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
- Community resilience
- 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

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