



Title of the study programme	Micro-Credential in Countering Hybrid Threats
Study level	Master's studies
Learning environment	Online: August 30- December 7, 2024 Face-to-face: December 09-13,2024 in Tallinn, Estonia
European Qualifications Framework Level	Level 7
ECTS Credits	21 ECTS
Language	English

CALL FOR APPLICATION OF MICRO-CREDENTIAL PROGRAMME IN COUNTERING HYBRID THREATS

IMPLEMENTED BY THE ESTONIAN ACADEMY OF SECURITY SCIENCES, MYKOLAS ROMERIS UNIVERSITY(LITHUANIA) AND POLICE ACADEMY OF THE MINISTRY OF THE INTERIOR OF THE REPUBLIC OF CROATIA

Background and Rationale

The Joint Micro-Credential Programme in Countering Hybrid Threats has been created with the support of the Erasmus+ project in cooperation with the Estonian Academy of Security Sciences (the EASS), Mykolas Romeris University (MRU) of Lithuania and the Police Academy of the Ministry of the Interior of the Republic of Croatia.

Hybrid threats are one of the emerging security challenges with the potential to shape the future of the continent in the worst-case scenario. They are defined by the European Union as actions that use diplomatic, military, economic and technological tactics to destabilize a political opponent. Pressure, disinformation, and criminal use of Communications and Information Systems (CIS) are some examples of hybrid threats. They are designed to be difficult to detect or attribute.

Hybrid threats have not only come to stay, but they are also endlessly evolving: the so-called hybrid toolbox is constantly being updated. Some examples of hybrid attacks affecting the European Union are the referendum on the status of Crimea; the sudden massive influx of illegal migrants from the Russian Federation across the Arctic border into the Kingdom of Norway and the Republic of Finland in 2015-2016 (often at -30 degrees outside); the situation in which the Belarusian authorities created an artificial migration crisis. These are some of the examples of neighbouring countries demonstrating their ability to use the movement of people to increase their political and economic leverage over the Union, primarily against Lithuania, Latvia, Poland and Finland.



Funded by
the European Union

Russia's propaganda narratives and conspiracy theories show Russia as a hero in the COVID crisis aiming to show that the West could not cope with the crisis etc. The methods for achieving the hybrid effect are different and are usually used simultaneously. While cyber-attacks, customs restrictions, political pressure or fake news can be considered direct hybrid attacks, there are also more covert methods such as the use of local sanctions, soft films, music videos or books, children's summer camps, etc.

Awareness of hybrid threats and the development of resilience are continuously being developed, both within the European Union institutions and in cooperation with various partners. There is more common language and mutual understanding in this area than ever before. However, it covers a high political level, but does not cover all areas of hybrid threats and needs wider, knowledge-based dissemination. These threats are no longer a problem for just one, neither is the solution. Interoperability evolves in an efficient path only if all actors get involved in the creation of the new tools and solutions, all the players acting in the game. All agents should speak the same language and act as one single strong answer to the citizens.

Hybrid threat research, up-to-date training and public awareness are of key importance to combating hybrid threats. Officials and decision-makers, as well as businesses, senior executives and the public who are aware of and understand the dangers, are our strength and improve our resilience to hybrid threats.

Some specialities related to the handling of hybrid threats are taught in universities of the European Union Member States, as well as in applied law and defence training institutions, but these studies are either military-oriented or closed, with only a small part of the entire curriculum and open access. Hybrid attacks affect and can paralyze society as a whole or individual parts of it, either at a national or regional level. There is a broad understanding in the European Union of the challenges we face in the form of hybrid threats. Development of a Joint Micro-Credential Programme in Countering Hybrid Threats jointly in different universities in the European Union corresponds to the needs of the current and future security environment. This cooperation created a platform for exchanging experiences and enhancing competence by providing up-to-date knowledge and the critical analytical and administrative capacity at the strategic level, which is essential for making complex management decisions in a changing society, including in countering hybrid threats.

Aim of studies

Studies aim to develop students' strategic thinking skills to be able to comprehend and cope with challenges and controversies related to hybrid threats in the modern internal security area.

Upon completion of this curriculum, the student:

- has a systematic overview and broad knowledge of contemporary hybrid threats, forms of their appearance, risks, challenges and trends arising from globalisation and their influence on regional and national internal and border security;
- promotes respect for fundamental rights, professional and ethical standards, while ensuring internal security;
- demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats

Upon successful completion of studies, students will be awarded with joint Certificate signed by all Partner Universities: Estonian Academy of Security Sciences (the EASS), Mykolas Romeris University (MRU) of Lithuania and the Police Academy of the Ministry of the Interior of the Republic of Croatia.

Target Group and Entry Requirements

The target group of the course comprises managers, officials and employees of Border Guard, Internal Security, Police Institutions and related fields of the Nordic and Baltic, Schengen and Associated countries, as well as other European Union Member States who wish to acquire a broader knowledge of European Union internal security and hybrid threats and who envision their future careers in this field.

Entry requirements:

The admission requirements for this course are that those candidates must possess and present via e-mail:

- **Copy of Bachelors' degree (BA) Diploma** of Professional Higher Education or a corresponding qualification ;
- **Certificate** of English proficiency at B2 level ; in addition, online platform for English language self-test will be provided
- **Motivational letter**, proving willingness to study in an international environment
- Scanned **copy of ID** document (ID card or passport)
- **CV** of an applicant.

Two years of professional work experience in internal security or a related field is an advantage.

All documents must be in English and sent to e-mail address HYBRIDC@sisekaitse.onmicrosoft.com

Selection procedure:

Deadline for application is May 01, 2024.

The suitability and matriculation of the nominated candidates are decided by the Course Program Committee. All applicants will be interviewed online by Course Program Committee. The acceptance of students will be decided by this Committee consisting of two representatives of each Consortium Partner.

Interviews with applicants will be conducted between **May 20-31, 2024.**

Results of selection procedure will be announced by **June 15, 2024.**

Student Agreement will be signed with each student until **June 30, 2024**

Tuition Fee, Travel Cost and Accommodation

There is no tuition fee for the micro-credential programme in 2024. Due to the programme being part of a project funded by Erasmus+, applicants can focus solely on covering their travel and accommodation costs for the onsite week in Tallinn from December 9-13, 2024. Accommodation is not provided for the contact week.

Calendar Plan of Studies

Activity	Dates
Opening lecture (online)	August 30, 2024
Module 1, 10 ECTS (260 learning hours)	
Session 1. Hybrid threats: concept, definitions and wider interpretations	
Independent learning: 36 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Drafting the outline of the written analysis (Sessions 1, 2, 3 and 6) 	September 02 -06, 2024
Contact learning (online): 10 hours Lectures, seminars	September 06, evening 2 hrs September 07, 2024
Session 2. Hybrid threats and security strategies	
Independent learning: 27 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Drafting the outline of the written analysis (Sessions 1, 2, 3 and 6) 	September 09- 13, 2024
Contact learning (online): 8 hours Lectures, seminars	September 14, 2024
Session 3. Policy and regulation	
Independent learning: 33 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Drafting the outline of the written analysis (Sessions 1, 2, 3 and 6) 	September 16-20, 2024
Contact learning (online): 8 hours	September 21, 2024
Session 4. Warfare in the context of hybrid threats	
Independent learning: 33 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Preparation for the case study (tendencies of contemporary warfare and information warfare) 	September 23-27,2024
Contact learning (online): 14 hours	September 27,2024- 4 hrs September 28, 2024-10 hrs
Session 5. Information warfare	

Independent learning: 33 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Preparation for the case study (tendencies of contemporary warfare and information warfare) 	September 30- October 04,2024
Contact learning (online): 14 hours	October 04, 2024 - 4 hrs October 05, 2024- 10 hrs
Session 6. Common response to hybrid threats and strategies for tackling them	
Independent learning: 38 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Completing self-assessment tasks - Drafting the outline of the written analysis (Sessions 1, 2, 3 and 6) 	October 07 - October 11,2024
Contact learning (online): 6 hours	October 12,2024
Assessments (6 hours, online): <ul style="list-style-type: none"> - Solving the case study (tendencies of contemporary warfare and information warfare) - Written analysis preparation and submission. 	Oct 19 October 19, 2024
Individual consultations (7 hours, online)	According to individual agreements
Reassessments	October 26, 2024 - deadline for liquidation of student debts

Module 2, 11 ECTS (286 learning hours)	Dates
Session 1. European Union's external dimension in countering hybrid threats Session 2. Border security and management	
Independent learning: 55 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials. - Taking a self-assessment test (a multiple-choice test) about the European Union's external dimension in countering hybrid threats and border security and management. - Participation in forum discussions. 	October 21 - 31, 2024
Contact learning, online: 15 hours Lectures, seminars	November 01 - 02, 2024
Contact learning face-to-face: 10 hours (Session 2) Lectures, seminars	December 09 - 11, 2024, Tallinn
Session 3. Protection of critical infrastructure Session 4. Countering information advocacy and influence activities	
Independent learning: 66 hours <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials and complete self-assessment tasks. 	November 04 - 15, 2024

<ul style="list-style-type: none"> - Participation in forum discussions about actions countering information advocacy and influence activities; - Participation in forum discussions about psychological aspects related to radicalisation and different forms of extremism on social media. <p>Contact learning, online: 5 hours Lectures, seminar</p> <p>Contact learning (face-to-face): 6 hours (Session 4) Lectures, seminars</p>	<p>November 16, 2024</p> <p>December 09 - 11, 2024, Tallinn</p>
Session 5. Management and leadership in the context of hybrid challenges	
<p>Independent learning: 99 hours</p> <ul style="list-style-type: none"> - Reading mandatory literature and studying e-learning materials - Taking a self-assessment test (a multiple-choice test) about modern theories and concepts of management and leadership. <p>Contact learning (online): 5 hours Lectures, seminars</p> <p>Contact learning (face-to-face): 6 hours Lectures, seminars</p>	<p>November 18 - December 06, 2024</p> <p>November 30, 2024</p> <p>December 09 - 11, 2024, Tallinn</p>
<p>Module Assessment (15 hours, face-to-face)</p> <ul style="list-style-type: none"> - Tabletop exercise - solving case studies related to hybrid threats 	<p>December 13, 2024, Tallinn</p>
<p>Reassessments</p>	<p>January 10, 2025 - deadline for liquidation of student debts</p>
<p>Graduation ceremony</p>	<p>December 13, 2024, Tallinn</p>

Contact person:

Inge Lindsaar

HYBRIDC@sisekaitse.onmicrosoft.com