ACADEMIC FOCUS

Erasmus+ Mobility Projects at "Mihai Viteazul" National Intelligence Academy

In June 2024 "Mihai Viteazul" National Intelligence Academy (MVNIA) completed its 4th academic mobility project (KA131_2022) dedicated to the countries participating in the ERASMUS+ programme. The aforementioned project came as a natural follow-up to the KA103 mobility projects carried out in 2019 and 2020, respectively KA131 in 2021.

The objectives pursued within the KA131_2022 mobility project, a new stage in the development of the international dimention of MVNIA, were aligned with those stated in the Erasmus Guide and those established at the time of submitting the application for the Erasmus Charter: (1) promote lifelong learning by supporting four participants to improve the level of key competences (professional, cultural, linguistic); (2) increase the visibility of our institution among the European university community and exchanging good academic practices with other higher education institutions with similar profiles; (3) promote diversity, inclusion, equal opportunities and excellence; (4) improve the international dimension of vocational education and training through a better understanding of the practices, policies and education systems in the partner countries, thus contributing to the strengthening of a European Education Area; (5) increase the capacity the efforts to digitize the learning and teaching process, in a lingua franca, for a better adaptation to the requirements of the digital age; (7) foster and expand the previously established relations with higher education institutions and create new opportunities for training and promoting the accumulated knowledge through projects that will be submitted under other key actions.

MVNIA is actively involved in improving the quality of higher education, both nationally and internationally, considering the

uniqueness of the study programs offered. From this perspective, we believe that the partnership with higher education institutions with a similar profile through the funding offered within the KA131 mobility programme allow us to permanently orient ourselves towords streamlining activities and improving results in order to contribute to the development and consolidation of the European Education Area in the sector dedicated to security studies and international relations. The impact of the project implementation has had a ripple effect that was felt at all levels, ranging from the beneficiaries to the institutional one.

Moreover, the effects of the project have already become visible in processes such as updating the course and seminar materials used in the teaching process for those who were beneficieries of the teaching and training mobilities, or in the integration within the teaching process of new methods (e.g. gamification) that were picked up following various training mobilities.

It is beyond the shadow of a doubt that the 4th university mobility project has: led to an increase in the prestige and visibility of the MVNIA at national and European level; has allowed the strengthening of European partnerships, especially with Jagiellonian University from Krakow, Poland; has allowed the exchange of good practices, with facilitating the significant development of the professional, linguistic and intercultural competences of the participants.

Collectively, the four ERASMUS+ projects that have been implemented so far have encompassed a number of 14 beneficieries students and professors alike, who took part in different types of mobilities, as follows:

- 6 training mobilities;
- 4 traineeships;
- 2 teaching mobility
- 2 study mobility.

Moreover, MVNIA is currently implementing two more Erasmus+ KA131 mobility projects for which it has received funding under the 2023 and 2024 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.

Funded by the European Union

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 Actions[1].

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

[1] 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.

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 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 Systimaton 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 Anaptyxis Perif Dytikis Ellados – Greece; Etaireia Ydreyseos 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)[2] 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 Strategy[3], introducing a CE Mark for cybersecurity compliance.

[2] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018

Manufacturers and service providers must demonstrate that their digital products adhere to strict security standards. However, as highlighted in the EU Commission Impact Assessment[4], 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.

[4]https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-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 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 fo for SMEs[5].

[5] 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.**