SELECTION NOTICE

CENTRE OF EXCELLENCE IN SECURITY AND SOCIETAL RESILIENCE

Description of the Centre of Excellence in Security and Societal Resilience

The Centre of Excellence in Security and Societal Resilience (ESSER-SECURE) has been established as a strategic academic partnership between the following universities: 'Mihai Viteazul' National Intelligence Academy (ANIMV – coordinator), Babeș-Bolyai University (UBB – partner 1), the University of Bucharest (UB – partner 2) and "Carol I" National Defence University (UNAp – partner 3). The Centre is funded under the UEFISCDI PN-IV-P6-6.1-CoEx-2024-0084 call for proposals through the project 'Developing social and security resilience by promoting excellence in research (ESSER – SECURE)'.

The ESSER-SECURE Centre supports excellence in research led by senior researchers (key persons) and contributions from PhD students and postdoctoral researchers. Research activities are carried out in a coordinated manner across the partner institutions, ensuring complementarity, optimisation of resources and interdisciplinary collaboration.

The ESSER-SECURE Centre's research agenda focuses on crime, terrorism and the protection of critical physical and digital infrastructure, addressing the interdependencies between these areas in the context of societal resilience, based on a thematic framework that underpins the organisation of the selection and evaluation process (set out in the Annex to this call for applications).

Job descriptions

'Mihai Viteazul' National Intelligence Academy is organising a competition to fill vacancies in the project 'Developing social and security resilience by promoting excellence in research (ESSER-SECURE)', PN-IV-P6-6.1-CoEx-2024-0084, for a fixed term (as set out in the project's funding application and the schedule of activities), on a part-time basis.
Positions:

- 1 senior researcher post (key person) – employment period August 2026–December 2030, working hours 4 hours/day
- 7 postdoctoral researcher posts – employment period August 2026–December 2026, working hours 4 hours per day
- 7 PhD student posts – employment period August 2026–December 2026, working hours 4 hours per day

Eligibility criteria:

For the senior researcher vacancy:

- Candidates must hold the academic rank of professor, associate professor or senior lecturer, or the research rank of senior researcher[1]
- Candidates must be employed by a higher education institution or a scientific research institution.

For junior researchers vacancies:

- Postdoctoral researchers – individuals who hold a PhD obtained no more than 8 years prior to the selection process.
- PhD students – PhD students who can provide proof of enrolment in a doctoral programme.

Application documents

For the position of senior researcher

- Academic CV;
- statement of research and supervision interests;
- plan for the dissemination and publication of research results (3–5 pages);
- selective list of publications;
- certificate attesting to the applicant's academic or research qualification and their status as a tenured member of staff at a higher education or research institution;
- evidence of the ability to lead research and of the results thereof;
- identity card (other documents, where applicable: marriage certificate, document certifying a change of name, etc.).

For postdoctoral research positions

- a CV in Europass format, including a list of published works;
- a research proposal setting out the chosen topic, methodology, scientific literature to be used, the link between the proposed research topic and the research themes of the ESSER-SECURE Centre, as well as a plan for disseminating and publishing the research results (2–3 pages);
- a copy of the PhD degree certificate;
- identity card (other documents, if applicable: marriage certificate, document certifying a change of name, etc.)

[1] In accordance with Article 9(1) of Law No. 183/2024.

For PhD student positions

- a CV in Europass format;
- a research proposal setting out the chosen topic, methodology, the scientific literature to be used, the link between the proposed research topic and the research themes of the ESSER-SECURE Centre, as well as a plan for the dissemination and publication of the research (2–3 pages);
- certificate of PhD student status issued by the Doctoral School, confirming enrolment in a doctoral programme;
- identity card (other documents, if applicable: marriage certificate, document certifying a change of name, etc.)

Selection timetable

Stage	Description	Duration
1	Publication of the call for applications	13 July
2	Application submission period	13–28 July
3	Verification of administrative eligibility	29 July
4	Scientific evaluation of applications	30–31 July
5	Interviews	3 August
6	Final assessment and ranking	4 August
7	Notification of results	4 August
8	Submission of appeals (if applicable)	4–6 August
9	Review of appeals lodged (if applicable)	7 August
10	Final ranking, preparation and signing of the contract	7 August

To apply for the competition, interested candidates must email the following documents to dodoiu.valentina@animv.eu by 28 July 2026 at 16:00:

1. the application form for the competition, specifying the type of post for which they are applying;

2. the documents specific to each type of position.

Selection procedure

The selection procedure will ensure fairness, transparency and methodological consistency, and will include:

1. the preliminary check of administrative eligibility, carried out by the designated secretary of the Selection Committee at the time of registration – elimination stage. Candidates whose applications are deemed compliant following the preliminary check of administrative eligibility proceed to the scientific assessment stage.
2. scientific assessment of the application documents, carried out by the Selection Committee;
3. interview.

The following criteria will be applied during the selection process:

Category	**Criterion**	**Weighting**	**Visual weighting**
PhD students	Academic and research achievements	10%	10%
	Oral presentation skills	25%	25%
	Relevance of the proposal to the Centre's research themes	25%	25%
	Quality of the research proposal	40%	40%
Postdoctoral researchers	Academic and research achievements	25%	25%
	Oral presentation skills	10%	10%
	Relevance of the proposal to the Centre's research themes	25%	25%
	Quality of the research proposal	40%	40%
	Relevance of academic and professional	40%	40%

Category	Criterion	Weighting	Visual weighting
Senior researchers	achievements to the Centre's research themes		
	Oral presentation skills	20%	20%
	Research experience and experience in supervising/mentoring junior researchers	40%	40%

Assessment guidelines:

- Oral presentation – each candidate will present their research topic, methodology and expected results in a 10-minute session.
- Weighted scoring – the weights assigned to each criterion reflect their relative importance in the final assessment.
- Research alignment – it is essential to demonstrate alignment with the research priorities of the ESSER-SECURE Centre.
- Score accuracy – scores will be calculated to two decimal places, with the final ranking determined by the total weighted score.

Each candidate's final average will be calculated as a weighted average of the scores obtained for the specific evaluation criteria. The final mark will be calculated by multiplying the score obtained for each criterion by its respective weighting and summing the results; candidates will be ranked in descending order of their final averages. The candidate who has obtained the highest final mark will be declared successful, provided that they have achieved the minimum required mark of 70 points.
In the event of a tie in final scores, priority is given to the candidate with the higher score for the research proposal.

Communication and appeals regarding the results

The results of the competition will be published on the official ANIMV website (www.animv.ro) on 4 August 2026, indicating the registration number of the application.
Candidates may lodge appeals within 2 working days (5–6 August 2026) of the results being published. Appeals may relate only to the first stage of the competition. Appeals must be sent to the email address dodoiu.valentina@animv.eu.
Appeals will be resolved on 7 August 2026.
Further information can be obtained by emailing dodoiu.valentina@animv.eu.

Annex nr.1

RESEARCH TOPICS FOR PHD, POSTDOCTORAL AND SENIOR RESEARCHERS IN ESSER-SECURE CENTER OF EXCELLENCE

1. Future Violent Extremism and Radicalisation

Romania and CEE Early-Warning Cases

This research area investigates how radicalisation and violent extremism evolve in technologically transformed societies and how early-warning systems can be developed.

1.1 Emerging Radicalisation Pathways

- Online and hybrid radicalisation trajectories
- Cross-platform extremist ecosystems
- New forms of ideological mobilisation
- Extremism in gaming and virtual environments
- Romanian and CEE-specific radicalisation patterns

1.2 Youth, Identity and Vulnerability

- Identity crises and radicalisation
- Youth exposure to extremist narratives
- Education and prevention strategies
- Digital citizenship and resilience
- Romanian youth attitudes and vulnerability indicators

1.3 Technology and Extremism

- AI-generated extremist content
- Deepfakes and synthetic propaganda
- Algorithmic amplification of extremist narratives
- Emerging technologies and recruitment mechanisms

1.4 Early Warning and Prevention

- Detection indicators for radicalisation
- Behavioural and social markers
- Community-based prevention models
- Development of Romanian and regional early-warning frameworks

1.5 Comparative Extremism in CEE and the Black Sea Region

- Regional trends and similarities
- Influence of geopolitical tensions
- Importation and adaptation of extremist narratives
- Comparative case studies (Romania, Bulgaria, Poland, Hungary, Moldova etc.)

2. Crime–Terror–Hybrid Threat Nexus

Romania Validation Environment

This research area explores the convergence of criminal, terrorist, cyber, and hybrid actors.

2.1 Organised Crime Transformation

- AI-enabled organised crime
- Digital illicit markets
- Criminal innovation ecosystems
- Evolution of criminal networks in Romania and the region

2.2 Crime-Terror Convergence

- Financial and logistical intersections
- Shared infrastructures and facilitators
- Networked hybrid actors
- Comparative validation of nexus theories

2.3 Hybrid Threat Ecosystems

- State and non-state cooperation
- Proxy actors and influence networks
- Hybrid coercion mechanisms
- Regional hybrid threat mapping

2.4 Illicit Flows and Security

- Trafficking routes and logistics
- Migration-security intersections
- Cross-border criminal activities
- Romania as transit and gateway environment

2.5 Intelligence and Threat Assessment

- Detection of convergent threat ecosystems
- Network analysis applications
- Strategic warning methodologies
- Hybrid threat indicators

3. Critical Infrastructure Resilience. Social and Human Dimensions of Cybersecurity

Romania Frontier Testbed

This research area focuses on resilience beyond technology by integrating organisational, societal, and behavioural dimensions.

3.1 Critical Infrastructure Security and Resilience

- Energy systems resilience
- Transport and logistics security
- Communications and digital infrastructure
- Black Sea infrastructure vulnerabilities

3.2 Human Factors in Cybersecurity

- Human error and cyber incidents
- Cybersecurity culture
- Insider threats
- Security behaviour and decision-making

3.3 Organisational Cyber Resilience

- Leadership and cyber resilience
- Crisis management during cyber incidents
- Organisational adaptation
- Cyber resilience maturity assessment

3.4 Public Perceptions and Cybersecurity

- Citizen understanding of cyber risks
- Trust in digital services
- Cybersecurity awareness
- Digital resilience in Romanian society

3.5 Cybersecurity Workforce and Competencies

- Future cybersecurity competencies
- Skills shortages and talent development
- AI and workforce transformation
- Professionalisation frameworks

4. Information Manipulation and Cognitive Security

Romanian-Language Ecosystem Focus

This research area studies how information environments shape perceptions, trust, and resilience.

4.1 Foreign Information Manipulation and Interference (FIMI)

- Narrative ecosystems
- Influence operations
- Strategic communication
- Romania and Black Sea information environments

4.2 Cognitive Security and Trust

- Trust and distrust dynamics
- Epistemic security
- Conspiracy theories
- Institutional legitimacy

4.3 Polarisation and Democratic Resilience

- Social fragmentation
- Identity-based narratives
- Electoral information environments

- Democratic vulnerabilities

4.4 AI and Information Manipulation

- Synthetic media
- Deepfakes
- Automated influence campaigns
- AI-enhanced disinformation

4.5 Measuring Information Resilience

- Indicators of societal resilience
- Information literacy assessment
- Narrative monitoring tools
- Romanian and regional resilience benchmarking

5. National and Societal Resilience in the AI Era

Romania Transformation Trajectory

This research area investigates how societies adapt to technological disruption and strategic uncertainty.

5.1 Conceptualising Resilience

- National resilience models
- Domains of societal resilience (e.g., security, ecological, economic, technological etc.)
- Levels of resilience: societal, community, organisational, individual
- Resilience indicators
- Comparative resilience frameworks

5.2 AI and Societal Transformation

- Governance implications of AI
- Labour market disruption
- Social adaptation processes
- Public attitudes toward AI

5.3 Democratic Resilience in Technological Societies

- Governance under technological disruption
- Trust in institutions
- Digital citizenship
- AI and democratic accountability

5.4 Community and Local Resilience

- Urban resilience
- Rural resilience
- Vulnerable communities
- Regional disparities in Romania

5.5 Black Sea and Regional Resilience

- Cross-border resilience frameworks
- Regional crisis management
- Lessons from neighbouring states
- Romania as resilience hub

5.6 National and Allied Military Resilience

- Concepts, policies, and doctrines
- Command and control resilience
- Logistics resilience, including technical and material support, mobility and sustainment
- Cyber and communications resilience
- Strategic communication and information resilience within defence organisations
- Human factors in military resilience, including morale, cohesion and leadership
- Force generation and regeneration
- Civil-military cooperation and support to civilian authorities
- Civil resistance and support for military operations

5.7. The Role of Armed Forces in Whole-of-Society Approach to Resilience

- The role of military organisations in critical infrastructure protection
- Lessons identified and lessons learned from military support to societal resilience

6. Methodologies in Mapping and Investigating Security Processes: From Diagnosis to Foresight and Anticipatory Approaches

All Topics Transversal Methodological Approach

This section is dedicated to the development, testing, and validation of methodological frameworks, analytical tools, and research approaches that can support all other research areas of the Centre. It seeks to strengthen the scientific foundations of security and resilience research by advancing methodologies for diagnosis, assessment, mapping, monitoring, forecasting, and anticipation. As a transversal area, it is designed to generate methodological innovations applicable across the Centre's thematic portfolio and to facilitate the integration of knowledge, data, and analytical approaches across different security domains.

6.1 Security Diagnosis and Assessment

- Threat assessment methodologies
- Vulnerability assessment frameworks
- Security auditing and evaluation
- Diagnostic models for resilience

6.2 Mapping Security Ecosystems

- Network analysis
- Ecosystem approaches
- Actor mapping methodologies
- Complex systems analysis

6.3 Intelligence Methodologies

- Structured analytic techniques
- Strategic warning methodologies
- Intelligence support to resilience
- Intelligence-performance assessment

6.4 Security Foresight and Futures Studies

- Horizon scanning
- Emerging issues analysis
- Scenario development
- Alternative futures methodologies

6.5 Anticipatory Governance

- Early-warning systems
- Anticipatory policy-making
- Risk governance
- Strategic adaptation models

6.6 AI and Advanced Security Analytics

- AI-assisted intelligence analysis
- Predictive analytics
- Big data applications
- Human–AI analytical collaboration

6.7 Security Competencies and Professional Development

- Resilience competencies
- Security education and training
- Competency frameworks for the AI era