ACADEMIC FOCUS

Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) H2020 Grant agreement no: 883054

(May 2020 – April 2025)

EU-HYBNET is a 60-month project (2020-2025), financed through the Horizon 2020, which start in May 2020. The project is being developed and implemented by a consortium of 25 partners, coordinated by LAUREA University of Applied Sciences from Finland. The European Centre of Excellence for Countering Hybrid Threats and the Joint Research Centre are leading partners of the EU-HYBNET project.

EU-HYBNET bring together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats, by undertaking an in-depth analysis of gaps and needs and prioritizing those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which lead to the creation of a roadmap for success and solid recommendations for uptake, industrialization and standardization across the European Union.

The project aims to build an empowered, sustainable network, which:

- define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavors;
- monitor significant developments in research and innovation;
- deliver recommendations for uptake and industrialization of the most promising innovations that address the needs

of practitioners, and determine associated priorities for standardization;

- establish conditions for enhanced interaction among its members;
- persistently strive to increase its membership and continually build network capacity through knowledge exchange.

EU-HYBNET address four core themes to ensure coherence in the project's results: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration and 4) Information and Strategic Communication.

Romania represents the consortium through "Mihai Viteazul" National Intelligence Academy (MVNIA). MVNIA incorporate the project's research findings and information into its MA & PhD research programs. As students come from diverse areas (security practitioners, legal, media, private business), the impact of exploitation of the information reach a wide audience, and the EU-HYBNET training documents will also be employed to enhance capabilities of experts and practitioners in the fight against hybrid threats.

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academia, industry players, and SME actors across EU, collaborating with each other to counter hybrid threats.

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.

DNS4EU and European DNS Shield – 21-EU-DIG-EU-DNS Grant agreement no. 101095329

(01.01.2023 – 31.12.2026)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of "DNS4EU and European DNS Shield – 21-EU-DIG-EU-DNS" 36 months-project financed through granting authority: European Health and Digital Executive Agency (Hadea), under the call CEF-DIG-2021-CLOUD topics, type of action: Connecting Europe Facility Infrastructure Projects.

The overall objective of the project is to *strengthen European technology sovereignty* offering and significantly improve the situation with recursive DNS servers in Europe. DNS-EU offers to EU citizens, businesses, and public administration a *comparable alternative to global services* such as Google or Cloudflare, but to go further and become a leader supporting newest technologies and standards while respecting a high level of security and privacy.

The DNS recursive service will be available for all internet users in Europe. The DNS4EU cloud resolver will be running in at least 14 localities in 13 various countries across the EU. Expected performance of the DNS4EU Cloud resolver is way above 1 million requests per second.

From the technological point of view, the project combines cloud and on-premises components delivered through publicly available resolvers and thanks to introduction into ISPs networks. This shall secure a significant adoption rate among residential, corporate, and public end-users in the EU. The maturity of the solution will be ensured by adopting latest security and privacy-enhancing standards.

The DNS will be easy to configure by the end users and supported via a wide range of applications and operating systems and will provide focused security protection for EU countries against malware and phishing without sacrificing speed and stability. The service will strictly be following EU privacy requirements.

The project aims to develop widely recognized solution that will be used by at least 100 million users across Europe over 5 years, 35 million of them during the project. This will disrupt the dominance of the current players. The consortium believes that thanks to its technological maturity and targeted communication activities, the project will become one of the successful flagships, like the .eu domain or eIDAS, which will set the direction not only in Europe but also globally.

Role of The Romanian National Cyber Security Directorate (DNSC) in the DNS4EU project. The Romanian National Cyber Security Directorate (DNSC) is specialised body of central public administration, subordinated to the Government and in the coordination of the Prime Minister, with legal personality, financed entirely from the state budget, through the budget of the General Secretariat of the Government.

At the national level, DNSC is the competent authority for the national civilian cyberspace, including the management of risks and cyber incidents. DNSC performs functions and responsibilities such as: national CSIRT; cyber security incident response team for IT products and services used in the government sector; national cyber security certification authority; analysis and forecasting; identification, evaluation, monitoring and mitigation of cyber risks at national level; the management function of projects and services for activities; research and development; strategy and planning; cooperation and collaboration; alerting, prevention, awareness, and training; national competent authority for regulation, supervision, and control.

In the DNS4EU and European DNS Shield Project we're dedicated to create user-friendly guides and materials, (interactive web application and audio-visual materials) and other support material with clear instructions for setting up DNS for individual devices such as browsers, operating systems (including mobile), home routers or smart home devices (e.g. game consoles). Our commitment extends to provide clear instructions and ensuring accessibility, and enhancing cybersecurity for EU Citizens.

We focus to ensure compliance with lawful filtering requirements by developing automated tools to streamline the process, preparing tools for automated coverage of the lawful filtering requirements including the lists of the domains and the proper wording for the blocking page and providing a platform that allows ISPs and DNS4EU to take a burden of lawful filtering compliance off them. That will have the capability to automatically update the blacklists and allow us to meet the national requirements. Also, we will assess operational security requirements, reporting platform compliance with legal security standards, and ultimately, operationalizing the platform while meeting cybersecurity criteria.

Considering our expertise as part of CSIRTs Network, DNSC's participation in the DNS4EU project will strengthen the collaboration with CERTs and CSIRTs at European level, endorsing their participation to enhance threat intelligence exchange, effectively addressing both global and local cybersecurity threats.[1]

[1] We thank PhD Claudia Lascateu for the presentation. Please see more details about the journal on www.joindns4.eu

Romanian Cyber Care Health (RO-CCH) CNECT.H – Digital Society, Trust, and Cybersecurity Grant agreement no. 101101522

(January 2023 – March 2025)

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a non-reimbursable financing for the implementation of the "Romanian Cyber Care Health - RO-CCH" project that is a 27-month project (2023-2025), financed through CNECT.H – Digital Society, Trust, and Cybersecurity, under the call DIGITAL-2022-CYBER-02-SUPPORTHEALTH topics, type of action: Digital SME Support Actions.

The Romanian Cyber Care Health – RO-CCH project will support cyber security resilience in the Romanian healthcare system and health institutions, which have been put under stress over the recent years, especially further to the COVID-19 crisis, in view of limiting the damage of safety-critical cyber security incidents which have affected health institutions and health services providers. The overall objective is to reduce cyber security risks to increase patient trust and safety in healthcare and health institutions.

The project will support cross-fertilisation among cyber security and healthcare communities of practices in order to increase the awareness of cyber security threats affecting healthcare and health institutions and to define collaboratively multi-disciplinary cyber security training schemes tailored to healthcare and health institutions environments and related healthcare system stakeholders, hence establishing the foundations for cyber security skills in health sector across the European Union.

It is expected that market-ready innovative cyber security solutions will be adopted, including provisions developed in the framework of EU-supported research and innovation projects. Furthermore, healthcare and healthcare institutions (SMEs in particular) will be equipped with up-to-date tools to protect themselves against cyber threats, as well as revised data sharing practices to improve security collectively. All these aspects are predicted to make a significant contribution to the overall Digital Europe Programme objectives.

The aims of the project titled "Romanian Cyber Care Health (RO-CCH) are:

- Reducing cybersecurity risks in the healthcare sector of Romania, focusing on protecting patient privacy and sensitive healthcare data from cyberattacks and human errors.
- Supporting the implementation of objectives under the NIS Directive for Romanian healthcare institutions, especially considering the increasing risks due to digital technology use, including big data, artificial intelligence, and machine learning.
- Promoting awareness and education in cybersecurity, not only within the healthcare sector but also among the general public, including children, to foster a culture of cybersecurity awareness.
- Increasing resilience against cyber threats and improving the healthcare system's capacity to manage and limit the impact of cyber incidents, especially given the pressures from events like the COVID-19 pandemic.
- Encouraging cross-border solutions and promoting the sharing of best practices and tools within the cybersecurity and healthcare communities to tackle vulnerabilities more effectively.

The RO-CCH project involves implementing an on-line designated application to enhance cybersecurity awareness and risk management within Romania's healthcare sector, aiming to provide tools and training to healthcare practitioners and end-users to safeguard patient data and healthcare services.

These efforts are intended to increase patient safety and trust in the Romanian healthcare system by addressing the cybersecurity challenges faced by healthcare providers and institutions.

The RO-CCH project[2] aims to reduce cybersecurity risks and enhance resilience in Romania's healthcare sector by addressing vulnerabilities related to digital technologies and human errors, while supporting the implementation of the NIS Directive. The project also focuses on raising awareness of cybersecurity threats, sharing best practices, and promoting cross-border collaboration to improve patient safety and trust in healthcare institutions.

[2] We thank PhD Claudia Lascateu for the presentation. Please see more details about the journal on https://dnsc.ro/project-ro-cch

Studia Securitatis Journal

ISSN: 1843-1925

ISSN L: 2821-5966

Journal Overview. Founded in 2007, *Studia Securitatis Journal* is a peer-reviewed academic journal dedicated to the field of security studies, primarily focused on topics related to national security, international relations, defence policies, and various dimensions of security studies. It serves as a platform for scholars, researchers, and professionals in the field to disseminate their findings, analyses, and theoretical discussions on a wide array of security-related topics. It is published biannually by the Lucian Blaga University of Sibiu, Faculty of Social Sciences and Humanities, under the Research Centre in Political Science, International Relations and European Studies, and the Department of International Relations, Political Science and Security Studies. The journal has evolved from its origins in the Faculty of Political Science, International Relations and European Studies, reflecting its strong academic foundation and commitment to advancing the discourse on security.

Indexing and Affiliations. *Studia Securitatis Journal* is internationally recognized and indexed in several databases, enhancing its visibility and academic impact. These include: ERIHPLUS, CEEOL, DOAJ, EBSCO, INDEX COPERNICUS, ULRICH'S PERIODICAL DIRECTORY, INFOBASE INDEX, SOCIONET, RESEARCHBIB, MIAR, and GLOBAL IMPACT & QUALITY FACTOR.

Scope and Focus. *Studia Securitatis Journal* encompasses a broad range of security-related topics, offering critical analyses at the international, national, community, and private levels. It provides a multidisciplinary platform for exploring security through various lenses, including military, economic, social, political, environmental, and cultural perspectives. The journal also covers emerging areas of concern, such as AI systems, cybersecurity, public diplomacy, misinformation, hybrid warfare, and more. The thematic diversity ensures that the journal remains at the forefront of contemporary security studies. It covers a broad spectrum of security-related issues, including but not limited to:

- **National Security.** Articles and research papers exploring the strategies, policies, and challenges faced by nations in safeguarding their sovereignty, territorial integrity, and public safety.
- **International Relations and Global Security.** In-depth analysis of geopolitical dynamics, international conflicts, peacekeeping operations, and the role of international organizations like the UN, NATO, etc., in maintaining global peace and security.
- **Hybrid Warfare. Cyber Warfare**. The effects of cyber-attacks in hybrid strategies, including examples of state-sponsored hacking, ransomware, and cyber espionage. The implications for national security and critical infrastructure; *Information Warfare and Propaganda* - the use of disinformation, fake news, and psychological operations to influence public opinion, undermine governments, and destabilize societies. *Economic Warfare* - economic tools, such as sanctions, trade wars, and financial manipulation, are used in hybrid conflicts to weaken adversaries. *Irregular Forces and Proxy Wars* - the use of non-state actors, militias, and private military companies in hybrid warfare to achieve strategic objectives without direct confrontation.

- **Defence and Military Studies.** Analysis on defence policies, military strategies, the development and procurement of defence technologies, and the role of armed forces in national and international contexts.
- **Terrorism and Counterterrorism.** Analyses of terrorist organizations, radicalization processes, and the various counterterrorism strategies employed by states and international coalitions.
- **Human Security.** Exploration of security from a broader perspective, including human rights, environmental security, food security, and public health as elements of global security.
- **International Public Law, International Humanitarian Law (IHL) and Armed Conflicts, Human Rights Law.** Provides a robust framework to explore various global security issues, particularly in the realms of peace, conflict resolution, human rights, and the role of international organizations. The impact of international legal frameworks on modern conflicts, such as the laws governing cyber warfare and autonomous weapons.
- **Security in Emerging Technologies (AI, IoT, Blockchain).** Studies related to the way how these technologies are reshaping the security landscape, creating new threats and vulnerabilities while also offering innovative solutions. This makes them critical subjects for security studies.

Theoretical and Methodological Contributions. Articles contribute to the theoretical frameworks and methodologies used in security studies, offering new approaches to understanding and analysing security issues.

Audience and Accessibility. The primary audience of *Studia Securitatis Journal* includes academics, researchers, policymakers, defence and security professionals, scholars of security studies, political science and international relations, and anyone with a deep interest in security studies. The journal is tailored for a global audience of academics, researchers, journalists, academia, and experts from both governmental and non-governmental organizations. In alignment with its mission to promote open access to research, *Studia Securitatis* does not impose any article processing charges (APCs) or submission fees, ensuring that financial barriers do not hinder the dissemination of knowledge. Authors retain copyright over their work, and articles are published under a Creative Commons license, making them freely accessible to the public.

Peer Review Process. As an academic journal, *Studia Securitatis* likely employs a peer-review process to ensure the quality and credibility of the articles it publishes. This process involves experts in the field reviewing submissions for originality, methodological rigor, and contribution to the field before they are accepted for publication

Availability. The journal is accessible in online formats, allowing for a broader dissemination of its content. The online ISSN (L 2821-5966) indicates that it has a digital presence, making its articles accessible to a global audience via academic databases, libraries, or the journal's own website.

Contribution and Impact. *Studia Securitatis Journal* plays a significant role in advancing the study and understanding of security issues. By providing a scholarly platform for the exchange of ideas and research, it contributes to the ongoing debates and developments within the field of security studies. It also helps bridge the gap between academic research and practical policymaking, offering insights that can inform and shape security strategies at both the national and international levels. Overall, *Studia Securitatis Journal* is a vital resource for anyone involved in or studying the multifaceted world of security, offering cutting-edge research and analysis on some of the most pressing issues of our time.

Collaboration between *Studia Securitatis Journal* and the International Conference "Human Security. Theoretical Approaches and Practical Applications"[3]. Starting from 2022, this represents a significant partnership in the field of security studies. This collaboration aims to bridge the gap between academic research and practical solutions in addressing contemporary security challenges. The International

[3] Source: https://conferences.ulbsibiu.ro/hstapa

Conference "Human Security. Theoretical Approaches and Practical Applications" serves as a vital forum where theoretical frameworks and real-world applications converge. Participants from diverse backgrounds, including academia, government, and non-governmental organizations, gather to discuss pressing security issues such as human rights, conflict resolution, and sustainable development. Through this collaboration, selected papers and key insights presented at the conference are published in the December issue of *Studia Securitatis Journal*, providing wider dissemination of cutting-edge research and innovative solutions. This partnership not only enhances the academic discourse on human security, but also promotes the practical implementation of these ideas in policymaking and on-the-ground initiatives. Overall, the synergy between *Studia Securitatis Journal* and the International Conference "Human Security. Theoretical Approaches and Practical Applications" enriches the field of security studies by fostering a dynamic exchange of knowledge that is both theoretically sound and practically relevant.[4]

[4] We thank Lecturer Nicoleta Munteanu for the presentation. Please see more details about the journal on https://magazines.ulbsibiu.ro/studiasecuritatis/

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. 33 and 34 and which is scheduled to be published on June and December, 2025.

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**

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.**