ANUNȚ DE SELECȚIE

CENTRUL DE EXCELENȚĂ ÎN DOMENIUL SECURITĂȚII ȘI REZILIENȚEI SOCIETALE

Descrierea Centrului de Excelență în Securitate și Reziliență Societală

Centrul de Excelență în Securitate și Reziliență Societală (ESSER-SECURE) este înființat ca un parteneriat academic strategic între următoarele universități: Academia Națională de Informații „Mihai Viteazul” (ANIMV - coordonator), Universitatea Babeș-Bolyai (UBB – partener 1), Universitatea din București (UB – partener 2) și Universitatea Națională de Apărare „Carol I” (UNAp – partener 3). Centrul este finanțat în cadrul competiției UEFISCDI PN-IV-P6-6.1-CoEx-2024-0084 prin proiectul „Dezvoltarea rezilienței sociale și de securitate prin promovarea excelenței în cercetare (ESSER - SECURE)”.

Centrul ESSER-SECURE susține excelența în cercetare condusă de cercetători seniori (key persons) și contribuții ale cercetătorilor doctoranzi și cercetători postdoctorali. Activitățile de cercetare sunt implementate în mod coordonat în cadrul instituțiilor partenere, asigurând complementaritatea, optimizarea resurselor și colaborarea interdisciplinară.

Agenda de cercetare a Centrului ESSER-SECURE se concentrează pe criminalitate, terorism și protecția infrastructurilor fizice și digitale critice, abordând interdependențele dintre aceste domenii în contextul rezilienței societale, în baza unei tematici care stă la baza organizării procesului de selecție și evaluare (prezentată în Anexă la prezentul apel la candidaturi).

Descrierea posturilor

Academia Națională de Informații „Mihai Viteazul” organizează concurs pentru ocuparea unor posturi vacante în cadrul proiectului „Dezvoltarea rezilienței sociale și de securitate prin promovarea excelenței în cercetare (ESSER-SECURE)”, PN-IV-P6-6.1-CoEx-2024-0084, pe perioadă determinată (stabilită conform cererii de finanțare a proiectului și graficului de realizare a activităților), pe durată determinată și cu normă de muncă parțială.

Posturi:

- 1 post cercetător senior (key person) – perioada de angajare august 2026-decembrie 2030, norma de muncă 4 ore/zi;
- 7 posturi cercetători postdoctorali – perioada de angajare august 2026-decembrie 2026, norma de muncă 4 ore/zi;
- 7 posturi studenți doctoranzi – perioada de angajare august 2026-decembrie 2026, norma de muncă 4 ore/zi.

Criterii de eligibilitate:

Pentru postul vacant de cercetător senior:

- Candidații dețin gradul didactic de profesori universitari, conferențiari universitari, lectori universitari sau gradul de cercetare de cercetători seniori[1];
- Candidații sunt încadrați într-o instituție de învățământ superior sau într-o instituție de cercetare științifică.

Pentru posturile vacante pentru cercetători juniori:

- Cercetători postdoctorali – persoane care dețin o diplomă de doctorat obținută cu cel mult 8 ani înainte de concursul de selecție.
- Studenți doctoranzi – studenți doctoranzi care fac dovada înmatriculării într-un program de studii universitare de doctorat.

Documente de candidatură

Pentru postul de cercetător senior

- CV academic;
- declarație privind interesele de cercetare și de îndrumare;
- plan de diseminare și publicare a rezultatelor cercetării (3-5 pagini);
- listă selectivă de publicații;
- adeverință care să ateste gradul didactic universitar sau de cercetare științifică deținut și calitatea de titular într-o instituție de învățământ universitar sau de cercetare științifică;
- dovezi privind capacitatea de conducere a cercetării și rezultatele acesteia;
- carte de identitate (alte documente, dacă e cazul: certificat de căsătorie, document care atestă schimbarea numelui etc.).

Pentru posturile de cercetători postdoctorali

- curriculum vitae în format Europass, inclusiv lista de lucrări publicate;
- propunere de cercetare care să prezinte tema aleasă, metodologia, literatura științifică care va fi utilizată, legătura dintre tema de cercetare propusă și temele de cercetare ale Centrului ESSER-SECURE, precum și un plan de diseminare și publicare a rezultatelor cercetării (2-3 pagini);
- copie a diplomei de doctorat;
- carte de identitate (alte documente, dacă e cazul: certificat de căsătorie, document care atestă schimbarea numelui etc.)

[1] În conformitate cu Legea nr. 183/2024, articolul 9 alineatul (1).

Pentru posturile de studenți doctoranzi

- curriculum vitae în format Europass;
- propunere de cercetare care să prezinte tema aleasă, metodologia, literatura științifică care va fi utilizată, legătura dintre tema de cercetare propusă și temele de cercetare ale Centrului ESSER-SECURE, precum și un plan de diseminare și publicare a cercetării (2-3 pagini);
- adeverința statutului de student doctorand eliberat de Școala Doctorală, care să ateste înmatricularea într-un program de studii universitare de doctorat;
- carte de identitate (alte documente, dacă e cazul: certificat de căsătorie, document care atestă schimbarea numelui etc.)

Calendarul de selecție

Etapa	**Descriere**	**Durată**
1	Publicarea cererii de candidaturi	13 iulie
2	Perioada de depunere a candidaturilor	13-28 iulie
3	Verificarea eligibilității administrative	29 iulie
4	Evaluarea științifică a cererilor	30-31 iulie
5	Interviuri	3 august
6	Evaluare finală și clasificare	4 august
7	Notificarea rezultatelor	4 august
8	Depunerea contestațiilor (dacă este cazul)	4-6 august
9	Analizarea contestațiilor depuse (dacă este cazul)	7 august
10	Clasamentul final, pregătirea și semnarea contractului	7 august

Pentru înscrierea la concurs, persoanele interesate vor transmite pe adresa de email dodoiu.valentina@animv.eu, 28.07.2026 ora 16:00, următoarele documente:
1. cererea de înscriere la concurs cu specificarea tipului de post pe care se înscriu;
2. documentele specifice fiecărui tip de post.

Procedura de selecție

Procedura de selecție va asigura echitatea, transparența și coerența metodologică și va include:

1. verificarea preliminară a eligibilității administrative, efectuată de secretarul desemnat al Comisiei de concurs în momentul înregistrării – etapă eliminatorie. Candidații ale căror dosare sunt declarate conforme ca urmare a verificării preliminare a eligibilității administrative, intră în etapa de evaluare științifică.
2. evaluarea științifică a documentelor de candidatură, efectuată de Comisia de concurs;
3. interviu.

În procesul de selecție vor fi aplicate următoarele criterii:

Categorie	**Criteriu**	**Ponderere**	**Pondere vizuală**
Studenți doctoranzi	Realizări academice și de cercetare	10%	10%
	Abilități de prezentare orală	25%	25%
	Relevanța propunerii pentru temele de cercetare ale Centrului	25%	25%
	Calitatea propunerii de cercetare	40%	40%
Cercetători postdoctorali	Realizări academice și de cercetare	25%	25%
	Abilități de prezentare orală	10%	10%
	Relevanța propunerii pentru temele de cercetare ale Centrului	25%	25%
	Calitatea propunerii de cercetare	40%	40%
	Relevanța realizărilor academice și profesionale	40%	40%

Categorie	Criteriu	Pondere	Pondere vizuală
Cercetători seniori	pentru temele de cercetare ale Centrului		
	Abilități de prezentare orală	20%	20%
	Experiență în cercetare și experiență în supervizarea/îndrumarea cercetătorilor juniori	40%	40%

Linii directoare de evaluare:

- Prezentare orală – fiecare candidat va prezenta tema de cercetare, metodologia și rezultatele așteptate într-o sesiune de 10 minute.
- Punctaj ponderat - ponderile atribuite fiecărui criteriu reflectă importanța relativă a acestora în evaluarea finală.
- Alinierea cercetării - este esențială demonstrarea alinierii la prioritățile de cercetare ale Centrului ESSER-SECURE.
- Precizia punctajului – punctajele vor fi calculate cu două zecimale, clasamentul final fiind determinat de punctajul ponderat total.

Media finală a fiecărui candidat va fi calculată ca o medie ponderată a punctajelor obținute pentru criteriile de evaluare specifice. Nota finală se va calcula prin înmulțirea punctajului obținut la fiecare criteriu cu ponderea aferentă și însumarea rezultatelor, candidații fiind ierarhizați în ordinea descrescătoare a mediilor finale. Va fi declarat admis candidatul care a obținut cel mai mare punctaj final, cu condiția ca acesta să fi obținut punctajul minim necesar de 70 de puncte.
La punctaje finale egale are prioritate candidatul cu punctajul mai mare la propunerea de cercetare.

Comunicarea și contestarea rezultatelor

Rezultatele concursului vor fi afișate pe pagina oficială de internet a ANIMV (www.animv.ro) în data de 04.08.2026, cu indicarea numărului de înregistrare al dosarului de concurs.
Candidații pot formula contestații în termen de 2 zile lucrătoare (5-6 august 2026) de la afișarea rezultatelor. Contestațiile pot viza doar prima etapa a concursului. Contestațiile se vor transmite pe adresa de email dodoiu.valentina@animv.eu.

Contestațiile se soluționează pe 7 august 2026.

Informații suplimentare pot fi obținute pe adresa de e-mail dodoiu.valentina@animv.eu.

Anexa nr.1

RESEARCH TOPICS FOR RECRUITMENT, SELECTION AND RETENTION METHODOLOGY FOR PHD, POSTDOCTORAL AND SENIOR RESEARCHERS

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