad Vlade Republike Slovenije Za Informacijsko Varnost – Slovenia; TELEKOM SLOVENIJE DD – Slovenia; Eles Doo Operater Kombiniranega Prenosnega In Distribucijskega Elektroenergetskega Omrezja – Slovenia; Directoratul National de Securitate Cibernetica – Romania; Ministerul Sanatatii – Romania; Directia Generala de Protectie Interna – Romania; Clinica Ginecologie dr. Muntean SRL – Romania; Regione Autonoma Friuli-Venezia Giulia – Italy; INSIEL - Informatica Per Il Sistema Degli Enti Locali S.P.A. – Italy;

Perifereiako Tameio Anaptyksis Attikis – Greece; Perifereiako Tameio Anaptyksis Perif Dytikis Ellados – Greece; Etaireia Ydreuseos Kai Apochetefseos Proteyoysis Anonimi Etaireia – Greece; TIMELEX – Belgium; Diadikasia Business Consulting Symvouloi Epicheiriseon AE – Greece; Carr Communications Limited – Ireland; Eviden Germany GMBH – Germany (Affiliated)

The consortium's solutions will be validated through cross-sector and cross-border pilot programmes in four EU Member States – Romania, Slovenia, Italy, and Greece, ensuring their effective implementation and harmonization across different national contexts. By facilitating collaboration between stakeholders and aligning efforts with the CER and NIS2 Directives, ENDURANCE is positioned to play a key role in securing Europe's infrastructures against a rapidly evolving threat landscape. ENDURANCE project's mission undertakes targeted activities related to:

(a) Enhance strategic cooperation and collaboration among the European CI stakeholders at all levels (bringing together 100+ relevant practitioners and experts across Europe);

(b) Develop datasets, registries, methodologies, technologies, and services (at TRL6-7) for secure sharing and federated processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness;

(c) Provide harmonised and pragmatic strategy for the continuity of the interconnected essential services (adopted by 20+ relevant European sectorial and national CI authorities).

Specific objectives of the project refer to:

Objective #1 – UNITY: Encourage, enhance, and support the all-level, pan-European strategic cooperation, operational collaboration, and continuous communication, enabling exchange of experience and best practices. We will organize 12 national and 3 European workshops with competent authorities from different EU Member States (MSs), CI operators, and other relevant CI stakeholders to establish a framework for understanding the current functioning of the European CI and provide cooperation mechanisms at different levels: local, regional, national, cross-border; within and across sectors; between public and

private entities; with governments and policy makers. The necessary data will be collected for the development and co-creation of ENDURANCE results. The workshops will be gradually transformed into the Working Group on Disruption Resilience (WGDR) with the aim of having more than 100 members by the end of the project.

Objective #2 – PREPAREDNESS WITH SERVICES: Establish a trusted data space for CER-relevant data and deliver user-friendly and interoperable services for (1) secure exchange and federated processing of such data, (2) essential-service-oriented digital twins, (3) continuous identification and assessment of risks and resilience, and (4) human-centric simulation and interactive training, empowering a broader community of CI stakeholders.

Objective #3 – PREPAREDNESS WITH STRATEGY: Align and improve current practices, policies, strategies, and business continuity plans by generating a harmonized Pan-European strategy for disruption resilience. This will include a) ordinary interpretation of CER definitions; b) harmonized methodologies for cross-x risk assessments and resilience for all hazards; c) guidelines for a coordinated and effective cross-x response to disruptions; d) new models for coordinated crisis communication in situations with societal impact (pandemic, political conflicts, economic crises, natural disasters, etc.)

Objective #4 – RESOLVE THROUGH TEST: Design and coordinate large-scale and cross-x exercises with CI authorities and operators to stress test their preparedness and ensure that our results are effective and pragmatic. These will be run within 5 strategic and operational pilots (4 countries, including Romania – MESO Pilot Disruption Resilience for Digital & Health – where intersectoral challenges at local, regional and national levels will be identified, analysed and addressed).

Objective #5 – PROMOTE: Promote the ENDURANCE mission, activities, and results to the relevant CI stakeholders across Europe and generate great positive, direct, tangible, and immediate impacts.

All project outcomes will be co-created and evaluated in relevant settings with a variety of CI authorities and operators from different EU Member States, thereby preparing the results for a real-world uptake across different critical sectors and countries.

“The CRA-AI project will build highly automated AI enabled software to support SMEs and Micro SMEs on every step of their journey to achieve compliance with the Cyber Resilience Act”

**Grant Agreement No. 101190243
(January 2025 - December 2026)**

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of **the CRA-AI project will build highly automated AI enabled software to support SMEs and Micro SMEs on every step of their journey to achieve compliance with the Cyber Resilience Act**, acronym CRA-AI project, under the grant agreement no. 101190243. The project is financed by the granting authority: European Cybersecurity Industrial, Technology and Research Competence Centre through the Digital Europe Programme, under the call DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA topic, type of action: DIGITAL JU SME Support Actions.

The digital transformation of businesses across Europe has made cybersecurity a fundamental concern. For small and medium-sized enterprises (SMEs) and micro-enterprises, achieving compliance with the Cyber Resilience Act (CRA)⁴ can be particularly challenging. Addressing this need, the CRA-AI project is set to provide an AI-driven, highly automated software platform that will simplify their compliance journey and enhance cybersecurity resilience across the European market.

The Cyber Resilience Act is a cornerstone of the EU Cybersecurity Strategy⁵, introducing a CE Mark for cybersecurity compliance. Manufacturers and service providers must demonstrate that their digital products adhere to strict security standards. However, as highlighted in

⁴ See details on <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.

⁵ See details on <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018>.

the EU Commission Impact Assessment⁶, compliance is a major challenge for many SMEs, due to limited resources and expertise. The CRA-AI project aims to bridge this gap by integrating automation and AI-driven tools to facilitate compliance efficiently and cost-effectively.

This project brings together leading cybersecurity institutions and technology partners across Europe, ensuring a robust and scalable solution. The consortium is coordinated by Cyber Cert Labs LTD (Ireland), having as partners: UAB NRD CS (Lithuania), 42SECURE (Belgium), Grit Solutions Sociedad Limitada (Spain), Directoratul National de Securitate Cibernetica (Romania), Protostars AI Software Limited (Ireland), Red Alert Labs (France). The project benefits from expertise of associate partnerships with: Munster Technological University (Ireland), National Cyber Security Centre (Ireland), and Ministerie Van Economische Zaken En Klimaat (The Netherlands).

The main objective of the CRA-AI project is to develop a user-friendly AI-powered platform that will guide SMEs through every step of their compliance journey. The platform will integrate four existing cybersecurity tools and introduce new AI-based automation features to reduce complexity and costs. The key functionalities of the platform include:

- **Product Inventory:** Establishing an inventory of all products, components and/or modules a product or software relies on including where required a Software Bill of Materials (SBOM). This will allow the user to define a Target of Evaluation (ToE) which will define the scope of the CRA assessment.
- **Risk Assessment:** Performing risk assessments on the product or software to determine how its users could be impacted by vulnerabilities. Establishing the protection profile of the product or service which will define the security controls required and alignment with the essential requirements in Annex 1. Threat Modelling and Analysis (TMA) will also be included in the software

⁶ See details on <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment>.

to clearly identify threats and potential vulnerabilities in the product or service.

- **Testing:** Based on the ToE and the documented protection profile the user can define a full set of test criteria for the product or service. This can include penetration testing, vulnerability management and secure code reviews.
- **Documentation:** Generating the required “Information and instructions to the user” as defined in Annex 2 of the CRA. This includes contact information for the manufacturer or distributor, details of the intended use and a user-friendly explanation of the protection profile and the security controls that support the protection profile.
- **Assessment:** The software will align to the EUCC scheme and any associated standards that are defined by the scheme. There are two forms of assessment, self-assessment, and conformity assessment. The software will prepare and generate all the documentation related to the definition of the ToE, the protection profiles, all tests executed by or on behalf of the manufacturer or distributor and any other relevant information. This is an important activity as a manufacturer or distributor can be asked for this by a surveillance authority at any time. Also, where a conformity assessment is required, this documentation provides the Conformity Assessment Body (CAB) with all the necessary information to assess the product or service.
- **Monitoring:** Providing the capability to monitor the product or service for any vulnerabilities that are discovered after the product or service has been placed on the market.
- **Vulnerability Disclosure:** When vulnerabilities or flaws are discovered in a product or piece of software, other software or product vendors who have relied on or embedded this as a component in their product need to be alerted so they can take appropriate action.

To maximize its impact, the CRA-AI project is structured into seven work packages: Project Management and Coordination, Dissemination, Product development – CRA workflow, Product

development – Vulnerability management, Product development – Secure code analysis, Product development – Human security, Pilot cases. By combining AI-driven automation with an intuitive, easy-to-use platform, the CRA-AI project will significantly lower compliance costs and streamline regulatory processes for SMEs. This will empower small businesses to meet cybersecurity requirements efficiently, ultimately strengthening the EU’s digital resilience.

The Romanian National Cyber Security Directorate is the leader of the dissemination activities, using the “Cyber Cert Labs Readiness Assessment” survey as part of a market scan for SMEs in Romania. The output of this market scan will help inform the product designers, produce a national level report on CRA readiness for SMEs, and link with other National Coordination Centres (NCCs). Based on the market scan, the workshops, webinars and the national event organised by DNSC will document a case study which will be available to the NCCs working groups, to raise awareness on the Cyber Resilience Act for SMEs⁷.

⁷ We thank PhD Claudia Lascateu for the presentation.

CALL FOR PAPERS *ROMANIAN INTELLIGENCE STUDIES REVIEW*

“Mihai Viteazul” National Intelligence Academy publishes the *Romanian Intelligence Studies Review* (RISR), a high-quality peer reviewed and indexed research journal, edited in English and Romanian twice a year.

The aim of the journal is to create a framework for debate and to provide a platform accessible to researchers, academicians, professional, practitioners and PhD students to share knowledge in the form of high quality empirical and theoretical original research papers, case studies, conceptual framework, analytical and simulation models, literature reviews and book review within security and intelligence studies and convergent scientific areas.

Topics of interest include but are not limited to:

- Intelligence in the 21st century
- Intelligence Analysis
- Cyber Intelligence
- Open Source Intelligence (OSINT)
- History and memory in Intelligence
- Security paradigms in the 21st century
- International security environment
- Security strategies and policies
- Security Culture and public diplomacy

Review Process: RISR shall not accept or publish manuscripts without prior peer review. Material which has been previously copyrighted, published, or accepted for publication will not be considered for publication in the journal. There shall be a review process of manuscripts by one or more independent referees who are conversant in the pertinent subject area. Articles will be selected based on their relevance to the journal’s theme, originality and scientific correctness, as well as observance of the publication’s norms. The

editor evaluates the recommendation and notifies the author of the manuscript status.

The review process takes maximum three weeks, the acceptance or rejects notification being transmitted via email within five weeks from the date of manuscript submission.

Date of Publishing: RISR is inviting papers for No. 35 and 36 and which is scheduled to be published on June and December, 2026.

Submission deadlines: February 1st and July 1st

Author Guidelines: Author(s) should follow the latest edition of APA style in referencing. Please visit www.apastyle.org to learn more about APA style, and <http://www.animv.ro> for author guidelines. For more details please access the official website: **animv.ro** and **rrsi.ro**.

Contact: Authors interested in publishing their paper in RISR are kindly invited to submit their **proposals electronically in .doc/.docx format at our e-mail address rrsi@sri.ro, with the subject title: article proposal.**