JOINT MASTER'S PROGRAMME CURRICULUM IN COUNTERING HYBRID THREATS

METHODOLOGY FOR IMPLEMENTATION

Funded by the European Union

DECEMBER 4, 2023

Table of Contents

1. Introduction 4
   1.1 Background and Rationale 4
   1.2 Programme Descriptors 5
   1.3 Target Group and Entry Requirements 5
2. Course Learning Outcomes 6
3. Terms of Completion and Documents to be Issued upon Completion 6
4. Learner's Journey Briefly 6
5. Course Learning Strategy 8
6. Recommendations for Physical Activities During Online Studies 8
   6.1 Introduction 8
   6.2 Physical Activity Pauses During the Workday 10
   6.3 Physical Activity Bingo 12
   6.4 Healthy Campus Program Ideas 13
7. Course Assessment Strategy 15
8. Modules 16
   8.1 Module 1. Phenomena of Hybrid Threats 16
      8.1.1 Module Aim and Module Learning Outcomes 16
      8.1.2 Module Learning Strategy 17
      8.1.3 Module Assessment Strategy 18
      8.1.4 Module 1 Sessions 20
      8.1.5 Delivery Timetable for Module 1 41
   8.2 Module 2. Prevention and Cooperation in Countering Hybrid Threats 42
      8.2.1 Module Aim and Module Learning Outcomes 42
      8.2.2 Module Learning Strategy 42
      8.2.3 Module Assessment Strategy 43
      8.2.4 Module 2 Sessions 45
      8.2.5 Delivery Timetable for Module 2 65
   8.3 Module 3. Increasing resilience and bolstering societal and institutional capabilities to hybrid threats 66
      8.3.1 Module Aim and Module Learning Outcomes 66
      8.3.2 Module Learning Strategy 66
      8.3.3 Module assessment strategy 67

8.3.4 Module 3 Sessions 68
8.3.5 Delivery Timetable for Module 3 79
8.4 Module 4. Management and Leadership in the Context of Hybrid Threats and Hybrid Crises 80
8.4.1 Module Aim and Module Learning Outcomes 80
8.4.2 Module Learning Strategy 80
8.4.3 Module assessment strategy 81
8.4.4 Module 4 Sessions 84
8.4.5 Delivery Timetable for Module 4 95
8.5 Master's Exam. Theoretical-analytical Essay 97
8.5.1 Aim of the Master's exam and learning outcomes to be assessed 97
8.5.2 Assessment strategy 97
ANNEX 1 Assessments 99
Module 1 Assessments and assessment criteria 99
Module 2 Assessments and assessment criteria 110
Module 3 Assessments and assessment criteria 112
Module 4 Assessments and assessment criteria 114
Master's Exam. Assessment criteria 116
ANNEX 2 Mandatory reading 122
ANNEX 3 Recommended reading 143
ANNEX 4 Cross-reference Tables 171
Cross-reference Table of Course Learning Outcomes and Module Learning Outcomes 171
Cross-Reference Tables of Module Learning Outcomes and Sessions 177

1. Introduction

1.1 Background and Rationale

The Joint Master's Programme Curriculum 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 College of Republic of Croatia.

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 recent use of migrants as tools for hybrid attacks against European Union Member States, primarily against Lithuania, Latvia and Poland by Belarus, Russia's propaganda narratives and conspiracy theories to show Russia as a hero in COVID crises 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. Hybrid threat research, up-to-date training and public awareness are 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 specialties 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 national or regional level. There is a broad understanding in the European Union of the challenges we face in the form of hybrid threats. To this end the creation of a joint international master's program in internal security was important. Development of joint International Hybrid Master's Degree Curriculum jointly in different universities in European Union corresponds to the needs of 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.

1.2 Programme Descriptors

Title of the study programme	Countering Hybrid Threats
Study level	Master's studies
European Qualifications Framework Level	Level 7
ECTS Credits	60 ECTS
Nominal period of studies	1 academic year, full-time study
Language of instruction	English

1. Aim of the Curriculum

The curriculum aims to develop students' strategic thinking skills to comprehend and cope with challenges and controversies related to hybrid threats in the internal security area in the light of European Union policy and societal contexts.

The study programme provides a platform for exchanging experiences and enhancing competence by offering up-to-date knowledge, critical analytical and administrative capacity at the strategic level, which is essential for making complex management decisions in a changing society.

1.3 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 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, at a minimum:

- Bachelor's degree (BA) or Diploma of Professional Higher Education or a corresponding qualification;
- 2 years of professional work experience in internal security or a related field;
- English proficiency at B2 level;
- motivation and willingness to study in an international environment.

Selection procedure and the interview process:

The suitability and matriculation of the nominated candidates are decided by the Course Program Committee. Candidates are required to submit a motivation letter and participate in online interviews.

2. Course Learning Outcomes

Course learning outcomes describe the specific knowledge, skills, or expertise that the student will get from learning activities.

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;
- applies managerial and leadership theories and concepts for dealing with modern security challenges and threats;
- employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in the case of hybrid crises;
- creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security;
- demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and maintains a commitment to continuous learning and professional development.

3. Terms of Completion and Documents to be Issued upon Completion

The study ends with the master's exam. A prerequisite for admission to the master's exam is the completion of the curriculum until the master's exam. The curriculum is considered completed when all modules of the curriculum are completed.

The Master's Degree in Social Sciences (MA) is awarded to a student who has been officially registered on the Degree Programme and has fulfilled the assessment requirements of the Curriculum comprising 60 ECTS credits.

Master Award parchments are issued by implementing higher education institutions and signed by the heads of these institutions and are accompanied by a Diploma Supplement describing the nature, level, context, content, and grades obtained for the modules and the dissertation.

4. Learner's Journey Briefly

The course consists of 4 modules that are following each other. Each module contains a variable number of sessions. Each session consists of relevant topics relating to the module learning outcomes.

It is intended that the Consortium will share the programme delivery. A Consortium Partner will be nominated to coordinate the delivery of each module. Nevertheless, the responsibility for each module

will always rest with the Consortium, as it is the Consortium as whole that is responsible for this programme. To ensure quality, the delivery of the modules will not be shared. In principle, in every iteration of the programme, each Consortium Partner will be responsible for the delivery of at least one module. The decisions on the concrete allocation of the modules will be taken by the Governing Board of the Consortium, in advance of each iteration.

Delivering a module involves the institutional responsibility for the module organisation, delivery and quality assurance, the nomination of a local Module Coordinator/ Convenor, expert in module area, provision of teaching staff, as well as provision of facilities and logistical arrangements.

Modules and their allocation (tentative):

	Modules	**ECTS**	**Learning hours**				**Main Deliverer**
			Total	**Contact**	**Independent**	**Experiential**	
1	Phenomena of hybrid threats	14	364	36	328	0	Lithuania
2	Prevention and cooperation in countering hybrid threats	10	260	26	234	0	Croatia
3	Increasing resilience and bolstering societal and institutional capabilities to hybrid threats	8	208	21	84	103	Croatia
4	Management and leadership in the context of hybrid threats and hybrid crises	13	338	40	274	24	Estonia

The learning takes place in an academic formal environment or in an operational-organisational context, for the experiential learning phase. Usually, the contact week takes place on the premises of the Academic Partner or online. A centralised eLearning environment is available. The indicated readings and study materials are available in the libraries (including virtual libraries) of the partner institutions and/or made available for the students in an electronic format via the eLearning environment.

5. Course Learning Strategy

The Countering Hybrid Threats study programme respects and attends to the diversity of students and their needs, embraces flexible learning paths, recognises prior learning, and encourages a sense of autonomy in the student – while ensuring adequate guidance and support from the lecturers, facilitating the student´s progress in their studies in a supportive and effective learning environment.

The study methods are student-centred, encouraging active participation and reflecting the principles of adult learning. The learning methodology is based on different strategies that combine independent learning, experiential learning, seminars, workshops and lectures, ensuring the progression of the students' learning.

The programme comprises 4 thematic modules which are delivered across two semesters. The modules are planned one after the other: i.e., before the start of the next module, the student must complete the previous module. If students have not passed a module, they can conditionally progress until all reassessment options have been used. Module 1 is a prerequisite for all other modules: i.e., the student is not allowed to take any assessment of the following modules until Module 1 has been completed.

Each module is composed of an independent learning phase, face-to-face classroom and/or online activities (contact learning phase) and preparation of assessment assignments as an application of acquired knowledge and skills in solving complex real-life cases. Module 3 and Module 4 also contain a supervised application phase (experiential learning phase).

During the independent learning phase, students work through study materials, read sources from essential reading and complete independent work assignments. Tutoring is assured to keep participants active, motivate them and follow their progress, and provide feedback and support when needed.

The contact learning phase consists of specialized lectures, discussions, practical case studies, presentations, and seminars to research deeper into the module topics. Studies are combined with active feedback from participants and lecturers. The contact learning phase can take place in the form of classroom learning or online.

The experiential learning phase, in the form of practical assignments, is performed during the course to ensure constant involvement in the learning process and to foster the transfer of learning to a real-life environment, to build a link between gained academic knowledge and practical needs in the internal security area.

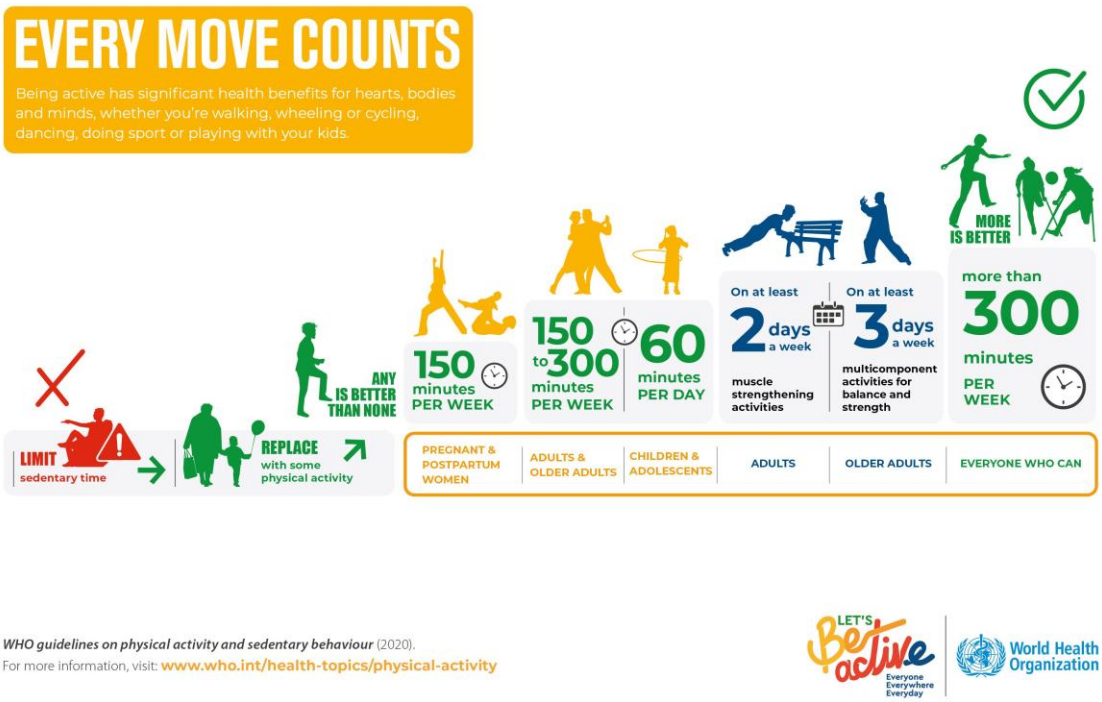
6. Recommendations for Physical Activities During Online Studies

6.1 Introduction

According to World Health Organization (WHO) suggestions for better health adults have to practice at least **150 to 300 minutes of moderate aerobic activity per week** (or the equivalent vigorous activity (75

to 150 min)). Adults should also do muscle strengthening activities at moderate or greater intensity that involve all **major muscle groups on 2 or more days a week**, as these provide additional health benefits[1].

In 2018 WHO added for the first-time to Global Recommendations on Physical Activity for Health, population-based guidelines on sedentary behaviour (Dempsey et.al, 2020)[2]. WHO Key messages consist of information, that too much **sedentary behaviour** can be unhealthy. It can increase the **risk of heart disease, cancer, and type-2 diabetes**. Limiting sedentary time and being physically active is good for health.



Graphics 1. WHO Guidelines on Physical Activity and Sedentary Behaviour [3]

[1] World Health Organization 2020, *WHO guidelines on physical activity and sedentary behaviour: at a glance*, Geneva: World Health Organization. Available from: https://iris.who.int/bitstream/handle/10665/337001/9789240014886-eng.pdf?sequence=1.

[2] Dempsey PC, Biddle SJH, Buman MP, et al. 2020, 'New global guidelines on sedentary behaviour and health for adults: broadening the behavioural targets', *International Journal of Behavioral Nutrition and Physical Activity*, no.17.

[3] World Health Organization 2021, *WHO Guidelines on Physical Activity and Sedentary Behaviour,* Available from: https://www.who.int/multi-media/details/who-guidelines-on-physical-activity-and-sedentary-behaviour.

Sitting almost all the time at work and not taking breaks is associated with an increased risk for self-reported poor general health and back/neck pain. People sitting almost all their time at work are recommended to take breaks from prolonged sitting, exercise regularly and decrease their leisure time sitting to reduce the risk for poor health.[4]

In September 2023 Song, Z et al. published article Daily stair climbing, disease susceptibility, and risk of atherosclerotic cardiovascular disease: A prospective cohort study. This study used data of 458,860 adult participants from the UK Biobank and during a median of 12.5 years of follow-up was shown that climbing stairs more than 5 times per day (50 steps) was associated with a lower risk of atherosclerotic cardiovascular disease (ASCVD).[5]

According to surveys walking and other physical activity (PA) is good for mental health. PA is connected to happiness and objective well-being (Castellanos-García, 2022) [6] , thus regular PA is necessary to support your studies.

Active microbreaks seems to lead to improvement in the physical, mental, and metabolic functions of the human body without posing detrimental effects to productivity. Different studies show, that active microbreaks may have the potential to decrease musculoskeletal discomfort, improve cardiometabolic markers, and help provide relief from fatigue and stress experienced throughout the workday (Radwan, et.al 2022).[7]

6.2 Physical Activity Pauses During the Workday

Learning means dedication. You can tie yourself strongly to the computer screen or books, devouring new knowledges. The pauses might seem unnecessary, because then you have to interrupt this important work, but they are meant to help your body to survive and serve you better during long life.

[4] Kallings, L V, Blom, V, Ekblom, B et al. 2021, Workplace sitting is associated with self-reported general health and back/neck pain: a cross-sectional analysis in 44,978 employees, BMC Public Health 21, 875. Available from: https://doi.org/10.1186/s12889-021-10893-8.

[5] Song, Z, Wan, L, Wang, W, Li, Y, Zhao, Y, Zhuang, Z, Dong, X, Xiao, W, Huang, N, Xu, M, Clarke, R, Qi, L & Huang, T 2023, Daily stair climbing, disease susceptibility, and risk of atherosclerotic cardiovascular disease: A prospective cohort study. Available from: https://doi.org/10.1016/j.atherosclerosis.2023.117300).

[6] Castellanos-García, P, Lera-López, F, Sánchez-Santosc, JM 2023, 'Light, moderate and vigorous physical activities: New insights into a virtuous circle with happiness'. *European Journal of Sport Science*, vol. 23, no. 7. Available from: https://www.tandfonline.com/doi/full/10.1080/17461391.2022.2089053.

[7] Radwan, A, Barnes, L, DeResh, R, Englund & R, Gribanoff, S 2022, Effects of active microbreaks on the physical and mental wellbeing of office workers: A systematic review, Cogent Engineering, 9:1.

If you have possibility to change position between sitting and standing, there are study results that show the less discomfort of those who **change position after every 30 minutes**[8]. If you don't have adjustable desk, minor movement are good – try to avoid prolonged postures. Physiotherapists recommend, that during sitting **the best posture is your next posture**.

Take one 1-2-minute break during every 30 minutes of sitting and at least 5-10 minutes break every second hour. Move and do exercises during the break.

- Stop and don't perform exercises or movements that cause severe discomfort or pain.
- Limit the movements if you are sick or injured, please consult with your health care provider before exercising.

Ideas for pauses/ examples of easy exercises (pick one of them or a few according to your preference):

- Walking, walking on the spot, stair climbing.
- Stepping forward, backward, sideways or doing half lunges.
- Shoulder circles and shrugs, arm circles, hip circles.
- Slow and controlled neck tilts and rotations on the wall.
- From the fist position separating and straighten fingers and stretch 5-10 sec.
- Arm straight, palm facing down, gently pushing on back of the hand. Fingers upward and pressing with another palm until stretching position, holding both stretches 3-5 sec. Or some other hands and wrists stretch.
- Arm swings, arms stretching horizontally to the sides (open your chest).
- Chair squats, half squats, squats.
- Incline push-ups, using wall, table, bench.

We might know, what to do for better health, but we will get the real benefits of following these knowledges. You can choose 1-3 exercises for active pause or practice more of them during workout.

For better posture practice these exercises:

- Chest stretches https://mindbodyspine.ca/chest-stretch/
- Hip flexors stretch https://backintelligence.com/hip-flexor-stretches/
- Plank https://www.shape.com/fitness/workouts/ab-workouts/30-day-plank-challenge
- Bridges https://greatist.com/health/bridge-exercise
- Bird Dog https://www.verywellfit.com/how-to-do-the-bird-dog-exercise-3498253

It is important also to rest your eyes during long computer work, some studies support 20-20-20 trick. After every work for 20 minutes, rest for 20 seconds by focusing vision to an object 20 feet (6 meters)[9].

[8] Roelofs, A & Straker, L 2002, 'The experience of musculoskeletal discomfort amongst bank tellers who just sit, just stand or sit and stand at work', *Ergonomics*. Vol.14.

[9] Anggrainy, P, Lubis, R R, & Ashar, T 2020, 'The effect of trick intervention 20-20-20 on computer vision syndrome incidence in computer workers', *Oftalmologicheskiĭ Zhurnal*, 84, pp.22-27.

Widely is suggested to practice eye-yoga exercises (e.g palming, blinking, sideways viewing, front and sideways viewing, diagonal viewing, rotational viewing, preliminary nose tip gazing, near and distant viewing).

6.3 Physical Activity Bingo

If you don't have a regular training program and/or you want to increase your physical activity, we encourage you to play bingo. Mark the performed activities during one month according to the example or make your own bingo grid. Choose the activities according to your fitness level and try to cover all activities in one row within one week.

Choose moderate-intensity aerobic exercises (you can talk during it, but not sing), walk faster short periods during regular walk etc.

Beginners BINGO

Stretches	Aerobic training at least 10 min	Strength exercises	Active rest (cycling/walk/ dancing)	Mindfulness (yoga, breathing, shinrin-yoku)	Eye exercises
Mindfulness (yoga, breathing, shinrin-yoku)	Stretches	Aerobic training at least 15 min	Eye exercises	Strength exercises	Active rest (cycling/walk/ dancing)
Strength exercises	Eye exercises	Active rest (cycling/walk/ dancing)	Mindfulness (yoga, breathing, shinrin-yoku)	Stretches	Aerobic training at least 20 min
Active rest (cycling/walk/ dancing)	Mindfulness (yoga, breathing, shinrin-yoku)	Stretches	Aerobic training at least 20 min	Eye exercises	Strength exercises

Advanced BINGO

Balance and stretches	Aerobic training at least 30 min	Strength exercises	Aerobic training at least 40 min	Eye exercises, mindfulness	Strength exercises
Mindfulness	Balance and stretches	Aerobic training at least 30 min	Eye exercises, mindfulness	Strength exercises	Active rest 1-2 hr (walk, cycling, dancing)

Strength exercises	Eye exercises, mindfulness	Aerobic training at least 40 min	Balance and stretches	Strength exercises and stretches	Aerobic training at least 45 min
Aerobic training at least 30 min	Strength exercises and stretches	Eye exercises, mindfulness	Aerobic training at least 30 min	Strength exercises and stretches	Active rest 1-2 hr (hiking, cycling, dancing)

6.4 Healthy Campus Program Ideas

As meaning the concept of health extends beyond mere connections with physical activity, here are examples of advice from the Healthy Campus program calendar provided by the Estonian Academy of Security Sciences. The feedback on these suggestions has been positive. While not everyone, including cadets and staff members, followed all of them, many admitted that they gained ideas to try something new and enhance their days.

1st Day	Accumulate climbing minutes by using stairs or tackling a hill. Aim for a total of about 3-5 minutes throughout the day, which can be completed in several sections. Choose a pace that suits your ability.
2nd Day	Pause gymnastics (low impact exercises).
3rd Day	Aerobic exercise (walking, running, skating, skiing or dancing) 15-30 minutes. Keep the intensity at a level where you can easily talk with your partner.
4rt Day	Bending and stretching exercises for 10-15 minutes. Find a comfortable place to do the exercises. Some of them can be done while sitting on a mat or carpet. Do not hold your breath while stretching. Try to relax the body area to be stretched beforehand and increase the stretch during a calm exhalation. You may feel a slight tingling sensation in your muscles. Avoid sudden jerks and crossing the pain threshold.
5th Day	Walk from one point to another during the day, incorporating necessary movements or additional exercise (with a colleague, family member or friend) 2-3 km. A brisk walk can be a form of exercise. By combining regular walks with special exercises, you can manage your calorie consumption and maintain or develop your physical abilities.
6th Day	Do name letter training. During the remote work period, institutions distributed several training options, enabling you to choose exercises based on the letters in your name. Discover what challenges your name offers! If a specific exercise is too much for you at first, replace it with an easier one.
7th Day	Since the Healthy Campus program also includes the prevention of risky behaviour, we share some basic information. According to the WHO, there is no safe level of drinking, and not drinking alcohol is the only way to avoid its damaging effects. If you or one of your friends consumes alcoholic beverages, find for yourself another activity for the day and at least a couple of days in the next weeks. Share the ideas or advices with your friend and practise these activities without drinking alcohol. You can

	make a donation to charity with the expense of the alcoholic drink that was left unpurchased. Stretch, try balance exercises or yoga. The simplest balance exercise is standing on one leg.
8th Day	Perform a cardio workout containing boxing movements for 10-30 minutes.
9th Day	Walk to the farthest corner of the house or around the house a couple of times. Of course, it's beneficial if you find a reason to go a greater distance – whether to take the waste to the appropriate collection box, to chat with a family member or friend, etc.
10th Day	Find an opportunity to do 20-30 minutes of physical work during the day. If that's not possible, follow a training video. If you are already active during the day with housework, exerting yourself to the point of slight panting and sweating, you need not worry about additional training, unless you have a specific competitive goal.
11th Day	Go for a hike, whether in nature or in the city. Choose a hike length that suits you and your companions. Discover something new about the journey, your surroundings or yourself during the hike.
12th Day	Perform push-ups against a table, wall or in a prone position. Pay extra attention to the push-up technique. You can start with lighter versions, resting your hands on the wall or the edge of the table. Do three sets of push-ups with rest breaks, adjust the number of repetitions to reach fatigue by the end of each set. Cadets across various disciplines perform this exercise in classes or tests. Those seeking variation can vary the pace, do push-ups in a narrow stance (emphasizing triceps) or by shift more load to the shoulders by pushing the hips up.
13th Day	Focus on leg exercises. Massage the foot on a tennis ball or roll a bottle under the sole (with the cap screwed on). Raise the arch of the foot while sitting straight in a chair. You can also develop dexterity by trying to pick up a pencil or other object from the floor with your toes.
14th Day	Increase the amount of vegetables in your daily food intake, especially if you don't already consume enough , or try a new recipe for healthy food.
15th Day	Do 2-10 squats at each activity break or incorporate squat exercises into your gym training.
16th Day	Run, walk, skate, ski or dance for 20-45 minutes. If some recommendations have been repeated, it's because of development tactics - activities must be repeated regularly and systematically, the load must be gradually added, and the techniques and tactics must be improved. Recovery weeks in training micro cycles help prevent overload. Supporting all aspects of health is important for getting in good shape.
17th Day	Do office-gymnastics. Find new places to do exercises, such as your study room, the bus stop, the canteen or a corridor or any other waiting room (e.g., rolling your legs from heels to toes, alternately tensing and relaxing the body muscles).
18th Day	Cook, tidy, decorate, take a walk, breathe deeply, relax your body, meditate. Plan a screen-free day or decrease usage of screens.
19th Day	Participate in moving activities or hike in nature. When you come back to your room, strengthen your back with plank exercises.
20th Day	Move in parallel with other activities. Walk indoors or outdoors and make a poem. Call a friend or family member and walk during the phone call (not in traffic!). Encourage your companions to get up from their chairs and stretch from time to time.

21st Day	Perform your preferable exercises or 5-10 therapeutic gymnastics exercises, which may be necessary to recover from an injury or to prevent injuries. You can choose exercises here: CSP Rehabilitation Exercises.If you wish, download the ROK application "Get Set - Train Smarter" to your smartphone and choose exercises that support the training program for your sport.
22nd Day	Healthy Campus advice: if you or one of your friends is a nicotine user, join or suggest joining a campaign to quit nicotine in the next month. Nicotine is one of the most addictive substances found in all tobacco products, including regular cigarettes, heated tobacco products, snuff, e-cigarettes and nicotine patches. Take care of your loved ones and recommend that they join the campaign as support to get rid of this negative habit!
23rd Day	Move with medium intensity for 30-60 minutes. In normal weather, it would be recommended to park your car further from your destination or get off one stop earlier when traveling by public transport. In slippery conditions, you can only do this if you wear safe shoes. In addition to exercise, pay attention to a healthy diet and choose foods in a way that incorporates several colours to keep your diet more versatile! If you need help gaining, maintaining or losing weight, write down the calories you consume using nutrition diaries, such as the MyFitnessPal phone application.
24th Day	Go to the gym or do strength training at home using backpack and water bottles as weights.
25th Day	Do endurance-oriented training for 20-45 minutes. You can also split the longer training in half later in the day, but don't skip it. Light movement will support recovery in case of muscle pain from the previous day's exercises.
26th Day	Clean the table and drawers or get rid of digital garbage. In the meantime, do strength, balance and coordination exercises.
27th Day	Practice eye yoga.
28th Day	A movement recommendation for sedentary people is to check their posture from time to time. The shoulders will automatically take the correct position if you move the pelvis forward while sitting, raise the chest and let the arms hang loosely. Go outside for a walk.
29th Day	Try juggling.
30th Day	If you don't have heart or lung problems, take a cold shower.

7. Course Assessment Strategy

The overall course assessment strategy has been designed to support and drive students' learning towards acquiring the course learning outcomes. A variety of assessment methods are used not only to ensure that students achieve the specified learning outcomes but also to enhance the student learning experience and develop students' critical thinking to apply the acquired knowledge and skills to tackle hybrid threats.

The assessment strategy for this program envisages assessment tasks as learning activities, where the learning will be achieved through performance, engagement, discussion, peer review and feedback. The

assessment methods and the assessment criteria can be found in the description of each module. Assessment methods are derived from the learning outcomes, i.e., assessment methods have been chosen that allow assessing the achievement of the module learning outcomes in the best way. At the end of the course, students will write a scientific essay (final exam) under supervision of academic staff members. A more detailed description of the assessment is provided in each module assessment strategy.

For successful completion of each taught module, a grade "E" or "Pass" is required. Attending the modules and fulfilling all requirements is compulsory. If students do not achieve all the requirements to proceed regularly to the following module, having been absent from assessment or having failed in the assessment, they can progress conditionally and be (re)assessed in a predefined period. Students who fail during the assessment are eligible for two re-assessment possibilities.

Students are entitled to receive feedback on their assessment after the announcement of the results so that they could know the strengths and weaknesses of their work before the re-assessment (if needed) takes place.

8. Modules

8.1 Module 1. Phenomena of Hybrid Threats

Pre-requisite Modules:	**No**		**ECTS Credits 14**
Contact learning hours	**Independent learning hours**	**Experiential learning**	**Total**
84	280	0	364

8.1.1 Module Aim and Module Learning Outcomes

Module aim: the student develops a critical understanding of how hybrid threats can affect global and European security, and skills to design solutions to respond to hybrid threats.

Upon completion of this module, the student will be able to:

- critically analyse hybrid threats in the context of global, European and national security;
- evaluate the security strategies aiming to ensure sustainable security concepts in the contemporary hybrid threats environment;
- discuss international and European Union policies and legal framework responding to hybrid threats, considering provisions of fundamental rights;
- critically analyse tendencies of contemporary warfare regarding hybrid threats;
- critically analyse cases of information warfare and their impact on fundamental rights;
- independently and creatively identify problems related to hybrid threats and develop and design solutions to respond to hybrid threats using different research strategies and methods in social science research.

8.1.2 Module Learning Strategy

This module serves as a foundation for subsequent modules of the programme. It is designed to maximize student interaction and co-operation so that social bonds between students from different countries of the European Union are formed early in the study programme. The module seeks to create an understanding of the phenomena of hybrid threats but also to begin building the skills of using various strategic analysis, research strategies and methods.

The learning process of the module is divided into 2 phases:

- **Independent learning phase**. The independent learning phase before the contact learning phase lasts for 3 weeks (120 hours). During this time, the student should lay the groundwork for contact learning for the module by getting acquainted with relevant literature, going through eLearning tools and completing self-assessment tasks. The self-assessment tasks will serve as a prerequisite for participating in the contact week. Also, it is expected that in completing the assessment assignments (written analysis, case studies and scientific essay) students will discuss and apply theories and methods covered in the learning materials; therefore, a demonstration of good content knowledge is critical. The eLearning platform will be open during the study period. Students will be able to contact the lecturers using the Moodle course and discuss any issues related to the contents in the forums.

  During the independent learning phase, the student will compile two files:
  - a draft outline of the written analysis, that includes the security strategy and hybrid threats to analyse and a preliminary list of references reviewed;
  - a draft outline of the essay, that includes the chosen problem related to hybrid threats and a preliminary list of references reviewed;

  At the end of the independent learning phase, the student will also perform the online test about international and European Union policies and the legal framework responding to hybrid threats.

- **Contact learning phase**. The contact learning phase lasts for 1 week (36 hours). During this week, students participate in lectures, which will cover key theoretical and methodological aspects of the module, and seminars applying and reflecting on the topics of the module.

  During the contact week, students will prepare two case studies and deliver the presentations.

Sessions of the Module 1:

- Session 1. Hybrid threats: concept, definitions and wider interpretations
- Session 2. Hybrid threats and security strategies
- Session 3. Policy and regulation
- Session 4. Warfare in the context of hybrid threats
- Session 5. Information warfare
- Session 6. A common response to hybrid threats and strategies for tackling them

- Session 7. Research strategies and methods

8.1.3 Module Assessment Strategy

There are five assessment assignments for the module:

- written analysis of security strategies aiming to ensure sustainable security concepts in the contemporary hybrid threats environment;
- online test with open-ended questions;
- case study of tendencies of contemporary warfare regarding hybrid threats;
- case study of information warfare and its impact on fundamental rights;
- drafting a scientific essay identifying problems related to hybrid threats and developing and designing solutions to respond to hybrid threats.

The written analysis of security strategies**.** The student will select the security strategy to analyse from the learning materials or from recently published EU policy documents. The topic will be previously agreed upon with the lecturer. The writing process will be guided by a supervisor. The analysis is assessed non-distinctively, and to pass, the student must meet all the assessment criteria. The lecturer gives feedback about meeting assessment criteria in written or/and oral form. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the analysis. The student has approximately two weeks for eliminating the deficiencies.

Online test with open-ended questions. The student must answer the questions within the allotted time. Students are allowed to use all study materials and necessary sources while answering. The test is assessed non-distinctively, and to pass, the student must answer each question correctly. In case of failing, the student will have the opportunity for reassessment, under the same conditions as the assessment in terms of the testing environment and allotted time. The student has approximately two weeks for reassessment.

Case study on tendencies of contemporary warfare regarding hybrid threats. Scenarios on contemporary warfare will be presented to students, and they will choose one case to analyse. The case study is performed as a group work. The group size is up to 5 students. It is allowed to work individually if the student has expressed their will to do so. The case study is assessed non-distinctively, and to pass, the student must meet all the assessment criteria. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the case study and/or the presentation. The lecturer gives feedback about meeting assessment criteria in oral form after the presentation.

If, based on the group members' evaluation, some of the group members did not contribute to the assignment, then the student should perform a new case study independently.

Case study of information warfare and its impact on fundamental rights. Scenarios on information warfare will be presented to students, and they will choose one case to analyse. The case study is performed as a

group work. The group size is up to 5 students. It is allowed to work individually if the student has expressed their will to do so. The case study is assessed non-distinctively, and to pass, the student must meet all the assessment criteria. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the case study and/or the presentation. The lecturer gives feedback about meeting assessment criteria in oral form after the presentation.

If, based on the group members' evaluation, some of the group members did not contribute to the assignment, then the student should perform a new case study independently.

Drafting a scientific essay. Students can choose the topics for the essay from a list provided by the lecturer/professor or provide their own topics. If the student chooses a topic not from the list, they must coordinate it with the lecturer/professor. The writing process will be guided by a supervisor.

The essay is assessed distinctively. The essay will be assessed by the opponent. A positive grade is achieved if each subsection of the essay is graded at least with the grade "E". The final grade is the average of grades of the subsections. The opponent gives feedback about meeting assessment criteria in written or/and oral form. In case a student will get the grade "F" at least in one subsection, the final grade will be "F" (fail). In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the essay. The student has approximately two weeks for eliminating the deficiencies.

The module is positively passed if each learning outcome is graded at least with the grade "E" or "Pass". The final grade of the module is the grade of the scientific essay.

For information on the assessment criteria see in the **ANNEX 1 Assessments**.

8.1.4 Module 1 Sessions

Session 1. Hybrid threats: concept, definitions and wider interpretations
Session aim: The session aims to create opportunities for students to develop skills to analyse hybrid threats in the context of global, European and national security
Session duration: 56 hours: 43 independent learning hours (13 hours before the contact week and 30 hours after the contact week) and 13 contact learning hours (6 hours online, 4 hours face to face, 3 hours for online consultation related to written analysis)
Learning environment(s) and requirements eLearning environment and classrooms for contact learning
Learner resources PCs and/or mobile devices with the latest versions of browsers
Session topics 1. Global and European Union definitions of hybrid threats 2. Hybrid threats and models of their appearance 3. Conspiracy theories 4. Influence of hybrid threats to internal security, economy, and international relations
Learning activities During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course and discuss any issues related to the contents in the forums. Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks. During the independent learning phase, the student will compile the draft outline of the written analysis, that includes the security strategy and hybrid threats to analyse, and a preliminary list of references reviewed. In the analysis, the student will demonstrate content knowledge of Sessions 1 and 2. The writing process will be guided by a supervisor. The written analysis will be completed after the contact week. In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.
Essential reading Bargués, P., Bourekba M., Colomina, C.(eds.) 2022, *Hybrid threats, vulnerable order* CIDOB *report # 08* CIDOB. Available from: https://www.cidob.org/en/publications/publication_series/cidob_report/cidob_report/hybrid_threats_vulnerable_order. [30 August 2023]. Cassam, Q., 2023, *Conspiracy Theories.* Soc 60, 190–199, 2023, Available from: https://link.springer.com/article/10.1007/s12115-023-00816-1. [3 January 2024]. Council of Europe (2016), *Legal challenges related to hybrid war and human rights obligations,* Committee on Legal Affairs and Human Rights, Rapporteur: Mr Boriss Cilevičs. Available from:

https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en [20 February 2024].

Countering Hybrid Threats 2022, Available from: https://defence-industry-space.ec.europa.eu/system/files/2022-03/Factsheet%20-%20Countering%20Hybrid%20Threats.pdf [21 February 2024].

Douglas, K. M., Sutton, R. M., 2023, *What are conspiracy theories? A definitional approach to their correlates, consequences, and communication*. Annual review of psychology, 74, 271-298, Available from: https://www.annualreviews.org/doi/abs/10.1146/annurev-psych-032420-031329. [24 January 2024].

European Commission 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats,* JOIN(2016) 18 final, 6 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 [20 February 2024].

European Commission 2020*, Identifying Conspiracy Theories.* Available from: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en. [12 January 2024].

Giannopoulos, G., Smith, H., Theocharidou, M. 2020, *The Landscape of Hybrid Threats: A Conceptual Model – Public Version*, (The European Commission and the European Centre of Excellence for Countering Hybrid Threats, 26 November 2020), Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305. [1 August 2023].

Heap, B. (ed.) 2019 Strategic Communications Hybrid Threats Toolkit. Applying the principles of NATO Strategic Communications to understand and counter grey zone threats. Nato Strategic Communications Centre of Excellence, p. 10. Available from: https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf [24 June 2024].

Hybrid CoE (2024), *Hybrid threats as a concept.* Available from: https://hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [20 February 2024].

Giannopoulos, G., Smith, H., Theocharidou, M. 2021, The Landscape of Hybrid Threats: A conceptual model, Publications Office of the European Union, Luxembourg. Available from: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [24 June 2024].

Sunstein, C. R., Vermeule, A., 2009, *Conspiracy theories: Causes and cures.* Journal of political philosophy, 17(2), 202-227 [online]. Available from: http://www.ask-force.org/web/Discourse/Sunstein-Conspiracy-Theories-2009.pdf [19 June 2023].

Uziębło, J. J. 2017, *United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats,* EU Diplomacy Papers 5/2017, College of Europe. Available from: https://www.coleurope.eu/sites/default/files/research-paper/edp-5-2017_uzieblo.pdf?download=1 [23 February 2024].

Recommended readings

Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. 2019, *Hybrid Threats. A Strategic Communications Perspective*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/pdfjs/?file=/publications/download/2nd_book_short_digi_pdf.pdf?zoom=page-fit [24 June 2024].

Bajarūnas, E., Keršanskas, B. 2018, *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome.* Lithuanian Annual Strategic Review, Volume 16, Issue 1 (pp. 123–170). https://doi.org/10.2478/lasr-2018-0006 Available from: https://journals.lka.lt/journal/lasr/article/152/info. [1 August 2023].

Bekkers, F., Meessen, R., Lassche, D. 2019, *Hybrid Conflicts: the New Normal?* TNO: Innovation for Life. Available from: https://www.tno.nl/publish/pages/7427/tno-2019-hybride.pdf [20 February 2024].

Berdal, M. 2011, The "New Wars'" Thesis Revisited. *The Changing Character of War*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:osobl/97801 99596737.003.0007. [24 June 2024].

Butter, M., 2020, *„Conspiracy theories in films and televisions shows",* Available from: https://tobias-lib.ub.uni-tuebingen.de/xmlui/bitstream/handle/10900/121641/Butter.%20Conspiracy%20Theories%20in%20Films%20and%20Television%20Shows.pdf?sequence=1&isAllowed=y. [22 November 2023].

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., Deravi, F., 2019, *Understanding conspiracy theories.* Political psychology, 40, 3-35 [online]. Available from: https://onlinelibrary.wiley.com/doi/full/10.1111/pops.12568. [12 July 2023].

Hanssen, M. (2018). Russian Hybrid Warfare: A Study of Disinformation. *Journal of Strategic Studies*. Available from: https://css.ethz.ch/en/services/digital-library/articles/article.html/1c93c122-e11f-45d4-afde-c5e17a3185fb. [24 June 2024].

Räikkä, J., 2018, *Conspiracies and conspiracy theories: An introduction*. Argumenta, 6, 1-12 [online]. Available from: https://www.argumenta.org/wp-content/uploads/2018/05/1-Argumenta-Juha-Ra%CC%88ikka%CC%88-Conspiracies-and-Conspiracy-Theories.pdf. [10 July 2023].

Sanz-Caballero, S. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, vol. 10, 360. Available from: https://www.nature.com/articles/s41599-023-01864-y. [1 February 2024].

United Nations Secretary-General 2019, *Developments in the field of information and telecommunications in the context of international security*. Report No. A/74/120, 24 June 2019. Available from: https://digitallibrary.un.org/record/3814154?ln=en [20 February 2024].

NATO 2016, *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.* Available from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [22 February 2024].

NATO 2018, *Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018*. Available from: https://www.nato.int/cps/en/natohq/official_texts_156624.htm [22 February 2024].

Session 2. Hybrid threats and security strategies

Session aim: The session aims to create opportunities for students to develop competencies to evaluate the security strategies in the contemporary hybrid threats environment

Session duration: 42 hours: 32 independent learning hours (9 hours before the contact week and 23 hours after the contact week) and 10 contact learning hours (4 hours online, 4 hours face to face, 2 hours for online consultation related to written analysis)

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Direct and indirect threats to the security environment
2. European Union strategies about internal security
3. Socio-cultural approach to security

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course and discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, the student will compile the draft outline of the written analysis, that includes the security strategy and hybrid threats to analyse, and a preliminary list of references reviewed. In the analysis, the student will demonstrate content knowledge of Sessions 1 and 2. The writing process will be guided by a supervisor. The written analysis will be completed after the contact week and should be submitted 10 days before the end of Module 1.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

Bardhan, P., 2022. A World of Insecurity: Democratic Disenchantment in Rich and Poor Countries. Harvard University Press.

European Commission 2015, *The European Agenda on Security*, Communication No. COM(2015) 185 final, 28 April 2015. Available from: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52015DC0185 [24 February 2024].

European Commission 2020, *EU Security Union Strategy*, Communication No. 2020 COM(2020) 605 final, 24 July 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605 [24 February 2024].

European Council 2003, „A Secure Europe in a Better World" European Security Strategy, 12 December 2003. Available from: https://op.europa.eu/en/publication-detail/-/publication/d0928657-af99-4552-ae84-1cbaaa864f96/ [24 February 2024].

European Council 2010, *Internal security strategy for the European Union: Towards a European security model*, 25-26 March 2010, Available from: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf [24 February 2024].

Fukuyama, F., 2022. Liberalism and Its Discontents. Farrar, Straus and Giroux.

Šlapkauskas, V., 2022. Theoretical and Methodological Aspects of the Definition of, and Research into, Security of a Small State // Europe Alone: Small State Security without the United States / edited by Schultz D, Pūraitė A, Giedraitytė V. Lanham: Rowman & Littlefield International.

Recommended readings

Bauman, Z., 2017. A Chronicle of Crisis: 2011–2016. Social Europe Editions.

Bauman, Z., 2001. Community. Seeking Safety in an Insecure World. Cambridge: Polity.

Berger, P. L., Luckmann, Th., 2011. The Social Construction of Reality. A Treatise in the Sociology of Knowledge. Open Road Media.

Buzan, B., 2008. People, States and Fear: An Agenda for International Security studies in the Post-Cold War Era. ECPR Press.

Bauman, Z., Donskis, L., 2013. The Loss of Sensitivity in Liquid Modernity. Cambridge: Polity.

Bergson, H., 2006. The Two Sources of Morality and Religion. Macmillan and Company Limited.

Countering Hybrid Threats (2022), Available from: https://defence-industry-space.ec.europa.eu/system/files/2022-03/Factsheet%20-%20Countering%20Hybrid%20Threats.pdf [21 February 2024].

Durkheim, E., 2011 [1925], Moral Education. Translated by E. K. Wilson and H. Schnurer. Mineola, New York: Dover Publications.

Durkheim, E., 1993 [1893], The Division of Labour in Society. Translated by G. Simpson. New York: The Free Press.

European Commission 2016, Joint Framework on countering hybrid threats. A European Union response, Communication No. JOIN(2016) 18 final, 6 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [24 February 2024].

European Commission 2017, Action Plan to support the protection of public spaces, Communication No. COM(2017) 612 final, 18 October 2017. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0612. [24 February 2024].

European Commission 2018, Increasing resilience and bolstering capabilities to address hybrid threats, Communication No. JOIN(2018) 16 final, 13 June 2018. Available from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016. [24 February 2024].

European Commission 2020b, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, Communication No. COM/2020/795 final, 9 December 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1631885972581&uri=CELEX%3A52020DC0795. [24 February 2024].

European Commission 2021, The EU Strategy to tackle Organised Crime 2021-2025, Communication No. COM(2021) 170 final, 14 April 2021. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1670427706474 [24 February 2024].

European Commission, High Representative of the Union for Foreign Affairs and Security Policy 2020) The EU's Cybersecurity Strategy for the Digital Decade. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [24 February 2024].

Etzioni. A. 2004, From Empire to Community: A New Approach to International Relations. New York: Palgrave Macmillan.

Gauvain, M., 2013, Sociocultural Contexts of Development. In Philip David Zelazo (Ed.). The Oxford Handbook of Developmental Psychology, Vol. 2: Self and Other (p.p. 425-444). New York: Oxford University Press.

Hayek, F. A., 1973, Law, Legislation and Liberty, Volume I: Rules and Order. London: Routledge and Kegan Paul [Don Mills: General Publishing].

Maslow, A. H., 1993 [1971]. "Theory Z". The farther reaches of human nature. New York: Arkana.

Rak J. & Bäcker R. (ed), 2022, Neo-militant Democracies in Post-communist Member States of the European Union /. London and New York, Routledge Taylor & Francis Group.

Šlapkauskas, V. 2023. Challenges of Predicting Social Conflicts in the Context of Crises and Hybrid Threats // Research Journal PUBLIC SECURITY AND PUBLIC ORDER, 2023 (33), p. 130-141.

Šlapkauskas V. 2021, The Role of Public Opinions on Society Security: A Socio-Cultural Approach // Research Journal PUBLIC SECURITY AND PUBLIC ORDER, No. 28, pp. 156-165.

Taylor, Ch., 1992. The Ethics of Authenticity. Harvard University Press.

Wolf M. 2023, The Crisis of Democratic Capitalism. By, Penguin Press.

Session 3. Policy and regulation

Session aim: The session aims to create opportunities for students to develop knowledge in strategical approach to hybrid threats and provisions of fundamental rights

Session duration: 42 hours: 32 independent learning hours before the contact week and 10 contact learning hours (4 hours online, 4 hours face to face, 2 hours assessment)

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. International legal framework and legal responses to hybrid threats
2. European Union policies and concepts addressing hybrid threats
3. Fundamental rights in the context of hybrid threats

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools.

During the independent learning phase, students will prepare for an online test with open-ended questions. One week before the contact learning phase, the students will take the test. The feedback about the test will be provided in Moodle.

In the contact week, the issues related to the online test will be discussed in depth in seminars.

Essential reading

Deppe, C. 2023, Disinformation in Cognitive Warfare, Fimi, Hybrid Threats. The Defence Horizon Journal. October 16, 2023. Available from: https://tdhj.org/blog/post/disinformation-cognitive-warfare-hybrid/ [30 June 2024].

European Commission 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM (2020) 605 final, pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [31 August 2023].

European Commission 2018, *Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats.* JOIN/2018/016 final. Document 52018JC0016, Available from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016 . [31 August 2023].

FAQ: Joint Framework on countering hybrid threats, 2016. Available from: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 [31 August 2023].

Fogt, M. 2021, 'Legal Challenges or "Gaps" by countering hybrid warfare – building resilience in jus ante bellum', *Southwestern Journal of International Law,* Vol. XXVII:1, Available from: https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf [25 February 2024].

Office of the United Nations High Commissioner for Human Rights 2008, Human Rights, Terrorism and Counter-terrorism. United Nations, Geneva. Available from: https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet32EN.pdf [30 June 2024].

Sari, A. 2020, Hybrid threats and the law: Concepts, trends and implications. Hybrid CoE Trend Report 3. April 2020. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Hybrid-CoE-Trend-Report-3.pdf [30 June 2024].

Recommended readings

Bay, S. 2024, *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks*. Hybrid CoE Research Report 12. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-content/uploads/2024/03/20240319-Hybrid-CoE-Research-Report-12-Countering-hybrid-threats-to-elections-WEB.pdf [30 June 2024].

Cantwell D. 2017, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone', *ASIL Insights* Issue: 14 Volume: 21, Available from: https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone [25 February 2024].

European Centre of Excellence for Countering Hybrid Threats, 2023. Hybrid threats as a Concept. Available from: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [4 September 2023].

European Council, 2023. EU's Strategic Compass for Security and Defence: Articles and reports. Available from: https://consilium-europa.libguides.com/strategic-compass/articles [4 September 2023].

Ferm, T. 2017, *Laws in the era of hybrid threats*. Hybrid CoE Strategic Analysis 3. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE-SA-3-Ferm.pdf[30 June 2024].

Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue *Addressing Hybrid Threats*, 2018. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf [4 September 2023].

Haataja, S. (2023) Cyber operations against critical infrastructure under norms of responsible state behaviour and international law, *International Journal of Law and Information Technology*, Volume 30, Issue 4, Winter 2022, Ppp. 423–443, https://doi.org/10.1093/ijlit/eaad006

Joint Staff Working Document, *Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats 16.9.2022 SWD(2022) 308 final.* Available from: https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD_2022_308_6_EN_document_travail_service_conjoint_part1_v5.pdf *[4 September 2023].*

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. 2023, Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, doi:10.2760/37899, JRC129019. Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. [4 September 2023].

Lonardo L. 2021, *EU Law Against Hybrid Threats: A First Assessment.* Available from: *https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2021_2_19_Articles_SS2_6_Luigi_Lonardo_00514.pdf* [4 September 2023].

McLaughlin, M. 2023, 'Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace', *Opiniojuris.,* Available from: http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/ [25 February 2024].

NATO 2023, *Collective defence and Article 5,* Available from: https://www.nato.int/cps/en/natohq/topics_110496.htm [25 February 2024].

Sanz-Caballero, S. 2023, 'The concepts and laws applicable to hybrid threats, with a special focus on Europe', *Humanities and Social Sciences Communications,* 10:360, https://doi.org/10.1057/s41599-023-01864-y.

Session 4. Warfare in the context of hybrid threats
Session aim: The session aims to create opportunities for students to develop skills to analyse tendencies of contemporary warfare regarding hybrid threats
Session duration: 70 hours: 54 independent learning hours and 16 contact learning hours (6 hours online, 10 hours face to face, of which 3 hours for case study)
Learning environment(s) and requirements eLearning environment and classrooms for contact learning
Learner resources PCs and/or mobile devices with the latest versions of browsers
Session topics 1. Hybrid warfare 2. Russian warfare as a new type of hybrid threat 3. Russian lawfare and ignorance of fundamental rights 4. Grey-zone conflicts, asymmetric warfare, terrorism as a hybrid threat 5. Countering hybrid warfare
Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, students will prepare for the case study about tendencies of contemporary warfare regarding hybrid threats.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars, students will solve the case study and make the presentations.

Essential reading

Adamsky, D. 2018, *From Moscow with coercion: Russian deterrence theory and strategic culture. The Journal of Strategic Studies*, Vol. 41, No. 1–2, pp. 33–60. Available from: https://doi.org/10.1080/01402390.2017.1347872 https://ir101.co.uk/wp-content/uploads/2018/10/adamsky-2018-from-moscow-with-coercion-russian-deterrence-theory-and-strategic-culture.pdf [30 June 2024].

Apetroe, A.C. 2016, Hybrid warfare: from "war during peace" to "neo-imperialist ambitions". The case of Russia. *Modelling the New Europe*. Issue No. 21, pp. 97-101. Available from: https://www.academia.edu/39885308/Online_journal_No_21_December [30 June 2024].

Clark, M. 2021, *The Russian military's lessons learned in Syria. Military learning and the future of war series.* Institute for the Study of War. January pp. 1-52. Available from: https://www.understandingwar.org/sites/default/files/The%20Russian%20Military's%20Lessons%20Learned%20in%20Syria_0.pdf [30 June 2024].

Coffey, L. 2019, How to Defeat Hybrid Warfare Before It Starts. *Defense One*, January 21, 2019. Available from: https://www.defenseone.com/ideas/2019/01/howdefeat-hybrid-warfare-it-starts/154296/. [30 June 2024].

Cordesman, A. H. 2020, Chronology of Possible Russian Gray Area and Hybrid Warfare Operations, *Center for Strategic and International Studies*, December 8, 2020, p. 15, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf. [30 June 2024].

Darczewska, J. 2014, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* May 2014. Centre for Eastern Studies Warsaw (OSW). Point of View, No 42, pp.1-26. Available from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf [30 June 2024].

Dobbs et al. 2020, *Grey-zone activities and the ADF*. A Perry Group Report. pp. 3-4. Available from: https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf). [30 June 2024].

Herta, L., M. 2016, Russia's hybrid warfare – why narratives and ideational factors play a role in international politics. *Modelling the New Europe*. 2016, Issue No. 21, pp.53-54. Available from: https://www.academia.edu/39885308/Online_journal_No_21_December . [30 June 2024].

Kravchenko, M. 2018, *Inventing Extremists. The Impact of Russian Anti-Extremism Policies on Freedom of Religion or Belief*. United States Commission on International Religious Freedom. Available from: https://www.uscirf.gov/sites/default/files/Inventing%20Extremists.pdf [30 June 2024].

Lele, A. 2014, Asymmetric Warfare: A state vs non-state conflict, *Oasis*, No 20, pp.97-111. Available from: https://www.redalyc.org/pdf/531/53163822007.pdf. [30 June 2024].

Leonaitė, E. & Žalimas, D. 2016, The Annexation of Crimea and Attempts to Justify It in the Context of International Law. *Lithuanian Annual Strategic Review. 2015-2016*. Volume 14. Military Academy of Lithuania. DOI: 10.1515/lasr-2016-0001.

Magnuson, S., Keay, M., Metcalf, K. 2022, Countering Hybrid Warfare: Mapping Social Contracts to Reinforce Societal Resiliency in Estonia and Beyond. *Texas National Security Review*. Volume 5, Issue 2 (Spring 2022). Available from: https://tnsr.org/wp-content/uploads/2022/01/TNSR-Vol-5-Issue-2-Magnuson-et-al.pdf. [30 June 2024].

Maternowski, C. & Malhotra, A. 2023, *Cutting through the Haze: Gray Zone Operations and Contemporary Threats*. The Canadian Army Journal. Available from: https://natoassociation.ca/wp-content/uploads/2023/08/Cutting-through-the-Haze-Summer-2023.pdf [30 June 2024].

Oates, S. 2016. Russian Media in the Digital Age: Propaganda Rewired. *Russian Politics*, *1*(4), 398-417. https://doi.org/10.1163/2451-8921-00104004.

Rácz, A. 2015, *Russia's hybrid war in Ukraine. Breaking the Enemy's Ability to Resist*. FIIA report No 43. 2015, The Finish institute on international affairs. pp. 1-101. Available from: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf [30 June 2024].

The Committee to Protect Journalists 2022, Understanding the Laws Relating to "fake news" in Russia. *Thomson Reuters Foundation*. Available from: https://cpj.org/wp-content/uploads/2022/07/Guide-to-Understanding-the-Laws-Relating-to-Fake-News-in-Russia.pdf [30 June 2024].

Uzman, G. 2017, Is hybrid warfare really new? Ankara Üniversitesi *SBF Dergisi*, 72(3). September 2017. pp. 525-540. Available from: https://dergipark.org.tr/tr/download/article-file/345212. [30 June 2024].

Recommended readings

Amos C. Fox. 2021, *Russian hybrid warfare: A framework*. Journal of military studies. December 2021, Volume & Issue. Volume 10, Issue 1, pp. 60–72. Available from: https://doi.org/10.2478/jms-2021-0004 or https://sciendo.com/article/10.2478/jms-2021-0004?tab=article [30 June 2024].

Bilal, A. 2021, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *Nato Review.* Available from: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html [30 June 2024].

Berkowitz, B. D. 2007, *The New Face of War: How War Will Be Fought in the 21st Century.* Free Press.

Borda. A. Z. (2022) Ukraine war: what is the Budapest Memorandum and why has Russia's invasion torn it up? *The Conversation*. March 2, 2022. Available from: https://theconversation.com/ukraine-war-what-is-the-budapest-memorandum-and-why-has-russias-invasion-torn-it-up-178184 [30 June 2024].

Buchan, P. 2013, Pandours, Partisans, and Petite Guerre: The Two Dimensions of Enlightenment Discourse on War. *Intellectual History Review*, Vol. 23, No. 3, pp. 329–347. Available from: https://doi.org/10.1080/17496977.2012.723338.

Epifanova, A. 2020, Deciphering Russia's "Sovereign Internet Law". Tightening Control and Accelerating the Splinternet. *German Council on Foreign Relations*. January 16, 2020. Available from: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [30 June 2024].

Galeotti, M. 2018, (Mis)Understanding Russia's two 'hybrid wars'. *Eurozine*. 29 November 2018. Available from: https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/#. [30 June 2024].

Giannopoulos, G., Smith, H. & Theocharidou, M. (eds) 2021, *The Landscape of Hybrid Threats: A Conceptual Model*. Available from: https://dgap.org/sites/default/files/article_pdfs/the_landscape_of_hybryd_threats-eu_publication_office.pdf [30 June 2024].

Hagen, R. A. 2023, *From Battlefield to Bytes: A Deep Dive into Hybrid Warfare*. Available from: https://www.linkedin.com/pulse/from-battlefield-bytes-deep-dive-hybrid-warfare-raymond-andrè-hagen/ [30 June 2024].

Kandrik, M. 2023, *Rethinking Russian Hybrid Warfare. Irregular Warfare Center*. Available from: https://irregularwarfarecenter.org/publications/perspectives/rethinking-russian-hybrid-warfare/ [30 June 2024].

Rumer, E. 2019, *The Primakov (Not Gerasimov) Doctrine in Action*. Carnegie Endowment for International Peace. Available from: https://carnegie-production-assets.s3.amazonaws.com/static/files/files__Rumer_PrimakovDoctrine_final1.pdf [30 June 2024].

Soldatenko, M. 2023, Constructive Ambiguity of the Budapest Memorandum at 28: Making Sense of the Controversial Agreement. *Lawfare*. The Lawfare Institute, February 7, 2023. Available from: https://www.lawfaremedia.org/article/constructive-ambiguity-of-the-budapest-memorandum-at-28-making-sense-of-the-controversial-agreement. [30 June 2024].

U.S. Army Training and Doctrine Command 2007, *Military Guide to Terrorism in the Twenty-First Century*. Handbook. Available from: https://apps.dtic.mil/sti/pdfs/ADA472623.pdf. [30 June 2024].

Watling, J.; Danylyuk, O. V. & Reynolds, N. 2023, *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War*, February 2022 – February 2023. 29 March 2023 Special Report, Royal United Services Institute for Defence and Security Studies. pp.1-39. Available from: https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022. [30 June 2024].

Watling, J. & Reynolds, N. 2022, *The Plot to Destroy Ukraine*. 15 February 2022, Special Report, Royal United Services Institute for Defence and Security Studies, pp.1-19. Available from: https://static.rusi.org/special-report-202202-ukraine-web.pdf. [30 June 2024].

Session 5. Information warfare

Session aim: The session aims to create opportunities for students to develop skills to identify problems related to information warfare

Session duration: 70 hours: 54 independent learning hours and 16 contact learning hours (6 hours online, 10 hours face to face, of which 3 hours for case study)

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Modern information environment and its vulnerabilities
2. Global knowledge warfare: the impact of strategic narratives produced by Russia, China, and the United States on changing security environment
3. Information advocacy activities such as fake news, disinformation campaigns, alternative reality, and use of radicalisation on the internet
4. Culture as a Soft Power and Hybrid Threat
5. Russian Trolls and fake news as a security threat

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, students will prepare for the case study about information warfare and their impact on fundamental rights.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars, students will solve the case study and make the presentations.

Essential reading

Barclay, D. A., 2018, *Fake News, Propaganda, and Plain Old Lies: How to Find Trustworthy Information in the Digital Age*, Rowman & Littlefield.

Bhatti, A. M., Mehmood, N. 2024, American Strategic Narrative - A Success Story or an Archetypal Rhetoric, Routledge Open Research. Available from: https://routledgeopenresearch.org/articles/3-23 [5 June 2024].

Binder, J. F., & Kenyon, J., 2022, *Terrorism and the internet: How dangerous is online radicalization?*. *Frontiers in psychology*, 6639. Available from:

https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.997390/full?utm_source=Email_to_authors_&utm_medium=Email&utm_content=T1_11.5e1_author&utm_campaign=Email_publication&field&journalName=Frontiers_in_Psychology&id=997390. [14 November 2023].

Confucius Institutes 2019, *Hybrid Threats: Confucius Institutes*, NATO Strategic Communication Centre of Excellence, 6 June 2019. Available from: https://stratcomcoe.org/cuploads/pfiles/confucius_institutes.pdf. [20 June 2023].

European Commission, 2018, *Final report of the High Level Expert Group on Fake News and Online Disinformation*. Available from: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation [9 December 2023].

Darczewska, J. 2014, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study.* Centre for Eastern Studies Warsaw. Point of View, No 42, pp.1-26. Available from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf .[26 August 2023].

European Commission, 2019, *Action Plan Against Disinformation: Report on progress,* June 2019, Available from: https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf [26 August 2023].

Fedasiuk, R. 2022, *How China's united front system works overseas,* The Strategist, Australian Strategic Policy Institute, 13 April 2022. Available from: https://www.aspistrategist.org.au/how-chinas-united-front-system-works-overseas/. [20 June 2023].

Giles, K.; Sherr, J.; Seaboyer, A. 2018, *Russian reflexive control*. Royal Military College of Canada. pp.1-71. Available from: https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control. [29 August 2023].

Gunton, K., 2022, The Impact of the Internet and Social Media Platforms on Radicalisation to Terrorism and *Violent Extremism*. Privacy, Security and Forensics in The Internet of Things (IoT). Available from: https://books.google.lt/books?hl=lt&lr=&id=4n1fEAAAQBAJ&oi=fnd&pg=PA166&ots=nCVvihlRZS&sig=ez0z5QzZDZqCYLtFgHqfRMmzDlA&redir_esc=y#v=onepage&q&f=false [2 January 2024].

Kedem, M. 2023, Beyond Illusion | Addressing the Cybersecurity Impact of Deepfakes and Synthetic Media. *SentinelOne blog*. December 12, 2023. Available from: https://www.sentinelone.com/blog/beyond-illusion-addressing-the-cybersecurity-impact-of-deepfakes-and-synthetic-media/. [30 June 2024].

Läänemets, M. 2022, *China's Strategic Narratives and Soft Power Engagements as a Means of Influence*. Available from: https://assets.nationbuilder.com/menleuropa/mailings/1419/attachments/original/Geopol-report_China_final_22.03.2022.pdf?1649242620. [20 June 2023].

Nissen, T. E. 2016, *Social Media's Role in 'Hybrid Strategies'*. NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/cuploads/pfiles/tomas_nissen_article_12-09-2016.pdf. [30 June 2024].

Periodic insight 2022, *Disinformation narratives about the war in Ukraine,* No 14. 21/10/2022 to 22/11/2022. https://edmo.eu/wp-content/uploads/2022/07/Periodic-insight-n.14-Disinformation-narratives-about-the-war-in-Ukraine.pdf [31 September 2023].

Pomerantsev, P. & Weis, M. 2014, The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. *The Interpreter*, The Institute of Modern Russia, Available from: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf. [30 June 2024].

Posetti, J., Matthews, A., 2018, *A short guide to the history of 'fake news' and disinformation.* International Center for Journalists, 7(2018), 2018-07. Available from: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf [17 October 2023].

Prus, J. 2015, *Russia's Use of History as a Political Weapon*. Policy papers, No. 12 (114), p. 1-8. Available from: https://www.files.ethz.ch/isn/191038/PISM%20Policy%20Paper%20no%2012%20(114).pdf. [30 June 2024].

Roeder, O. 2018, *Why We're Sharing 3 Million Russian Troll Tweets*, FiveThirtyEight. Available from: https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/. [29 August 2023].

Thiele, R. 2020, *Artificial Intelligence – A key enabler of hybrid warfare*. Hybrid CoE Working Paper 6. March 2020. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf. [30 June 2024].

Recommended readings

A minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session 2018, *Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National Security*., pp. 1-206. Available from: https://www.govinfo.gov/content/pkg/CPRT-115SPRT28110/pdf/CPRT-115SPRT28110.pdf .[29 August 2023].

Adamsky, D. 2019, *Russian Nuclear Orthodoxy. Religion, Politics, and Strategy*. Stanford University press.

Aïmeur, E., Amri, S., & Brassard, G. 2023, Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, *13*(1), 30. https://doi.org/10.1007/s13278-023-01028-5.

Allington, D., 2020, *Conspiracy Theories, Radicalisation and Digital Media*. London: Kings College London. Available from: https://gnet-research.org/wp-content/uploads/2021/02/GNET-Conspiracy-Theories-Radicalisation-Digital-Media.pdf [3 January 2024].

Barnays, E. 1928, Propaganda. Horace Liveright INC. Available from: https://www.voltairenet.org/IMG/pdf/Bernays_Propaganda_in_english_.pdf. [28 August 2023].

Bartlett, J., & Miller, C., 2010, *The power of unreason: Conspiracy theories, extremism and counter-terrorism* London: Demos. pp. 1-54. Available from: http://westernvoice.net/Power%20of%20Unreason.pdf [28 September 2023].

Bennett, L. & Livingston, L. 2020, *The disinformation order: Disruptive communication and the decline of democratic institutions*. European Journal of Communication No. 33(2), April 2020. pp.122-139. Available from: https://journals.sagepub.com/doi/10.1177/0267323118760317 or https://www.researchgate.net/publication/324193884_The_disinformation_order_Disruptive_communication_and_the_decline_of_democratic_institutions .[29 August 2023].

Bennett, L. & Livingston, L. 2020, *A Brief History of the Disinformation Age Information Wars and the Decline of Institutional Authority from Part I - Disinformation in Political and Historical Context.* Cambridge University Press. October 2020. pp.3-40. Available from: https://www.cambridge.org/core/books/disinformation-age/brief-history-of-the-disinformation-age/7F0A2F8BABA0B5CA802EC3AB4F76B818 .[29 August 2023].

Chesney, R., & Citron, D. 2019, Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*. Available from: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war. [30 June 2024].

Cialdini, R. B. 2009, *Influence Psychology of persuasion*. HarperCollins Publishers Ltd. pp.1-263.

Codarin, L., Harth, L., Lulu, J. 2021, *Hijacking the mainstream. CCP influence agencies and their operations in Italian parliamentary and local politics*, Sinopsis, 20 November 2021. Available from: https://sinopsis.cz/wp-content/uploads/2021/11/it0.pdf. [20 June 2023].

Doob, L. W. 1950, *Goebbels' Principles of Propaganda*. Public opinion quarterly. pp. 419-442.

Easton, I. 2022, *The Final Struggle. Inside China's Global Strategy*, Eastbridge Books.

Egelhofer j.l., Lecheler S., 2019, *Fake news as a two-dimensional phenomenon: a framework andresearch agenda.* Annals of the International Communication Assotiation, 2019, VOL. 43, NO. 2, 97–116. Available from: https://www.tandfonline.com/doi/epdf/10.1080/23808985.2019.1602782?needAccess=true&role=button. [5 October 2023].

Evans A. T., Williams H. J. 2022, *How extremism operates online. R*AND Corporation. Available from: https://www.rand.org/pubs/perspectives/PEA1458-2.html. [3 January 2024].

Golovchenko, Y.; Buntain, C.; Eady, G.; Brown, M.; Tucker, J. A. 2016, *Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube During the 2016 US Presidential Election*, 2020. Available from:

https://deliverypdf.ssrn.com/delivery.php?ID=714022009114095071114064083097092126021037057034004075122023003076104018076118122117023061006041103116116084005007121074109122019027055089080083126071087082099081125063047077101073011110011065068095070124085027024107003125071122126019095088107088091083&EXT=pdf&INDEX=TRUE .[29 August 2023].

Helberg, J. 2021, *The Wires of War. Technology and the Global Struggle for Power*, Avi Reader Press.

Kilcullen D 2020, The changing strategic threat Picture, The World of Intelligence. Technology. Apple Podcasts. Available from: https://podcasts.apple.com/au/podcast/the-world-of-intelligence/id1477524651?i=1000477406483 or with transcription https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/1db4fe07. [29 August 2023].

Li, E. 2018, The Rise and Fall of Soft Power. Joseph Nye's concept lost relevance, but China could bring it back. *Foreign policy*. 20 August 2018. Available from: https://foreignpolicy.com/2018/08/20/the-rise-and-fall-of-soft-power/. [30 June 2024].

Miao, J. T. 2021, *Understanding the soft power of China's Belt and Road Initiative through a discourse analysis in Europe*. Regional Studies, Regional Science, Vol. 8, Issue 1, pp. 162-177. Available from: https://www.tandfonline.com/doi/full/10.1080/21681376.2021.1921612. [20 June 2023].

Miskimmon, A., O'Loughlin, B., and Roselle, L. 2014, *Strategic Narratives: Communication Power and the New World Order*, London: Routledge.

Mölder, H.; Sazonov, V.; Chochia, A. & Kerikmäe, T. (eds) 2021, *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighbourhood, 2021,* Editors, Springer Nature, pp.1-423.

Olson, S., Prestowitz, C. 2011, *The Evolving Role of China in International Institutions. The U.S.-China Economic and Security Review Commission (prepared by The Economic Strategy Institute)*, January 2011. Available from: https://www.uscc.gov/sites/default/files/Research/TheEvolvingRoleofChinainInternationalInstitutions.pdf. [20 June 2023].

Papkova, I. 2011, *The Orthodox Church and Russian Politics,* Oxford University Press, pp. 1-265.

Rid, I. T. 2020, *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux. pp. 1-528.

Roselle, L., Miskimmon, A., and O'Loughlin, B. 2014, *Strategic narrative: A new means to understand soft power, Media, War & Conflict*, Vol. 7, no. 1, pp. 70-84. Available from: https://www.academia.edu/6682695/Roselle_L_Miskimmon_A_and_OLoughlin_B_2014_Strategic_narrative_A_new_means_to_understand_soft_power_Media_War_and_Conflict_vol_7_no_1_70_84. [20 June 2023].

Sârbu, A., Anca, G. 2023, Using Artificial Intelligence Tools for Obtaining Cognitive Warfare Advantages. *The Defence Horizon Journal*. October 23, 2023. Available from: https://tdhj.org/blog/post/artificial-intelligence-cognitive-warfare-twitter/. [30 June 2024].

United States of America v. Internet Research Agency LLC A/K/A Mediasintez LLC A/K/A Glavset LLC A/K/A Mixinfo LLC A/K/A Azimut LLC A/K/A Novinfo LLC, etc. Indictment. 2018. Available from: https://www.justice.gov/file/1035477/download. [28 August 2023].

Session 6. Common response to hybrid threats and strategies for tackling them

Session aim: The session aims to create opportunities for students to develop and design solutions to respond to hybrid threats

Session duration: 28 hours: 22 independent learning hours (8 hours before the contact week and 14 hours after the contact week) and 6 contact learning hours (4 hours online, 4 hours face to face, 2 hours for online consultation related to written analysis)

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Developing a common strategic approach to tackling hybrid threats
2. Countering hybrid threats: steps for Europe

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, the student will compile the draft outline of the written essay, which includes the chosen problem related to hybrid threats and a preliminary list of references reviewed.

The essay will be completed after the contact week and should be submitted 7 days before the end of Module 1.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

Aho, A., et al., 2023, Hybrid threats: A comprehensive resilience ecosystem. April 20, 2023. The European Centre of Excellence for Countering Hybrid Threat Available from: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ [28 June 2024].

European Commission. 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM(2020) 605 final,27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [14 July 2022].

European Commission, 2023, *Communication from Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and Committee of the Regions. Towards a more resilient, competitive and sustainable Europe* COM/2023/558 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0558&qid=1708862129657 [10 February 2024].

European Union, 2022, *Countering Hybrid Threats,* European Union, March 2022. Available from: https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-countering-HybridThreats_NewLayout.pdf [3 September 2023].

Hybrid threats: a comprehensive resilience ecosystem, 2023, Publications Office of the European Union, Luxembourg, doi:10.2760/37899. Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [12 September 2023].

Keršanskas, V., 2020, Deterrence: Proposing a more strategic approach to countering hybrid threats. The European Centre of Excellence for Countering Hybrid Threat. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf [28 June 2024].

Monaghan, S., 2022, Hybrid CoE Paper 12: Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. March 31, 2022. The European Centre of Excellence for Countering Hybrid Threat. Available from: https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/ [28 June 2024].

Sanz-Caballero, S. , 2023, *The concepts and laws applicable to hybrid threats, with a special focus on Europe*. Humanit Soc Sci Commun 10, 360, 2023. Available from:. https://doi.org/10.1057/s41599-023-01864-y [3 Febuary 2024].

Recommended readings

Bajarūnas, E., Keršanskas, B. 2018, Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome. Lithuanian Annual Strategic Review, Volume 16, Issue 1 (pp. 123–170). https://doi.org/10.2478/lasr-2018-0006 Available from: https://journals.lka.lt/journal/lasr/article/152/info [1 August 2023].

Balaban, M., & Mielniczek, P., 2018, *Hybrid conflict modeling. In 2018* Winter Simulation Conference (WSC) (pp. 3709-3720). IEEE. Available from: https://www.researchgate.net/profile/Mariusz-Balaban/publication/330880179_HYBRID_CONFLICT_MODELING/links/5ceb02a092851c4eabc114a2/HYBRID-CONFLICT-MODELING.pdf [12 November 2023].

European Union External Action, 2021, *"Questions and Answers about the East StratCom Task Force"* , October 27, 2021. Available from: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcomtask-force_en#11232 [29 August 2023].

Lasoes N., 2022, *Realising the EU Hybrid Toolbox: opportunities and pitfalls,* December 2022. Available from: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf [26 December 2023].

Moeini, A., Paikin, Z. 2023, IN SEARCH OF A EUROPEAN SECURITY ORDER AFTER THE UKRAINE WAR. The Institute for Peace & Diplomacy. Available from: https://peacediplomacy.org/wp-content/uploads/2023/04/In-Search-of-a-European-Security-Order-After-the-Ukraine-War.pdf [1 February 2024].

Sanz-Caballero, S. 2023, The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities and Social Sciences Communications, Vol. 10, 360 (2023). Available from: https://www.nature.com/articles/s41599-023-01864-y [1 February 2024].

Wigell, M., Mikkola, H., Juntunen, T., 2021, *Best Practices in the whole-of-society approach in countering hybrid threats. Study Requested by the INGE committee, European Parliament Coordinator,* 2021 May Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf [26 October 2023].

Zandee D., van der Meer S., Stoetman A., 2021, *Countering hybrid threats Steps for improving EU-NATO cooperation*, 2021 October. Available from: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [26 December 2023].

Session 7. Research strategies and methods

Session aim: The session aim is to create opportunities for students to develop skills in academic writing and conducting research

Session duration: 19 independent learning hours and 6 contact learning hours

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Models of strategic analysis
2. Research strategies and methods in social science research
    a. Evaluating and selecting sources
    b. Collection of material/ and its systematization
3. Structure of student paper
    a. Formulating a problem
    b. Setting the aim of the study and hypothesis
    c. Setting research questions or hypothesis
    d. Theoretical part of the work
    e. Research methodology. Creating or selecting a model or concept to prepare for a study
    f. Ethical issues in research. Responsibility for conducting a study and storing data
    g. Presentation and analysis of research results. Formulating conclusions
4. Drafting and formatting a student paper
    a. Academic writing style
    a. Citing and referencing sources

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, the student will compile the draft outline of the written essay, meeting already the criteria of a student paper.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

ASA 2021, *Ethical guidelines for good research practice*. Association of Social Anthropologists of the UK (ASA). https://www.theasa.org/ethics/

Šlapkauskas, V & Zuzevičiūtė, V. 2022, Between Security and Safety - Outlines for the Contours of Research in Search of a Holistic Approach // Europe Alone : Small State Security without the United States / edited by David Schultz, Aurelija Pūraitė, Vidmantė Giedraitytė. Lanham: Rowman & Littlefield International, Chapter 18. ISBN 9781538167281. eISBN 9781538167298. p. 403-422.

Recommended readings

Baldwin J. R., Pingault J.-B., Schoeler T., Sallis H. M., Munafò M. R. 2022, Protecting against researcher bias in secondary data analysis: Challenges and potential solutions. *European Journal of Epidemiology*, 37(1), 1–10.

Gioia, D. 2021, A Systematic Methodology for Doing Qualitative Research. The Journal of applied behavioral science, 2021, Vol.57 (1), p.20-29.

Marx, S, 2023, Mapping as critical qualitative research methodology. International journal of research & method in education, 2023, Vol.46 (3), p.285-29.

McIntyre, D. 2020, *How to think about homeland security. Volume 1, The imperfect intersection of national security and public safety*. Rowman & Littlefield.
Shared „Dublin“ Descriptors for the Short Cycle, First Cycle, Second Cycle and Third Cycle Awards. 2004, Draft 1.31 working document on JQI meeting in Dublin on 18/10/2004. Viewed on 6 June 2023. Internet access: http://www.unidue.de/imperia/md/content/bologna/dublin_descriptors.pdf.

Urcia, Ivan A. 2021, Comparisons of Adaptations in Grounded Theory and Phenomenology: Selecting the Specific Qualitative Research Methodology. International journal of qualitative methods, 2021, Vol.20, p.16094069211045.

Zyphur, M. J., & Pierides, D. C. 2017, Is quantitative research ethical? Tools for ethically practicing, evaluating, and using quantitative research. *Journal of Business Ethics*, *143*(1), 1–16. https://doi.org/10.1007/s10551-017-3549-8.

8.1.5 Delivery Timetable for Module 1

Module 1	September 1 - October 3, 2025
Phase	**Dates**
Independent learning phase - Reading mandatory literature and studying e-learning materials - Drafting the outline of the written analysis - Draft the outline of the essay - Preparation for the case study (about tendencies of contemporary warfare about hybrid threats) - Preparation for the case study (of information warfare and their impact on fundamental rights) **Assessment:** - Online test	**September 1 - 19, 2025** September 15, 2025 - online test
Contact learning phase **Assessments:** - Solving the case study about tendencies of contemporary warfare about hybrid threats - Solving the case study about information warfare and their impact on fundamental rights	**September 22 - 26, 2025**
Preparation of assessment tasks: - **Written analysis** (of security strategies) preparation and submission - **Written essay** (problems related to hybrid threats) preparation and submission	**September 29 - October 3, 2025** - October 24, 2025 - deadline for submitting the written analysis - October 27, 2025 - deadline for submitting the essay
Reassessments	November 21, 2025 - deadline for liquidation of student debts

8.2 Module 2. Prevention and Cooperation in Countering Hybrid Threats

Pre-requisite Modules:	Module 1		ECTS Credits 10
Contact learning hours	**Independent learning hours**	**Experiential learning**	**Total**
60	200	0	260

8.2.1 Module Aim and Module Learning Outcomes

Module aim: the student develops skills to manage tools for prevention and cooperation in countering hybrid threats.

Upon completion of this module, the student will be able to:

- explain the specifics of modern crimes of hybrid nature and criminal procedure concepts and their connection with the principles of fundamental rights;
- identify problems, recommend, and elaborate tools and methods of protection against hybrid threats by working in a team and benefiting from team learning processes;
- explain risks related to cybersecurity and business continuity and infringement of fundamental rights;
- critically analyse the importance of prevention and countering hybrid threats using relevant tools and means of cooperation.

8.2.2 Module Learning Strategy

Module 2 deals with tools for prevention and cooperation in countering hybrid threats.

The learning process of the module is divided into 2 phases:

- **Independent learning phase**. The independent learning phase before the contact learning phase lasts for 3 weeks (120 hours). During this time, students should lay the groundwork for the contact learning phase of the module by getting acquainted with relevant literature, going through eLearning tools, and completing self-assessment tasks. The self-assessment tasks will serve as a prerequisite for participating in the contact week. Additionally, while completing the assessment assignments (written analysis, case study) students should be able to discuss and apply knowledge and methods covered in the learning materials. The eLearning platform will be open during the study period, and students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

  During the independent learning phase, the student will compile a draft outline of the written analysis, which includes tools and means of cooperation to analyse, and a preliminary list of references reviewed.

- **Contact learning phase**. The contact learning phase lasts for 26 hours in the online environment. During this phase, students participate in lectures, which will cover key theoretical and methodological aspects of the module, as well as seminars applying and reflecting on the topics of the module.

  During the contact learning phase, students will prepare the case study and deliver the presentation.

  After the contact phase, students will perform the online test about specifics of modern crimes of hybrid nature, criminal procedure concepts, and risks related to cybersecurity and business continuity. They will also complete a written analysis and submit 5 days before the end of Module 2.

Sessions of Module 2:

- Session 1. Crimes of a hybrid nature
- Session 2. International criminal law and legal tools for tackling hybrid threats
- Session 3. Prevention of hybrid threats
- Session 4. Cybersecurity and cyber incident management
- Session 5. International cooperation

8.2.3 Module Assessment Strategy

There are three assessment assignments for the module:

- online test with open-ended questions;
- case study about identifying problems, recommending and elaborating methods of social protection against hybrid threats;
- written analysis of the importance of prevention and countering hybrid threats using relevant tools and means of cooperation.

Online test with open-ended questions. The student must answer the questions within the allotted time. Students are allowed to use all study materials and necessary sources while answering. The test is assessed non-distinctively, and to pass, the student must answer to each question correctly. In case of failing, the student will have the opportunity for reassessment under the same conditions as the assessment in terms of testing environment and allotted time. The student has approximately two weeks for reassessment.

Case study about identifying problems, recommending and elaborating methods of social protection against hybrid threats. Scenarios on social protection against hybrid threats will be presented to students, and they will choose one case to analyse. The case study is performed as a group work, and the group size is up to 5 students. It is allowed to work individually if the student has expressed their will to do so. The case study is assessed non-distinctively, and to pass, the student must meet all the assessment criteria. In

case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the case study and/or the presentation. The lecturer gives feedback about meeting assessment criteria in oral form after the presentation.

If based on the group members' evaluation, some of the group members did not contribute to the assignment, then the student should perform a new case study independently.

Written analysis of the importance of prevention and countering hybrid threats using relevant tools and means of cooperation**.** The student will select the topic from the learning materials or from recently published European Union (policy) documents. The topic will be previously agreed upon with the lecturer. The writing process will be supported by the lecturer, if necessary. The analysis is assessed non-distinctively, and to pass, the student must meet all the assessment criteria. The lecturer gives feedback about meeting assessment criteria in written or/and oral form. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the analysis. The student has approximately two weeks for eliminating the deficiencies.

For information on the assessment criteria see in the **ANNEX 1 Assessments.**

8.2.4 Module 2 Sessions

Session 1. Crimes of a hybrid nature

Session aim: The session aims to create opportunities for students to develop knowledge to specify modern crimes of hybrid nature

Session duration: 42 independent learning hours (36 hours before the contact week and 6 hours after the contact week) and 6 contact learning hours

Learning environment(s) and requirements

eLearning environment

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. *Modus operandi* used for committing crimes of hybrid nature
2. Modern crimes and specifics of white-collar crimes and terrorism
3. Compromising and destabilisation of financial security and state finance
4. Corruption as a hybrid threat
5. Detecting radicalisation, violent extremism, terrorism, and organised crime
6. Assassinations and other state-orchestrated crimes (poisoning, accident falls, staged suicides, etc.)

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

After the contact learning phase, the student will have one week to prepare for an online test with open-ended questions. In the online test the student will demonstrate content knowledge of Session 1, Session 2 and Session 4. The feedback about the test will be provided in Moodle.

Essential reading

Aleksi Aho; Catarina Midões; Arnis Šnore., 2020, Hybrid threats in the financial system, Hybrid CoE Working Paper 8, Hybrid CoE, Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf. [3 February 2025].

Bachmann, S.D. and Gunneriusson, H., 2014. Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *The Journal on Terrorism and Security Analysis*.

Communication from the Commission to the European parliament, the European council, the Ccouncil, the European economic and social committee and the Committee of the regions on the EU security union strategy, COM/2020/605 final, Bruxelles, 24.7.2020.

Council decision (EU, Euratom) 2020/2053, of 14 December 2020 on the system of own resources of the European Union and repealing Decision 2014/335/EU Euratom, Official Journal of the European Union L 424/1, 15.12.2020

Consolidated version of The treaty on European Union, Official Journal of the European Union C 202/13, 7.6.2016.

Consolidated version of The treaty on the functioning of the European Union, Official Journal of the European Union C 202/47, 7.6.2016.

European Commission 2023, *Joint Communication to the European Parliament, the Council and the European Economic and Social Committee on the fight against corruption.* JOIN(2023)12 final. Available from: https://commission.europa.eu/document/download/b6888f6a-45ed-4af7-b85a-6712dfe8952c_en?filename=JOIN_2023_12_1_EN.pdf. [1 February 2024].

European Commission 2023, *Proposal for a directive of the European Parliament and of the Council on combating corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371 of the European Parliament and of the Council.* COM (2023) 234 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0234. [1 February 2024].

European Commission 2020a, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM (2020) 605 final, pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [13 January 2024].

European Commission 2020b, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.* COM(2020) 795 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795. [13 January 2024].

European External Action Service 2023, *Missions and Operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

European External Action Service 2022, *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security*. Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en. [20 September 2023].

European Parliament and the Council of the European Union 2021, *Regulation (EU) 2021/784 of the European Parliament and of the Council* of *29 April 2021on addressing the dissemination of terrorist*

content online. (OJL 172, 17.5.2021). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784. [13 January 2024].

European Parliament and the Council of Europe 2022, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065 [13 January 2024].

European Union Agency for Fundamental Rights 2021, *Report. Directive (EU) 2017/541 Combatting Terrorism. Impact on Fundamental Rights and Freedoms. Luxembourg: Publications Office of the European Union.* Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-directive-combating-terrorism_en.pdf. [13 January 2024].

Europol 2023, *European Union Terrorism Situation and Trend Report*. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

Faleg, G (ed) 2022, *The EU's Civilian Headquarters: Inside the control room of civilian crisis management*. European Union Institute for Security Studies EUISS, Chaillot Paper 175, Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/eus-civilian-headquarters. [10 September 2023].

Huss, O, Beke, M, Wynarski, J, & Slot, B 2023, *Handbook of good practices in the fight against corruption.* Publications Office of the European Union. doi:10.2837/575157.

Informal Ecofin, 2019. *Resilience of financial market infrastructure and the role of the financial sector in countering hybrid threats,* EU2019.FI Available from: https://valtioneuvosto.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf. [3 February 2025].

Institute for Economics & Peace 2024, *Global Terrorism Index 2024: Measuring the Impact of Terrorism*, Sydney. Available from: http://visionofhumanity.org/resources. [26 February 2024].

Johnson III, B.M., 1992, Executive Order 12,333: The permissibility of an American assassination of a foreign leader. *Cornell Int'l LJ*, 25, p.401.

Lakhani, S, White, J & Wallner, C 2022, *The gamification of (violent) extremism. An exploration of emerging trends, Future threat scenarios and potential P/CVE solution,.* Luxembourg: Publications, Office of the European Union. Available from: https://home-affairs.ec.europa.eu/system/files/2022-09/RAN%20Policy%20Support-%20gamification%20of%20violent%20extremism_en.pdf. [13 January 2024].

MacLachlan, K 2019, *Corruption as Statecraft.* s.l.: Transparency International.

Missiroli, A., 2024, From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses. In *Addressing Hybrid Threats* (pp. 40-56). Edward Elgar Publishing.

Pisoiu, D & Renard, T 2022, *Responses to returning foreign terrorist fighters and their families*, RAN Manual, 2nd Edition, Radicalisation Awareness Network. Available from: https://home-affairs.ec.europa.eu/document/download/7cbeded1-383c-4b58-b74b-88ececeb93f0_en?filename=ran_manual_responses_returning_foreign_terrorists_and_their_families_en.pdf. [13 January 2024].

Ranstrop, M 2019, *Islamist Extremism. Practical Introduction, RAN Factbook,* RAN Centre of Excellence.

Schmitt, M.N., 1992, State-sponsored assassination in international and domestic Law. *Yale J. Int'l L.*, 17, p.609.

Sternkenburg, N 2019, *Far-right extremism. Practical introduction. RAN Factbook,* The RAN Centre of Excellence. Available from: https://home-affairs.ec.europa.eu/system/files/2019-12/ran_fre_factbook_20191205_en.pdf. [13 January 2024].

Zengel, P., 1991, Assassination and the law of armed conflict. *Mil. L. Rev.*, 134, p.123.

Recommended readings

Bértoa, F. C., and Tsutskiridze, L., 2024. *Money Rules: Parties, Oligarchs and Funding Regulation in Post-Soviet Countries*. Taylor and Francis.

Council of the European Union, 2022, *Draft Council conclusions on a framework for a coordinated EU response to hybrid campaigns. Draft Council Conclusions,* 10013/22.

Council of the European Union 2021, *Mini-concept on civilian CSDP support to countering hybrid threats. European External Action Se*rvice*, Written Consultation on the third revision of the Mini-concept on civilian CSDP support to countering hybrid threats,* WK 11851/2020 REV 2.

Darczewska, Jolanta. 2014. *The anatomy of Russian information warfare. The Crimean operation, a case study*. OSW Studies, vol. 42.

Dayspring, S.M., 2015, Toward a theory of hybrid warfare: the Russian conduct of war during peace (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Official Journal of the European Union L 333/164, 27.12.2022.

Demertzis, Maria; Wolff, Guntram B., 2019. Hybrid and cybersecurity threats and the European Union's financial system, Bruegel Policy Contribution, No. 2019/10, Bruegel, Brussels. Available from: https://hdl.handle.net/10419/237635. [3 February 2025].

European Commission 2018, *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council,* JOIN (2018) 16 final. Available from: EUR-Lex - 52018JC0016 - EN - EUR-Lex (europa.eu). [21 November 2022].

European Commission 2016, *Joint Framework on countering hybrid threats a European Union response. Joint communication to the European Parliament and the Council,* JOIN (2016) 18 final. Available from: JOIN_2016_0018_FIN.ENG.xhtml.1_EN_ACT_part1_v8.docx (europa.eu). [21 November 2022].

EUR-Lex 2012, 'Consolidated Version of the Treaty on the Functioning of the European Union', *Official Journal of The European Union,* C 326. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF. [20 September 2023].

Faleg, G & Kovalčíková, N 2022, 'Rising hybrid threats in Africa: Challenges and implications for the EU', Brief no. 3, European Union Institute for Security Studies. Available from: https://www.iss.europa.eu/content/rising-hybrid-threats-africa. [21 November 2022].

Gaglio, I, Guzzon, J, Bartz, K, Marcolin, L, Kryeziu, R, Disley, E & Hulme, S 2023, *Strengthening the fight against corruption: assessing the EU legislative and policy framework.* Publications Office of the European Union. doi:10.2837/22427.

Galeotti, M., 2016, Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?, *Small Wars & Insurgencies*, 27(2), 282-301.

Gilinskiy, Y., 2006, Crime in contemporary Russia. *European Journal of Criminology*, 3(3), 259-292.

Goldfarb, A., 2010, Death of a Dissident: The Poisoning of Alexander Litvinenko and the Return of the KGB. Simon and Schuster.

Gonçalves, C.P., 2019, Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats. In *Cyberspace*. IntechOpen.

Hoogenboom, B., and Hoogenboom, B., 2010, *Blinded by the Light: The Interweaving of (Organised) Crime, White Collar Crime, State Crime and Terrorism*. The Governance of Policing and Security: Ironies, Myths and Paradoxes, pp. 149-168.

Huss, O 2022, *Strategic Corruption as a Threat to Security and the New Agenda for Anti-Corruption.* Available from: https://www.corruptionjusticeandlegitimacy.org/post/strategic-corruption-as-a-threat-to-security-and-the-new-agenda-for-anti-corruption. [1 February 2024].

Kondrushenko, Y., 2019, Responding to Hybrid Warfare: The Case of the Attempted Assassination of Sergey Skripal.

Korauš, Antonín; Jančíková, Eva; Gombár, Miroslav; Kurilovská, Lucia; Černák, Filip., 2024. Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures. Journal of Risk Financial Management. 2024, 17(2), p. 55; Available from: https://doi.org/10.3390/jrfm17020055.

Kostarakos, M., 2023, European Union and NATO Cooperation in Hybrid Threats. In *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies* (pp. 405-423). Cham: Springer International Publishing.

Neville, S.B., 2015, Russia and hybrid warfare: identifying critical elements in successful applications of hybrid tactics (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Schmid, A P 2023, Terrorism prevention: Conceptual issues (Definitions, typologies and theories), In: Handbook of Terrorism Prevention and Preparedness, ed. Schmid, A P, The Hague: International Centre for Counter-Terrorism. Available from: https://www.icct.nl/sites/default/files/2023-01/Chapter-2-Handbook-.pdf. [13 January 2024].

Sari, A., 2020, Hybrid threats and the law: Concepts, trends and implications. *Hybrid Centre of Excellence Trend Report*.

United Nations Office on Drugs and Crime (UNODC), 2004. *United Nations Convention Against Corruption.* Available from: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf. [1 February 2024].

Ware, J. 2023, *The third generation of online radicalization*, Program on Extremism at George Washington University. Available from: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/third-generation-final.pdf. [13 January 2024].

White, R.F., 2008, Assassination discourse and political power: The death of Alexander Litvinenko. *Assassination Research*, 5(2), pp.1-8.

Session 2. International criminal law and legal tools for tackling hybrid threats

Session aim: The session aims to create opportunities for students to learn essential elements of European and international criminal law and procedure

Session duration: 36 independent learning hours (30 hours before the contact week and 6 hours after the contact week) and 6 contact learning hours

Learning environment(s) and requirements
eLearning environment

Learner resources
PCs and/or mobile devices with the latest versions of browsers

Session topics

1. International and European Union criminal law and criminal procedure against responsible states and actors
2. Criminalisation of new types of criminal activities as a preventive tool
3. Court jurisdiction in criminal procedure on European and international level
4. Remedies and other tools for the prevention of hybrid attacks
5. Context of fundamental rights

Learning activities
During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

In the contact week, which will take place in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

After the contact learning phase, the student will have one week to prepare for an online test with open-ended questions. In the online test, the student will demonstrate content knowledge of Session 1, Session 2 and Session 4. The feedback about the test will be provided in Moodle.

Essential reading

Council Decision 2014/145/CFSP of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. Available from: https://eur-lex.europa.eu/eli/dec/2014/145(1)/oj. [11.December 2024.]

Dinstein, Y., 2017, *War, aggression and self-defence*. Cambridge University Press.

Hufbauer, G.C., Schott, J.J., Elliott, K.A. and Oegg, B.,2010, *Economic sanctions: New directions for the 21st century*. Peerson Institute for International Economics.

Johnson, L. D. 2022, United Nations Response Options to Russia's Aggression: Opportunities and Rabbit Holes, *Just Security*, 1.

Kempees, P., 2021., *Hard Power' and the European Convention on Human Rights*. International Studies in Human Rights. Brill.

Piper, D.C. 1972, The Legal Control of the Use of Force and the Definition of Aggression. *Ga. J. Int'l & Comp. L.*, 2, p.1.

Ruys, T. 2010, *'Armed attack'and Article 51 of the UN Charter: evolutions in customary law and practice* (Vol. 74). Cambridge University Press.

Sari, A. 2020, *Hybrid threats and the law: Concepts, trends and implications*. Hybrid Centre of Excellence Trend Report, 3.

Vasiliev, S. 2022, Aggression against Ukraine: Avenues for Accountability for Core Crimes, EJIL:Talk, 3 March 2022.

Recommended readings

Casey-Maslen, S. 2024. *Hybrid Warfare Under International Law*. Bloomsbury Academic.

Elliott, K.A. and Uimonen, P.P. 1993, *The effectiveness of economic sanctions with application to the case of Iraq*. Japan and the World Economy, 5(4), pp.403-409.

Elliott, K.A. and Hufbauer, G.C. 1999, Same song, same refrain? Economic sanctions in the 1990's. *American Economic Review*, 89(2), pp.403-408.

Fogt, M.M. 2021, Legal Challenges or Gaps by Countering Hybrid Warfare-Building Resilience in Jus Ante Bellum. *Sw. J. Int'l L.*, 27, p.28.

Fridman, O., 2018, *Russian "Hybrid Warfare": Resurgence and Politicization*. Oxford University Press.

Górka, M. 2023, The Wagner Group as a Tool of Russian Hybrid Warfare. *Polish Political Science Yearbook*, 52(2), pp. 83-98.

Harris, D. J., O'Boyle, M., Bates, E., and Buckley, C. 2023, *Law of the European convention on human rights*. Oxford University Press.

Heller, K. Jon, 2022, Creating a Special Tribunal for Aggression Against Ukraine is a Bad Idea, *Opinio Juris*, 7 March 2022.

Hufbauer, G.C. and Jung, E., 2020, What's new in economic sanctions?. *European economic review*, 130, p.103572.

Lonardo, L. 2021, EU Law against hybrid threats. A first assessment, in European Papers, 2021, vol. 6, pp. 1075–1096.

McDougall, C., 2022, Prosecuting Putin for his Crime of Aggression Against Ukraine: Part Two, *Oxford Human Rights Hub*, 8 March 2022.

Mowbray, A., 2012, *Cases, materials, and commentary on the European Convention on Human Rights*. Oxford University Press.

Regulation EU Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 Amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences.

Rizzotti, M. A., 2019, Russian Mercenaries, State Responsibility, and Conflict in Syria: Examining the Wagner Group under International Law. *Wis. Int'l LJ*, 37, p. 569.

Sanz-Caballero, S., 2023, The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, 10(1), pp. 1-8.

Sari, A., 2020. Hybrid threats and the law. Concepts, trends and implications. In: Hybrid CoE Trend Report 3, Apr 2020, p. 8.

Schabas, W. A., 2015, *The European convention on human rights: a commentary*. Oxford University Press.

United Nations Security Council, 'Resolution 138 on questions relating to the case of Adolf Eichmann, UN Doc S/RES/138(1960).

Van Dijk, P., and Van Hoof, G. J., 2023. *Theory and practice of the European Convention on Human Rights*. Martinus Nijhoff Publishers.

Session 3. Prevention of hybrid threats
Session aim: The session aims to create opportunities for students to develop knowledge on prevention tools and methods of countering crimes of hybrid nature
Session duration: 18 independent learning hours and 6 contact learning hours (of which 3 hours for assessment)
Learning environment(s) and requirements eLearning environment
Learner resources PCs and/or mobile devices with the latest versions of browsers
Session topics/Indicative content 1. Prevention strategies in countering hybrid threats 2. Tools and methods for preventing hybrid incidents 3. Hybrid attack methods in combination with psychological aspects and methods of protection
Learning activities During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums. Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks. During the independent learning phase, students will prepare for the case study about identifying problems, recommending and elaborating tools and methods of protection against hybrid threats. During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars. During the contact week, students will solve the case study and make presentations.
Essential reading European Union Agency for Cybersecurity (ENISA) 2020, *Threat landscape for cybersecurity 2020*. Available from: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020. [4 April 2024]. Ganguly, A, R, Bhatia, U, Flynn, S, E 2018, *Critical infrastructures resilience: Policy and engineering principles,* Routledge, New York. Hurst, W & Shone, N 2024, Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation, Title of host publication Management and Engineering of Critical Infrastructures, Academic Press, Cambridge, pp. 265-286. Institute for Security Governance, Naval Support Activity Monterey 2018, *Comprehensive approach to countering hybrid threats,* Available from: https://instituteforsecuritygovernance.org/documents/113018911/119118404/P319283_EM%26R_C

omprehensive+Approaches+to+Counter+Hybrid+Threats.pdf/d8c4e29b-6a28-95b1-f3fc-333c438c88e2?t=1617292238514. [22 April 2024].

Lerner, J S, Li, Y, Valdesolo, P & Kassam, K S 2015, 'Emotion and decision making', Annual Review of Psychology, vol. 66, pp. 79-823. Available from: Emotion and Decision Making | Annual Reviews. [28 April 2024].

Matlary, J H 2015, *Resilience as a strategic concept*, Routledge, London.

Nelson, A, Rekhi, S, Souppaya, M & Scarfone, K 2024, *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 Community Profile*, NIST Special Publication 800-61 Revision 3 2024. Available from: https://csrc.nist.gov/pubs/sp/800/61/r3/ipd. [28 April 2024].

Recommended readings

Akbar, K A, Halim, S M, Hu, Y, Singhal, A, Khan, L, & Thuraisingham, B 2022, *Knowledge mining in cybersecurity: From attack to defense*, IFIP Annual Conference on Data and Applications Security and Privacy, Cham: Springer International Publishing, Switzerland , pp. 110-122.

Anderson, R & Moore, T 2006, 'The economics of information security', *Science*, vol 314, Issue 5799, pp. 610-613.

Brown, A R 2018, 'Leveraging Artificial Intelligence for Proactive Defense Against Hybrid Threats', *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 4, pp. 567-584.

Choo, K R 2011, 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, vol. 30, no. 8, pp. 719-731.

Garcia, P, Darroch, F, West, L & Brooks-Cleator, L 2020, *Ethical applications of big data-driven AI on social systems: Literature analysis and example deployment use case.* Information, 11(5), 235.

Hoffman, F G 2007*, Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies, Arlington, Virginia. Available from: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. [4 April 2024].

Johnson, J T 2017, *Roadmap for photovoltaic cyber security*, Sandia National Lab, Albuquerque, New Mexico.

Jones, S & Rid, T 2019, 'The cyber-terror trap: How governments respond to mass media scare stories', *International Affairs*, vol. 95, no. 2, pp. 245-266.

Kahneman, D 2011, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York.

Kanamaru, H, Fujita, J & Arai, T 2023, *A Study on the Classification of OT Security Risk Mitigation Measures*, 62nd Annual Conference of the Society of Instrument and Control Engineers (SICE), Tsu, Japan, pp. 274-279.

Keplin, J 2023, '*Building state resilience against hybrid activities*', *Przegląd Bezpieczeństwa Wewnętrznego*, pp. 241-266.

Kjærgaard, K, Karen, K, & Petersen, L 2017, 'Public–private partnerships on cyber security: a practice of loyalty', *International Affairs*, vol. 93, no. 6, pp. 1435–1452. Available from: https://doi.org/10.1093/ia/iix189. [4 April 2024].

Ponemon Institute 2019, *Cost of a Data Breach Report*, Available from: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258, [4 April 2024].

Rossow, C, Dietrich, C J, Davi, L & van der Walt, C 2017, *Sandnet: Network traffic analysis of malicious software*, In Proceedings of the 2017, Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM), Conference on Computer and Communications Security, pp. 1807-1824.

Smith, J 2019, 'The role of intelligence in proactive defense against hybrid threats', *Journal of Strategic Security*, vol. 12, no. 3, pp. 45-62.

Stohl, M 2019, *The Politics of Cybersecurity: How states and security experts understand, perform and discuss security in the digital age*, Routledge, Oxfordshire.

Sunstein, C R 2018, *#Republic: Divided democracy in the age of social media*, Princeton. Available from: https://doi.org/10.1515/9781400890521. [11 April 2024].

Weimann, G 2015, *Terrorism in cyberspace: the next generation*, Woodrow Wilson Center Press. Available from: https://cris.haifa.ac.il/en/publications/terrorism-in-cyberspace-the-next-generation. [11 April 2024].

Session 4. Cybersecurity and cyber incidents management
Session aim: The session aims to raise students' awareness of cybersecurity risks, business continuity challenges, and potential infringements on fundamental rights.
Session duration: 24 independent learning hours (18 hours before the contact week, 6 hours after the contact week) and 4 contact learning hours
Learning environment(s) and requirements eLearning environment
Learner resources PCs and/or mobile devices with the latest versions of browsers
Session topics/Indicative content 1. Cybersecurity, cyberattacks, mitigation of risks, and cyber incident management including the recovery of essential systems 2. Role of information systems and their security management in crises 3. Role of intelligence in countering and detecting cybercrimes. The infringement of the fundamental rights
Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

After the contact learning phase, the student will have one week to prepare for an online test with open-ended questions. In the online test, the student will demonstrate content knowledge of Session 1, Session 2 and Session 4. The feedback about the test will be provided in Moodle.

Essential reading

Anderson, R & Moore, T 2009, 'Information security: Where computer science, economics, and psychology meet', *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, vol. 367, no. 1898, pp. 2717-2727.

Cichonski, P, Millar, T, Grance, T & Scarfone, K 2016, *Computer security incident handling guide*, National Institute of Standards and Technology, Special Publication 800-61, Revision 2. Available from: Computer Security Incident Handling Guide (nist.gov). [02 April 2024].

Christou, G 2016, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, London.

Libicki, M C, Ablon, L & Webb, T 2015, *The defenders dilemma: Charting a course toward cyber security*, RAND Corporation, Santa Monica.

National Intelligence Council 2012, Global trends 2030: *Alternative worlds. National Intelligence Council*. Available from: Global trends 2030: alternative worlds - Atlantic Council. [2 April 2024].

Taddeo, M & Floridi, L 2021, *The Debate on the Moral Responsibilities of Online Service Providers, Centre of Digital Ethics*. Available from: The Debate on the Moral Responsibilities of Online Service Providers by Mariarosaria Taddeo, Luciano Floridi :: SSRN. [2 April 2024].

United Nations System 2013, *United Nations plan of pction on disaster risk reduction for resilience*, New York, USA. Available from: https://www.preventionweb.net/files/33703_actionplanweb14.06cs1.pdf. [23 April 2024].

Universal Declaration of Human Rights, Article 19. Available from: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf. [4 April 2024].

Recommended readings

Anderson, R & Moore, T 2006, 'The Economics of Information Security', *Science*, *314*(5799), pp. 610–613. Available from: http://www.jstor.org/stable/20031627. [22 April 2024].

Birnhack, M 2012, *Reverse engineering informational privacy law*. Volume 15, Yale Journal of Law & Technology, 24. Yale University, New Haven.

Bodeau, D & Dawkins, C 2014, 'The public-private partnership for cybersecurity: Aligning expectations and driving success', *Journal of Cybersecurity*, vol. 3, issue 2, pp. 175-198.

Brenner, SW 2009, *Cyber Threats: The Emerging Fault Lines of the Nation State*, New York, online edn, Oxford Academic. Available from: https://doi.org/10.1093/acprof:oso/9780195385014.001.0001, [4 April 2024].

Choo, KKR 2011, 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, vol. 30, no. 8, pp. 719-731.

Comfort, L K, Kilkon, K & Zagorecki, A 2001, 'Coordination in rapidly evolving disaster response systems: The role of information', *American Behavioral Scientist*, vol. 44, no. 7, pp. 1032-1045.

Comfort, L K, Kilkon, K & Zagorecki, A 2001, 'Coordination in rapidly evolving disaster response systems: The role of information', *American Behavioral Scientist*, vol. 44, no. 7, pp. 1032-1045.

Curtis, A 2018, *Freedom of information in the digital age*, Routledge, London.

Deibert, R 2013, *Black Code: Inside the Battle for Cyberspace*, McClelland & Stewart, Toronto.

Deibert, R 2019, *Reset: Reclaiming the internet for civil society*, House of Anansi Press, Toronto.

Floridi, L, Cowls, J, Beltrametti, M, Chatila, R, Chazerand, P, Dignum,V, Luetge, C, Madelin, R, Pagallo, U, Rossi, F, Schafer, B, Valcke, P & Vayena, E 2018, 'AI4 People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations ', *Minds & Machines,* vol. 28, pp. 689–707. Available from: https://doi.org/10.1007/s11023-018-9482-5. [22 April 2024].

Greenwald, G 2014, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, New York.

Herath, TC, & Rao, HR 2009, *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness*, Decision Support Syst., 47, pp. 154-165.

Kirwan, G & Power, A 2013, *Cybercrime: The psychology of online offenders*, Cambridge University Press.

Kushner, D 2013, *The Real Story of Stuxnet - IEEE Spectrum*, Available from: https://spectrum.ieee.org/the-real-story-of-stuxnet. [22 April 2024].

Radsan, A J & Murphy, J D 2008, 'Intelligence legalism and the National Security Agency's civil liberties gap', *Stanford Law Review*, vol. 60, no. 3, pp. 549-598.

Simchi-Levi, D, Kaminsky, P, & Simchi-Levi, E 2014*, Designing and managing the supply chain: Concepts, strategies, and case studie*s, McGraw-Hill Education. Available from: (PDF) Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies, David Simchi-Levi Philip Kaminsky Edith Simchi-Levi (researchgate.net). [2 April 2024].

Singer, PW & Friedman, A 2015, *Cybersecurity and cyberwar: What everyone needs to know*, Oxford University Press. Avaliable from: https://whateveryoneneedstoknow.com/display/10.1093/wentk/9780199918096.001.0001/isbn-9780199918096. [23 April 2024].

Solove, D J 2008, *Understanding privacy*, Harvard University Press, United states of America.

Van der Sloot, B 2020, 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 11, 160.

Whitman, M E, & Mattord, H J 2018, *Management of information security* (6th ed.), Cengage Learning, Cheriton House, North Way, Andover, Hampshire

Session 5. International cooperation

Session aim: The session aims to create opportunities for students to develop skills to analyse the importance of international cooperation for the prevention of hybrid threats

Session duration: 114 independent learning hours (18 hours before and 96 hours after the contact week) and 4 contact learning hours

Learning environment(s) and requirements

eLearning environment

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Cooperation in the prevention and countering of hybrid threats
2. International cooperation in detecting and prosecuting perpetrators of hybrid attacks
3. Countering hybrid threats with international partners and organizations (European Union, EUROPOL, INTERPOL, NATO, Frontex)

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the independent learning phase, the student will compile a draft outline of the written analysis, that includes tools and means of cooperation to analyse, and a preliminary list of references reviewed. The written analysis will be completed after contact week and should be submitted 5 days before the end of Module 2.

In the contact week, which will take place in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

Bertolini, M., Minicozzi, R., Sweijs, T. 2023, *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies, pp. 10-13, 17-18. Available from: https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/. [17 January 2025].

Billing, F., Feldtmann, B. 2024, *The Role of Criminal Law Approaches Against Hybrid Attacks*, Bergen Journal of Criminal Law and Criminal Justice, Volume 12, Issue 2, pp. 2-3, 6, 18-19, 21-22, 24. Available from: https://boap.uib.no/index.php/BJCLCJ/article/view/4440. [23 January 2025].

Bratko, A., Zaharchuk, D., Zolka, V. 2021, *Hybrid warfare – a threat to the national security of the state*. Revista de Estudios en Seguridad Internacional, Vol. 7, No. 1, pp. 151, 152, 158. Available from: http://dx.doi.org/10.18847/1.13.10. [12 December 2024].

Brown, C. S. D. 2015, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, International Journal of Cyber Criminology, Vol 9 Issue 1 January – June, pp. 65-66, 86, 97. Available from: https://zenodo.org/records/22387. [20 January 2025].

Convention on Cybercrime Budapest, 23.XI.2001. Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention. [23 January 2025].

Council of the European Union 2022, *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security. Available from: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.* [14 January 2024].

European Commission 2018, *Joint communication to the European Parliament and the Council, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018JC0016. [14 January 2024].

European Commission 2016, *Joint Framework on countering hybrid threats - a European Union response.* JOIN/2016/018 final. Document 52016JC0018, p. 2. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [12 December 2024].

European Commission 2020, *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN (2020) 18 final, p. 4. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [6 December 2024].

Gaiser, L. 2019, *Nato - EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework*. National Security and the Future, 20(1-2), pp. 17-18, 20. Available from: https://hrcak.srce.hr/231815. [13 December 2024].

Khmyrov, I., Khriapynskyi, A., Aliieva, P., Kopotun, I., Svoboda, I. 2024, *International experience of advanced countries in state management of countering hybrid threats*. № 36. Universidade

Portucalense, Porto, pp. 373-377. Available from: https://revistas.rcaap.pt/juridica/article/view/36758. [12 December 2024].

Laitinen, M., Armstrong-Smith, S. 2022, *Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations*. Cyber Security: A Peer-Reviewed Journal Vol. 5, 3, pp. 190, 196-197, 202-203. Available from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.henrystewartpublications.com/sites/default/files/CSJ5.3Tackling%20cybercrime%20and%20ransomware%20headonDisrupting%20criminal%20networks%20and%20protecting%20organisations.pdf. [20 January 2025].

Oancea, R., Gligorea, I., Raţiu, A., Dragomir, I. 2024, *Cybersecurity*, in: *Hybrid Warfare Reference Curriculum*, Volume I, Compulsory Lectures, Edited by Zoltán Jobbágy – Edina Zsigmond, Ludovika University Press, Budapest, 2024, pp. 149-150. Available from: https://csnsc.uk/hybrid-warfare-reference-curriculum-volume-i/. [6 December 2024].

Olech, A. K. 2021, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*. Instytut Nowej Europy, pp. 2-3, 7. Available from: https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/. [12 December 2024].

Wigell, M., Mikkola, H., Juntunen, T. 2021, *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union PE 653.632. May 2021, pp. 1, 4. Available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf. [12 December 2024].

Recommended readings

Bachmann, S.-D., Gunneriusson, H. 2015, *Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security*. Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, p. 87. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506063. [12 December 2024].

Bachmann, S. D., Gunneriusson, H. 2014, *Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security*. The Journal on Terrorism and Security Analysis, p. 33. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2252595. [23 January 2025].

Bajarūnas, E. 2020, *Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond*. European View, 19(1), pp. 63. Available from: https://doi.org/10.1177/1781685820912041. [12 December 2024].

Bajarūnas, E., Keršanskas, V. 2018, *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome*. Lithuanian Annual Strategic Review, 16(1), p. 159. Available from: https://journals.lka.lt/journal/lasr/article/152/info. [12 December 2024].

Balcaen, P., Du Bois, C., Buts, C. 2021, *Sharing the Burden of Hybrid Threats: Lessons from the Economics of Alliances*, Defence and Peace Economics, DOI: 10.1080/10242694.2021.1991128, p. 4. Available from: https://doi.org/10.1080/10242694.2021.1991128. [18 December 2024].

Bendiek, A. 2018, *The EU as a Force for Peace in International Cyber Diplomacy*. Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs, p. 1. Available from: https://www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy. [20 January 2025].

Bertolini, M., Minicozzi, R., Sweijs, T. 2023, *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies, pp. 7, 12. Available from: https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/. [6 December 2024].

Bhardwaja, A., Mangata, V., Viga, R., Halderb, S., Contib, M. 2021, *Distributed Denial of Service Attacks in Cloud: State-of-the-Art of Scientific and Commercial Solutions*. Computer Science Review, p. 24. Available from: https://www.researchgate.net/publication/348097190_Distributed_denial_of_service_attacks_in_cloud_State-of-the-art_of_scientific_and_commercial_solutions?enrichId=rgreq-857443269456ff0c47ac7fc329282664-XXX&enrichSource=Y292ZXJQYWdlOzM0ODA5NzE5MDtBUzoxMTI2NTU4OTcwNDYyMjA4QDE2NDU2MDM5OTcwMDY%3D&el=1_x_2. [20 January 2025].

Cîrdei, I. A., Ispas, L. 2017, *A Possible Answer of the European Union to Hybrid Threats*. Scientific Bulletin, De Gruyter Open, Vol. 22 (Issue 2), p. 73. Available from: https://doi.org/10.1515/bsaft-2017-0009. [12 December 2024].

Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007R0168. [20 January 2024].

Danyk, Y., Maliarchuk, T., Briggs, C. 2017, *Hybrid War: High-tech, Information and Cyber Conflicts*, Connections QJ 16, no. 2, pp. 15-16. Available from: https://doi.org/10.11610/Connections.16.2.01. [20 January 2025].

European Commission 2016, *Joint Framework on countering hybrid threats - a European Union response*. JOIN/2016/018 final. Document 52016JC0018, p. 13. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [17 January 2025].

European Commission 2020, *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN (2020) 18 final, p. 15. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [17 January 2025].

Filipec, O. 2021, *Preventing Hybrid Threats: From Identification to an Effective Response*. European Studies. 8, p. 19. Available from: https://www.researchgate.net/publication/354034499_Preventing_Hybrid_Threats_From_Identification_to_an_Effective_Response. [18 December 2024].

Ivanov, I., Shalamanov, V. 2020, *NATO and Partner countries cooperation in countering asymmetric and hybrid threats in South Eastern Europe's cyberspace*. NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Volume 149: Toward Effective Cyber Defense in Accordance with the Rules of Law, p. 11. Available from: https://www.researchgate.net/publication/351702431_NATO_and_Partner_countries_cooperation_in_countering_asymmetric_and_hybrid_threats_in_South_Eastern_Europe's_cyberspace. [17 January 2025].

Microsoft 2022, *Digital Crimes Unit: Leading the fight against cybercrime*. Available from: https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/. [20 January 2025].

Microsoft Digital Defense Report 2024 - The foundations and new frontiers of cybersecurity, p. 95. Available from: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024. [20 January 2025].

Monaghan, S. 2019, *Countering Hybrid Warfare: So What for the Future Joint Force?* PRISM, 8(2), p. 90. Available from: https://www.jstor.org/stable/26803232. [17 January 2025].

Ratsyborinska, V. 2022, *EU-NATO and the Eastern Partnership Countries Against Hybrid Threats (2016-2021)*. National Security and the Future, 23(2), pp. 89-90. Available from: https://doi.org/10.37458/nstf.23.2.3. [12 December 2024].

Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction (recast). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006R1920. [20 January 2024].

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R2219. [20 January 2024].

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA - 32016R0794. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0794. [16 January 2024].

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1726. [18 January 2024].

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing

Council Decision 2002/187/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1727. [18 January 2024].

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1896. [17 January 2024].

Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010. Available from: https://eur-lex.europa.eu/eli/reg/2021/2303/oj. [20 January 2024].

Sari, A. 2018, *Blurred Lines: Hybrid Threats and the Politics of International Law - Strategic Analysis January 2018*. Hybrid CoE, p. 8. Available from: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-4-blurred-lines-hybrid-threats-and-the-politics-of-international-law/. [12 December 2024].

Simons, G., Danyk, Y., Maliarchuk, T. 2020, *Hybrid war and cyber-attacks: creating legal and operational dilemmas*, Global Change, Peace & Security, pp. 4, 6. Available from: https://doi.org/10.1080/14781158.2020.1732899. [20 January 2025].

Skopik, F., Pahi, T. 2020, *Under false flag: using technical artifacts for cyber attack attribution*. Cybersecurity, 3:8, pp. 1, 4. Available from: https://doi.org/10.1186/s42400-020-00048-4. [20 January 2025].

Swaminathan, A., Ramakrishnan, B., Kanishka, M., Surendran, R. 2022, *Prediction of Cyber-attacks and Criminality Using Machine Learning Algorithms*, 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, pp. 1, 8. Available from: https://www.researchgate.net/publication/366704973_Prediction_of_Cyber-attacks_and_Criminality_Using_Machine_Learning_Algorithms?enrichId=rgreq-8e82f656e93d9f2843abf2ddff2e0fbd-XXX&enrichSource=Y292ZXJQYWdlOzM2NjcwNDk3MztBUzoxMTQzMTI4MTIyNDI5NzMyNkAxNzA4MTY4OTk1NDEz&el=1_x_2. [20 January 2025].

Taneski, N., Kirkova, R. 2018, *The Concept of Hybrid Threats*, International Journal, Scientific Papers, pp. 1795. Available from: https://eprints.ugd.edu.mk/22011/ [19 December 2024].

Tudorache, P., Bârsan, G. 2024, *Strategies to Counter Hybrid Threats*, in: *Hybrid Warfare Reference Curriculum*, Volume I, Compulsory Lectures, Edited by Zoltán Jobbágy – Edina Zsigmond, Ludovika University Press, Budapest, 2024, pp. 160, 162. Available from: https://csnsc.uk/hybrid-warfare-reference-curriculum-volume-i/. [6 December 2024].

Veena, K., Meena, K., Teekaraman, Y., Kuppusamy, R., Radhakrishnan, A. 2022, *C SVM Classification and KNN Techniques for Cyber Crime Detection*. Wireless Communications and Mobile Computing, Wiley, Volume 2022, pp. 7-8. Available from: https://doi.org/10.1155/2022/3640017. [20 January 2025].

8.2.5 Delivery Timetable for Module 2

Module 2	November 3 - December 19, 2025
Phase	**Dates**
Independent learning phase - Reading mandatory literature and studying e-learning materials	**November 4 - 21, 2025**
Contact learning phase (online) **Assessment:** - Solving the case study about identifying problems, recommending and elaborating methods of social protection against hybrid threats.	**November 24 - 28, 2025**
Preparation of assessment tasks: - **Online test** about content of Session 1, Session 2 and Session 4. - **Written analysis** of the importance of prevention and countering hybrid threats using relevant tools and means of cooperation	**December 1 - 15, 2025** - December 8, 2025 - online test - December 15, 2025 - deadline for submitting the written analysis
Reassessments	January 16, 2026 - deadline for liquidation of student debts

8.3 Module 3. Increasing resilience and bolstering societal and institutional capabilities to hybrid threats

Pre-requisite Modules:	Module 1		ECTS Credits 8
Contact learning hours	**Independent learning hours**	**Experiential learning**	**Total**
49	76	84	208

8.3.1 Module Aim and Module Learning Outcomes

This module aims to create opportunities for students to develop skills to elaborate methods of social resilience and protection against hybrid threats.

Upon completion of this module, the student will be able to:

- explain tools for fostering resilience of the state and non-state actors to hybrid threats;
- explain the role of protection of fundamental rights in preparation for responding to hybrid threats, including in cooperation with civil-military and other stakeholders;
- selectively identify and present good practices related to the protection of critical infrastructure and strategic objects.

8.3.2 Module Learning Strategy

Module 3 deals with methods of social resilience and protection against hybrid threats.

The module consists of 3 phases:

- **Independent learning phase**. Independent learning lasts for 2 weeks (80 hours). During this time, the student should lay the groundwork for contact learning for the module by getting acquainted with relevant literature, going through eLearning tools and completing self-assessment tasks. The self-assessment tasks will serve as a prerequisite for participating in the contact week. Also, in completing the assessment assignment (written analysis) students should be able to discuss and apply knowledge and methods covered in the learning materials. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

  During the independent learning phase, the student will compile a draft outline of the written analysis, that includes critical infrastructure and strategic objects to analyse, and a preliminary list of references reviewed.

- **Contact learning phase**. The contact learning phase lasts for 21 hours in the online environment. During this phase, students participate in lectures, which will cover key theoretical and

methodological aspects of the module, and seminars applying and reflecting on the topics of the module.

After the contact phase, the student will perform the online test about tools for fostering resilience of the state and non-state actors to hybrid threats and the role of protection of fundamental rights in preparation for responding to hybrid threats.

- **Experiential learning phase**. The experiential learning will take place in the students' work environments. The experiential learning phase lasts for 103 hours and will be devoted to identifying and presenting good practices related to the protection of critical infrastructure and strategic objects. Students will analyse their own workplaces as critical infrastructure or strategic objects and study various practices related to their protection. If a student's workplace cannot be considered a critical infrastructure or strategic object, the student can analyse simulated critical infrastructure and/or strategic objects provided by the lecturer (e.g., national crisis reserves, national databases, energy supplies, transport). At the end of the phase, students will prepare the written analysis, which should be submitted 5 days before the end of Module 3.

Sessions of Module 3:

- Session 1. Common resilience-building approach against hybrid threats
- Session 2. Fostering the resilience of the state and non-state actors to hybrid threats
- Session 3. Protection of critical infrastructure

8.3.3 Module assessment strategy

There are two assessment assignments for the module:

- online test with open-ended questions;
- written analysis of identifying and presenting good practices related to the protection of critical infrastructure and strategic objects.

Online test with open-ended questions. The student must answer the questions within the allotted time. Students are allowed to use all study materials and necessary sources while answering. The test is assessed non-distinctively, and to pass, the student must answer each question correctly. In case of failing, the student will have the opportunity for reassessment, under the same conditions as the assessment in terms of testing environment and allotted time. The student has approximately two weeks for reassessment.

The written analysis of identifying and presenting good practices related to the protection of critical infrastructure and strategic objects**.** The student will analyse their place of work as a critical infrastructure or strategic object. The topic will be previously agreed upon with the lecturer. In case the student's own workplace cannot be considered a critical infrastructure or strategic object, the student can analyse a simulated critical infrastructure and/or strategic object provided by the lecturer (e.g., national crisis reserves, national databases, energy supplies, transport). The writing process will be supported by the lecturer, if necessary. The analysis is assessed non-distinctively and to pass the student must meet all the

assessment criteria. The lecturer gives feedback about meeting assessment criteria in written or/and oral form. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the analysis. The student has approximately two weeks to eliminate the deficiencies.

For information on the assessment criteria see in the **ANNEX 1 Assessments**.

8.3.4 Module 3 Sessions

Session 1. Common resilience-building approach against hybrid threats
Session aim: The session aims to create opportunities for students to develop knowledge in resilience-building against hybrid threats
Session duration: 26 independent learning hours (24 hours before and 2 hours after the contact week) and 6 contact learning hours
Learning environment(s) and requirements eLearning environment
Learner resources PCs and/or mobile devices with the latest versions of browsers
Session topics 1. Awareness of the existence of hybrid challenges 2. Identification of gaps in preparedness for and response to hybrid threats. Role of fundamental rights in preparation for responding to hybrid threats 3. Introduction of anti-propaganda initiatives in the region 4. Managing the outbreak of information disorder 5. Implications for security policy and strengthening the resistance of the society to hybrid threats
Learning activities During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums. Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read all the reading list and go through all eLearning tools. After that, students must complete self-assessment tasks. During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars. After the contact learning phase, the student will take an online test with open-ended questions. In the online test, the student will demonstrate content knowledge of Session 1 and Session 2. The feedback about the test will be provided in Moodle.
Essential reading

Council of Europe, 2023, *REYKJAVÍK DECLARATION - United around our values*. p.p. 7, 10, 15. Available from: https://rm.coe.int/4th-summit-of-heads-of-state-and-government-of-the-council-of-europe/1680ab40c1. [12 December 2024].

Council of the European Union, 2022, How the EU responds to crises and builds resilience, Available from: https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/, [03 December 2024].

European Commission, 2018a, *Communication from the commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions*. *Tackling online disinformation: a European Approach. p.p. 3-16.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236. [15 December 2024].

European Commission, 2018b, *Joint communication to the European Parliament, the European council, the council, the European economic and Social committee and the committee of the regions. Action Plan against Disinformation*. p.p. 1-12. Available from: https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf. [15 December 2024].

European Commission, Directorate-General for Communications Networks, Content and Technology 2018, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office of the European Union. Available from: https://data.europa.eu/doi/10.2759/739290. [12 July 2024].

European Commission, 2016, *Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response,* JOIN/2016/018 final. p. 3-17. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [15 December 2024].

European Parliament, 2022, *Foreign interference in all democratic processes in the European Union. European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)*. p.p. 13. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022IP0064. [12 December 2024].

European Parliament, 2021, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf, [27 December 2024].

Fiott, D. and Parkes, R., 2019, *Protecting Europe: The EU's Response to Hybrid Threats*. EU Institute for Security Studies.

Giannopoulos, G., Smith, H., Theocharidou, M. 2021, *The Landscape of Hybrid Threats: A conceptual model*, EUR 30585 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. p.p. 11. Available from: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf. [10 December 2024].

Hybrid CoE, *Frequently asked questions on hybrid threats*. p.p. 1-2. Available from: https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf. [12 December 2024].

OSCE, UN, OAS, ACHPR, 2017, *Joint declaration on freedom of expression and "fake news", disinformation and propaganda*. p.p. 1-5. Available from: https://www.osce.org/files/f/documents/6/8/302796.pdf. [12 December 2024].

Smith, B. Lannes, 2024, *"Propaganda"*, Encyclopedia Britannica. Available from: https://www.britannica.com/topic/propaganda [10 December 2024].

Recommended readings

Boin, A & Rhinard, M 2022, "Crisis Management Performance and the European Union: The Case of COVID-19." Journal of European Public Policy, 30 (4): pp. 655–75. doi:10.1080/13501763.2022.2141304.

Council of the European Union, 2021, *The Council adopted conclusions on resilience and crisis response - Consilium*, doc. 14276/21. Available from: https://data.consilium.europa.eu/doc/document/ST-14276-2021-INIT/en/pdf, [03 December 2024].

ECHR*,* 2022*, European Convention on Human Rights-A living instrument.* p.p. 11. Available from: https://www.echr.coe.int/documents/d/echr/Convention_Instrument_ENG. [12 December 2024].

European Commission, 2024, *Tackling disinformation and information manipulation*. p.p. 1-4. Available from: https://ec.europa.eu/commission/presscorner/api/files/attachment/878789/Tackling%20Disinformation_Factsheet_EN.pdf. [15 December 2024].

European Commission, 2020, *Communication from the commission to the European Parliament, the Council, the European economic and social Committee and the committee of the regions. On the European democracy action plan*, COM/2020/790 final. p.p. 19-27. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:790:FIN. [12 December 2024].

European Parliament, 2021, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf, [27 December 2024].

European Parliament, 2019, *Online disinformation and the EU's response.* p. 1-2. Available from: https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf. [12. December 2024].

Grbeša Zenzerović, M., Nenadić, I., 2022, *Jačanje otpornosti društva na dezinformacije: analiza stanja i smjernice za djelovanje – studija*. Zagreb: Agencija za elektroničke medije. Available from: *https://www.aem.hr/wp-content/uploads/2022/09/Studija_dezinformacije_2-izdanje.pdf*. [12 December 2024].

Helbing, D 2013, Globally networked risks and how to respond. Nature, 497 (7447), pp.51-59. Available from: https://www.nature.com/articles/nature12047. [12 July 2024].

Hrvatska enciklopedija, mrežno izdanje. *"Promidžba"*, Leksikografski zavod Miroslav Krleža, 2013. – 2024. Available from: https://enciklopedija.hr/clanak/promidzba. [16 December 2024).

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., 2023, *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg, doi:10.2760/37899, JRC129019. p.p. 8-21. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. [12 December 2024].

Larsson, O., 2013, Sovereign power beyond the state: a critical reappraisal of governance by networks. *Critical Policy Studies*, 7(2), pp.99-114.

NATO, 2024, *NATO's aproach to counter information threats - Public summary.* Available from: https://www.nato.int/cps/en/natohq/official_texts_231905.htm. [18 October 2024].

Nye, JS 2010, Cyber Power, Harvard Kennedy School. Available from: https://www.researchgate.net/publication/236602842_Globally_networked_risks_and_how_to_respond. [12 July 2024].

Van der Meer, T G L A & Jin, Y 2020, Seeking formula for misinformation treatment in public health crises: The effects of corrective information type and source, Health Communication, 35(5), pp.560-575. Available from: https://pubmed.ncbi.nlm.nih.gov/30761917/. [12 July 2024].

Wardle, C & Derakhshan, H 2017, Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. Available from: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policymaking.html. [12 July 2024].

Session 2. Fostering the resilience of the state and non-state actors to hybrid threats

Session aim: The session aims to create opportunities for students to develop knowledge about forms and methods of cooperation in tackling hybrid threats

Session duration: 26 independent learning hours (24 hours before and 2 hours after the contact week) and 6 contact learning hours

Learning environment(s) and requirements

eLearning environment

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. European Union's concept of resilience and the inclusion of capabilities to prevent, withstand and recover from a hybrid attack
2. Cooperation with corporate and strategic infrastructure sectors
3. Cooperation with civil society stakeholders
4. Civil-military cooperation during hybrid attacks
5. Awareness of the protection of fundamental rights in the context of cooperation

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read all the reading list and go through all eLearning tools. After that, students must complete self-assessment tasks.

During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

After the contact learning phase, the student will take an online test with open-ended questions. In the online test the student will demonstrate content knowledge of Session 1 and Session 2. The feedback about the test will be provided in Moodle.

Essential reading

Cusumano, E & Corbe, M 2017, *A Civil-Military Response to Hybrid Threats*. Available from: https://link.springer.com/book/10.1007/978-3-319-60798-6. [15 December 2024].

Directive (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). pp. 64-70. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555. [15 December 2024].

Directive (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. pp. 171-176,

182-187. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557. [15 December 2024].

ENISA, 2017, *Public Private Partnerships (PPP), Cooperative models.* pp. 7, 11-14. Available from: https://op.europa.eu/hr/publication-detail/-/publication/597dee0f-2285-11e8-ac73-01aa75ed71a1. [20 December 2024].

EUCPN 2019, Policy on Community-oriented policing in the EU. Brussels. Avalabe at: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://eucpn.org/sites/default/files/document/files/POLICY%20PAPER%202019%20COP_ENG_LR.pdf. [December 30 2024].

European Commission, 2020, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS* on the EU Security Union Strategy, pp. 6-7. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605, [15 December 2024].

European Commission, 2023, Proposal for a COUNCIL RECOMMENDATION on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance, COM/2023/526 final. pp. 8-9,11-15. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023DC0526. [15 December 2024].

European Parliament, 2023, *SECURITY IMPLICATIONS OF CHINA-OWNED CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION*, pp. 8, 15-19. Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf. [12 December 2024].

Hufnagel, S., 2015, Transnational Policing and Regulation: The Effect of Shared Fundamental Rights on the Formalisation of Cross-Border Police Cooperation. *EJPS*, p.204.

Hybrid CoE, *Frequently asked questions on hybrid threats*. pp. 1-2. Available from: https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf. [12 December 2024].

Juntunen, T., Wigell, M. & Mikkola, H., 2021, Best Practices in the whole-of-society approach in countering hybrid threats. Available at: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632. [December 30 2024].

Linkov, I. and Trump, B., 2019, *The Science and Practice of Resilience*. New York: Springer International.

Niinistö, S 2024, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness Report*. Available from: https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf. [2 December 2024].

OECD 2019, *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris., pp. 14-17, 50-56. Available from: *https://doi.org/10.1787/02f0e5a0-en*. [20 December 2024].

Sanz-Caballero, S., 2023, The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanit Soc Sci Commun 10, 360. Available at: https://doi.org/10.1057/s41599-023-01864-y. [December 30 2024].

Sučić, I. & Karlović, R., 2017, Community policing in support of social cohesion Community. In: Bayerl et.al. Policing - A European Perspective: Strategies, Best Practices and Guidelines. Cham: Springer. 7-20.

Recommended readings

Bauman, Z., 2000, Liquid Modernity. Cambridge: Polity Press.

Di Gregorio, A., 2022, Rule of law crisis and the constitutional 'awareness' of the EU. In *Rule of Law in Crisis* (pp. 152-173). Routledge.

Dunay, P & Roloff, R 2017, *Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank*, Available from: https://www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0. [2 December 2024].

Giddens, A. & Sutton, P. W., 2017, Sociology (8th ed.). Oxford: Polity Press.

Hybrid CoE, 2024, *Hybrid CoE key themes for 2024.* Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/12/Hybrid-CoE-key-themes-for-2024.pdf. pp. 1-4. [15 December 2024].

Joseph, J., 2018, *Varieties of Resilience: Studies in Governmentality*, Cambridge: Cambridge University Press.

Kellerbauer, M., Klamert, M. and Tomkin, J., 2024, *The EU Treaties and Charter of Fundamental Rights: a Commentary*. Oxford University Press.

Mitchell, T., and Harris, K., 2012, *Resilience: A Risk Management Approach*. London: Overseas Development Institute.

Niinistö, S 2024, Outsmart malicious actors to deter hybrid attacks. Available from: https://commission.europa.eu/document/download/934d5577-2d06-4cef-8aa3-8edd2556dd59_en?filename=2024_Niniisto-factsheet_6.pdf. [2 December 2024].

OECD (2023)., *REPORT ON THE IMPLEMENTATION OF THE OECD RECOMMENDATION ON THE GOVERNANCE OF CRITICAL* RISK. p. 27 https://one.oecd.org/document/C(2023)163/en/pdf. [20 December 2024].

Rathnayaka, B., Siriwardana, C., Robert, D., Amara, 2022, *Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review*. International Journal of

Disaster Risk Reduction, 2022, pp. 103-123. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2212420922003429?via%3Dihub. [20 December 2024].

Rouet, G. and Pascariu, G., 2019, *Resilience and the EU's Eastern Neighbourhood Countries.*

Tikanmäki, I. & Ruoslahti, H., 2022, How are Hybrid Terms Discussed in the Recent Scholarly Literature?. In: European Conference on Cyber Warfare and Security. Available from: https://www.researchgate.net/publication/361218645_How_are_Hybrid_Terms_Discussed_in_the_Recent_Scholarly_Literature. [December 30 2024].

Tridimas, G. and Tridimas, T., 2017, Public awareness of EU rights and the functions of the European Ombudsman: some unpleasant findings. In *Accountability in the EU* (pp. 74-93). Edward Elgar Publishing.

Wigell, M, Mikkola, H & Juntuen T 2021, *Best Practices in the whole-of-society approach in countering hybrid threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf. [2 December 2024].

Session 3. Protection of critical infrastructure

Session aim: The session aims to create opportunities for students to develop skills to identify and analyse good practices related to the protection of critical infrastructure and strategic objects

Session duration: 32 independent learning hours, 9 contact learning hours, 103 hours of experiential learning

Learning environment(s) and requirements

eLearning environment

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Threats and *modus operandi* for affecting critical infrastructure and strategic objects of the state
2. Supporting the resilience of the European Union and neighbours' critical infrastructure

Learning activities

During independent learning hours, the students will work at home using the Moodle course and will be assisted by the module lecturers. Students will be able to contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read all the reading list and go through all eLearning tools.

During the independent learning phase, the student will compile a draft outline of the written analysis, that includes critical infrastructure and/or strategic objects to analyse, and a preliminary list of references reviewed. The written analysis will be completed at the end of the experiential learning phase.

During the contact week in the online environment, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

The experiential learning will take place in the students' work environments. The experiential learning phase lasts for 79 hours and will be devoted to identifying and presenting good practices related to the protection of critical infrastructure and strategic objects. Students will analyse their own workplaces as critical infrastructure or strategic objects and study various practices related to their protection. If a student's workplace cannot be considered a critical infrastructure or strategic object, the student can analyse simulated critical infrastructure and/or strategic objects provided by the lecturer (e.g., national crisis reserves, national databases, energy supplies, transport). At the end of the phase, students will prepare the written analysis, which should be submitted 5 days before the end of Module 3.

Essential reading

Council of the European Union 2022, *Council recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure – Adoption,* 15454/22. Available from: https://data.consilium.europa.eu/doc/document/ST-15454-2022-INIT/en/pdf. [4 April 2024].

European Commission 2023*, Hybrid threats. A comprehensive resilience ecosystem.* Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf?cv=1. [4 April 2024].

European Parliament and the Council of the European Union, 2022, *Directive on the resilience of critical entities and repealing Council Directive 2008/114/EC.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_51_2022_INIT&qid=1670576357609&from=EN, PE-CONS 51/22, 30.11.2022. [09 December 2022].

Liang, Q & Xiangsui, W 2020, *Unrestricted warfare: China's master plan to destroy America*, Albatross Publishers, Prague, Czech Republic.

Singer, P W & Brooking, E T 2018, *Likewar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, Massachusetts, US.

Recommended readings

Adger, W N 2000, 'Social and ecological resilience: Are they related? *Progress in Human Geography*,' vol. 24, no 3, pp.347-364. Available from: https://doi.org/10.1191/030913200701540465. [4 April 2024].

Baldwin, A, D 2020, *Economic Statecraft*, Princeton University Press, Princeton. Available from: https://press.princeton.edu/books/paperback/9780691204420/economic-statecraft. [23 April 2024].

Bascomb, N 2016, *Sabotage: The mission to destroy Hitler's atomic bomb*, Scholastic Incorporated, New York.

Britannica 2024, *Civil Rights*. Available from: https://www.britannica.com/topic/civil-rights. [8 March 2022].

Britt, T W & Oliver, K K 2013, *Morale and cohesion as contributors to resilience*, in Sinclair, RR & Britt TW (Eds.), Building psychological resilience in military personnel: Theory and practice, American Psychological Association, pp. 47-65. Available from: https://doi.org/10.1037/14190-003. [4 April 2024].

Chesley, D L & Amitrano, M 2015, 'Risk and growth, but not as we know them', *Resilience: A journal of strategy and risk*, pp. 1-6. Available from: https://www.pwc.ch/de/publications/2016/pwc_ceo_survey_resilience_e.pdf. [4 April 2024].

Council of Europe 2021, *State of democracy, human rights and the rule of law: A democratic renewal for Europe*, Secretary General of the Council of Europe. pp. 1-46. Available from: https://rm.coe.int/annual-report-sg-2021/1680a264a2. [4 April 2024].

Energy Community 2020, *Annual Implementation Report 2020*, Vienna: Energy Community Secretariat. Available from: https://www.energy-community.org/news/Energy-Community-News/2020/11/23.html. [4 April 2024].

European Commission 2019, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal*. Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN. [4 April 2024].

European External Action Service 2020, *European neighborhood policy and enlargement negotiations*. Available from: https://ec.europa.eu/neighbourhood-enlargement/, [4 April 2024].

European Investment Bank 2020, *European Investment Bank Annual Report 2020*, Luxembourg: European Investment Bank. Avaliable from: https://www.eib.org/en/publications/financial-report-2020. [4 April 2024].

European Union Agency for Cybersecurity 2018, *Capacity building in cybersecurity: A strategy for the European Union*, Publications Office of the European Union, Luxembourg.

European Western Balkans 2019, *Investing in the Western Balkans: Western Balkans Investment Framework Annual Report 2019*. Brussels: European Union.

Macaulay, T 2008, *Critical infrastructure: Understanding its component parts, vulnerabilities, operating risks, and interdependencies*, US: CRC Press Broken Sound Parkway, NW Suite 300, Boca Raton, Florida, US.

Williamson Murray, W & Mansoor, R P 2012, *Hybrid warfare: Fighting complex opponents from the ancient world to the present*, Cambridge University Press, Shaftesbury Road Cambridge, UK.

8.3.5 Delivery Timetable for Module 3

Module 3	January 5 - February 9, 2026
Phase	**Dates**
Independent learning phase: - Reading mandatory literature and studying e-learning materials	**January 5 - 16, 2026**
Contact learning phase (online) **Assessment:** Online test, about Session 1 and Session 2	**January 19 - 21, 2026** January 21, 2026 – online test
Experiential learning phase **Assessment:** **Written analysis** of identifying and presenting good practices related to the protection of critical infrastructure and strategic objects	**January 22 - February 4, 2026** February 4, 2026 – deadline for written analysis
Reassessments	March 27, 2026 - deadline for liquidation of student debts

8.4 Module 4. Management and Leadership in the Context of Hybrid Threats and Hybrid Crises

Pre-requisite Modules:	Module 1		ECTS Credits 13
Contact learning hours	**Independent learning hours**	**Experiential learning**	**Total**
54	260	24	338

8.4.1 Module Aim and Module Learning Outcomes

The module aims to create opportunities for students to develop competencies of leadership in a hybrid environment.

Upon completion of this module, the student will be able to:

- explain the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies;
- critically analyse the European Union's approach to internal and border security management;
- evaluate the role of fundamental rights in the European Union's internal and border security management;
- critically evaluate actions countering information advocacy and influence activities;
- analyse and interpret psychological aspects related to radicalisation and different forms of extremism on social media;
- propose combined approaches for management and leadership for encountering modern security challenges and threats based on modern theories, considering professional ethics, fundamental rights, and principles of equal treatment of diverse groups;
- apply strategic communication skills in a hybrid context based on ethical values and evaluate the results;
- employ appropriate tools and techniques to strategically manage civilian, human and technical resources, and make decisions in case of hybrid crises, and critically evaluate their peers' problem-solving performance.

8.4.2 Module Learning Strategy

The learning strategy of Module 4 aims to facilitate the integration of all gained knowledge and skills through case study-based learning, which provides the opportunity to peer learning and sharing of best practices in solving complex cases about hybrid crises, considering fundamental rights, professional ethics and protection of vulnerable groups.

The module consists of 3 phases:

- **Independent learning.** The independent learning phase lasts for 7 weeks (274 hours). During this time, students should prepare for the case study and tabletop exercise by getting acquainted with relevant literature, going through eLearning tools and completing self-assessment tasks. The self-assessment tasks will serve as a prerequisite for participating in the contact week.
  The tasks that students must complete are:
  - self-assessment test (a multiple-choice test) about the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies;
  - 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;
  - self-assessment test (a multiple-choice test) about modern theories and concepts of management and leadership.

- **Experiential learning phase**. The experiential learning phase will last 3 days (24 hours) and will take place at the European Union's external border. During the experiential learning phrase, students will gain experience in the European Union's approach to internal and border security management and the role of fundamental rights in this context. They will have an opportunity to visit a border crossing point at the European Union's external border, contact experts and get experience in the implementation of integrated border management. As a part of the experiential learning phase, students are required to solve a case study that addresses the appearance of hybrid threats at the European Union's external border.

- **Contact learning phase**. The contact learning phase lasts for 1 week (40 hours). During this phase, students participate in lectures, which will cover key theoretical and methodological aspects of the module, and seminars applying and reflecting on the topics of the module (22 hours). During the contact week, students will prepare and perform the tabletop exercise (18 hours).

Sessions of Module 4:

- Session 1. European Union's external dimension in countering hybrid threats
- Session 2. Border security and management
- Session 3. Countering information advocacy and influence activities
- Session 4. Management and leadership in the context of hybrid challenges

8.4.3 Module assessment strategy

There are two assessment assignments for the module.

Case study

The case study about the European Union's approach to internal and border security management and the role of fundamental rights in internal and border security management. The scenario will be presented to students after visiting the European Union's external border. The case study is performed as a group

work. The group size is up to 5 students. The information on the case will be provided in steps. The resolution of the case study will be observed and tutored by lecturers/trainers.

The case study is assessed non-distinctively and to pass the student must meet all the assessment criteria. In case of failing, the student will have the opportunity for reassessment, which consists of eliminating the deficiencies found in the case study and/or the presentation. The lecturer gives feedback about meeting assessment criteria in verbal form after the presentation.

If, based on the group members' evaluation, some of the group members did not contribute to the assignment, then the student should perform a new case study independently.

Tabletop exercise

The tabletop exercise will integrate all the knowledge and skills that students have acquired during the entire course. It will be a practical exercise about solving 4 cases of hybrid crises, which include case scenarios at national, regional and EU levels. Students are tasked to:

- assess the situation based on European Union policies and legal framework responding to hybrid threats;
- employ appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises;
- select and apply appropriate management and leadership tools and methods;
- to evaluate and propose solutions for cooperation, communication (including with third countries);
- recommend measures for prevention and countering hybrid threats;
- all solutions should consider fundamental rights, professional ethics and protection of vulnerable groups.

The tabletop exercise is conducted as group work, utilizing the facilities of the Estonian Academy of Security Sciences simulation centre. The group size is up to 5 students. The tasks for all the groups are the same. The scenarios will be presented to groups, and they will distribute tasks among group members. The group work is supervised by lecturers, who will provide the final grade of the student's performance.

Students have 3 hours for solving each case and prepare for the presentation. Groups are required to present their work and defend it in front of other groups after each case. The duration of each presentation is 20-25 minutes. Peer groups' constructive and essential feedback is an integral part of the assessment. Each group is expected to provide feedback and opposing views to one peer group. The time limit for providing feedback and asking questions about the peers' cases is 15 minutes. The lecturers will also provide their feedback about the group work.

The case study is assessed non-distinctively, and the students must meet all the assessment criteria to pass.

In case of failing, students will have the opportunity for reassessment, which involves addressing the identified deficiencies found in the presentation and delivering the presentation again in an online environment after approximately two weeks.

If a student was not able to attend the assessment due to justified reasons, they will be offered an online assessment opportunity after approximately two weeks.

For information on the assessment criteria see in the **ANNEX 1 Assessments.**

8.4.4 Module 4 Sessions

Session 1. European Union's external dimension in countering hybrid threats

Session aim: The session aims to create opportunities for students to develop knowledge about European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies

Session duration: 41 independent learning hours and 4 contact learning hours

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. European Union's external dimension in countering hybrid threats. Cooperation with third countries in the context of hybrid crises. Common Security and Defence Policy (CSDP) missions
2. Common Security and Defence Policy and crisis response mechanisms with diplomatic engagement
3. European Union-NATO cooperation in countering hybrid threats

Learning activities

During independent learning hours, students will work at home using the Moodle course and will be assisted by the module lecturers. Students can contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory for students to read the entire reading list and go through all eLearning tools. After that, students are expected to complete a self-assessment test (a multiple-choice test) on the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies. The self-assessment tasks will serve as a prerequisite for participating in the contact week. Feedback about the test will be provided in Moodle.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

Council Conclusions 2022, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*. Available from: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/. [10 October 2023].

European External Action Service 2023, *Missions and Operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

European External Action Service 2022, *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and*

security. Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en. [20 September 2023].

European External Action Service 2021, *Crisis management and response*. Available from: https://www.eeas.europa.eu/eeas/crisis-management-and-response_en. [25 October 2023].

European Council 2022, *How the EU responds to crises and builds resilience*. Available from: https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/. [20 October 2023].

Faleg, G (ed) 2022, *The EU's Civilian Headquarters: Inside the control room of civilian crisis management*. European Union Institute for Security Studies EUISS, Chaillot Paper 175, Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/eus-civilian-headquarters. [10 September 2023].

North Atlantic Treaty Organisation 2023, *Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. Available from: https://www.nato.int/cps/en/natohq/official_texts.htm?keywordquery=EU-NATO%20relations&search=true. [2 September 2023].

Permanent Structured Cooperation 2023, *Permanent Structured Cooperation*. Available from: https://www.pesco.europa.eu/. [25 October 2023].

Rehrl, J (ed) 2021, *Handbook on CSDP. The Common Security and Defence Policy of the European Union*. 4th Ed. Federal Ministry of Defence of the Republic of Austria.

Rühle, M & Roberts, C 2021, *Enlarging NATO's toolbox to counter hybrid threats*. Available from: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html. [16 October 2023].

Zandee, D, van der Meer, S & Stoetman, A 2022, *Countering hybrid threats: Steps for improving EU-NATO cooperation,* Clingendael Report, Netherlands Institute of International Relations. Available from: https://www.clingendael.org/pub/2021/countering-hybrid-threats/. [2 September 2023].

Recommended readings

Andersson, J J 2023, *European Defence Partnerships: Stronger Together*, European Union Institute for Security Studies EUISS, Brief no. 3. Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/european-defence-partnerships. [20 September 2023].

Andersson, JJ & Cramer, CS 2023, *EUISS Yearbook of European Security*. EU Institute for Security Studies. Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/yearbook-european-security-2023. [10 October 2023].

Boin, A & Rhinard, M 2023, 'Crisis Management Performance and the European Union: The Case of COVID-19'. *Journal of European Public Policy*, vol. 30(4), pp. 655–675. Available from: https://doi.org/10.1080/13501763.2022.2141304. [27 October 2023].

Brethous, M & Kovalčíková, N 2023, *Next level partnership: Bolstering EU–NATO cooperation to counter hybrid threats in the Western Balkans*, EUISS Brief no 2, Luxembourg: Publications Office of

the European Union. Available from: https://www.iss.europa.eu/content/next-level-partnership-bolstering-eu-nato-cooperation-counter-hybrid-threats-western-balkans. [3 September 2023].

Council of the European Union, 2022, *Draft Council conclusions on a framework for a coordinated EU response to hybrid campaigns. Draft Council Conclusions,* 10013/22.

Council of the European Union, 2021, *Mini-concept on civilian CSDP support to countering hybrid threats. European External Action Se*rvice*, Written Consultation on the third revision of the Mini-concept on civilian CSDP support to countering hybrid threats,* WK 11851/2020 REV 2.

Countering hybrid threats: EU–NATO cooperation [Policy Podcast]. Available from: https://www.europarl.europa.eu/rss/podcast/eprs-policy-podcast/mp3/2017/hybrid-threats-eu-nato.mp3. [4 September 2023].

Cullen, P, Juola, C, Karagiannis, G, Kivisoo, K, Normark, M, Rácz, A, Schmid, J & Schroefl, J 2021, *The landscape of Hybrid Threats: A Conceptual Model*, Giannopoulos, G, Smith, H and Theocharidou, M (eds), Luxembourg: Publications Office of the European Union. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305. [18 October 2023].

Directorate-General for Research and Innovation (European Commission) 2022, *Strategic crisis management in the EU – Improving EU crisis prevention, preparedness, response and resilience*, Luxembourg: Publications Office of the European Union. https://data.europa.eu/doi/10.2777/517560. [27 October 2023].

European Commission, 2018, *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council,* JOIN (2018) 16 final. Available from: EUR-Lex - 52018JC0016 - EN - EUR-Lex (europa.eu). [21 November 2022].

EUR-Lex. Summaries of EU Legislation 2020, *Crisis Management – Framework for Participation Agreements*. Available from: https://eur-lex.europa.eu/EN/legal-content/summary/crisis-management-framework-for-participation-agreements.html. [26 October 2023].

EUR-Lex 2012, 'Consolidated Version of the Treaty on the Functioning of the European Union', *Official Journal of The European Union,* C 326. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF. [20 September 2023].

European Commission, 2016, *Joint Framework on countering hybrid threats a European Union response. Joint communication to the European Parliament and the Council,* JOIN (2016) 18 final. Available from: JOIN_2016_0018_FIN.ENG.xhtml.1_EN_ACT_part1_v8.docx (europa.eu) [21 November 2022].

European Defence Agency 2023, *Coordinated annual review on defence*. Available from: https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card). [25 October 2023].

European External Action Service 2021, *The Common Security and Defence Policy*. Available from: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en. [20 September 2023].

European External Action Service 2023, *About CSDP structure, instruments and agencies*. Available from: https://www.eeas.europa.eu/eeas/csdp-structure-instruments-and-agencies_en. [23 October 2023].

European External Action Service 2023, *Missions and operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

Faleg, G & Kovalčíková, N 2022, 'Rising hybrid threats in Africa: Challenges and implications for the EU', Brief no. 3, European Union Institute for Security Studies. Available from: https://www.iss.europa.eu/content/rising-hybrid-threats-africa. [10 October 2023].

Jungwirth, R, Smith, H, Willkomm, E, Savolainen, J, Alonso Villota, M, Lebrun, M, Aho, A & Giannopoulos, G 2023, *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Luxembourg: Publications Office of the European Union. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC129019. [10 September 2023].

North Atlantic Treaty Organisation 2023, *EU-NATO task force on the resilience of critical infrastructure 2023, Final assessment report.* Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf. [10 October 2023].

NATO Energy Security Centre of Excellence 2023, *NATO ENSEC COE Official website*. Available from: https://www.enseccoe.org/en. [2 September 2023].

NATO Library 2023, *NATO–EU relations*. Available from: https://natolibguides.info/nato-eu/documents. [20 September 2023].

NATO Strategic Communications Centre of Excellence (NATO StratCom COE) 2020, *NATO Strategic Communications Centre of Excellence Official website*. Available from: https://stratcomcoe.org/. [2 September 2023].

Permanent Structured Cooperation 2023, *About PESCO.* Available from: https://www.pesco.europa.eu/. [20 October 2023].

PreventionWeb 2022, *Strategic crisis management in the European Union*, Science advice for policy by European Academies. Available from: https://www.preventionweb.net/publication/strategic-crisis-management-european-union. [27 October 2023].

The European Centre of Excellence for Countering Hybrid Threats, *Hybrid COE Official website*. Available from: https://www.hybridcoe.fi/. [2 September 2023].

The NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE Official website*. Available from: https://ccdcoe.org/. [2 September 2023].

Session 2. Border security and management

Session aim: The session aims to create opportunities for students to develop skills to critically analyse the European Union's approach to internal and border security management and evaluate the role of fundamental rights in it

Session duration: 55 independent learning hours, 4 contact learning hours, 24 hours experiential learning (of which 8 hours for assessment)

Learning Environment(s) and Requirements

eLearning environment and classrooms for contact learning. Possibility to visit the European Union's external border.

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. European Union's approach to internal and border security management. Fundamental rights as a horizontal component of border security management
2. Situational awareness and the role of intelligence in situational awareness
3. The most common types of intelligence used in border management
4. Migration as a tool for hybrid attacks. Protection of fundamental rights of migrants

Learning activities

During independent learning hours, students will work at home using the Moodle course and will be assisted by the module lecturers. Students can contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

The experiential learning phase will last for 3 days (24 hours) and will take place at the European Union's external border. The students will gain experience in the European Union's approach to internal and border security management and the role of fundamental rights in it. They will have an opportunity to visit a border crossing point at the European Union's external border, contact experts and get experience in the implementation of integrated border management. As a part of the experiential learning phase, students must pass the assessment by solving a case study about the appearance of hybrid threats at the European Union's external border.

Essential reading

Council of the European Union 2009, Updated EU Schengen Catalogue *External borders Control Return and readmission Recommendations and best practices* (7864/09), pp. 13-15. Available from: https://data.consilium.europa.eu/doc/document/ST-7864-2009-INIT/en/pdf. [10 March 2023].

European Commission 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response.* JOIN/2016/018 final, Document

52016JC0018, p. 2. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [21 January 2023].

European Commission 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strateg,* COM(2020) 605 final,

pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [13 December 2022].

European Commission 2022, *Developing a multiannual strategic policy for European integrated border management in accordance with Article 8(4) of Regulation (EU) 2019/1896. Policy document,* COM (2022) 303 final*,* Article 3. Available from: EUR-Lex - 52022DC0303 - EN - EUR-Lex (europa.eu). [21 November 2022].

European Commission 2023, *Communication from the Commission to the European Parliament and the Council establishing the multiannual strategic policy for European integrated border Management*. COM(2023) 146 final. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:f7b5247b-c296-11ed-a05c-01aa75ed71a1.0001.02/DOC_1&format=PDF [11 April 2023].

European Commission 2023, *Annexes to the Communication from the Commission to the European Parliament and the Council establishing the multiannual strategic policy for European integrated border Management*. COM(2023) 146 final*.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0146&from=EN [11 April 2023].

European Commission 2024, *Managing migration responsibly*. Available from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/story-von-der-leyen-commission/managing-migration-responsibly_en. [27 August 2024].

European Parliament 2024, Legislative train 05.2024. Available from: https://www.europarl.europa.eu/legislative-train/carriage/revision-of-the-schengen-borders-code/report?sid=8101. [27 August 2024].

European Parliament and the Council of the European Union 2019, *Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624*, Recitals 1-5, 9-57, Article 3. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN. [27 January 2023].

Official Journal of the European Union 2016*, Consolidated versions of the Treaty on European Union and the Treaty on the functioning of the European Union*, (2016/C 202/01), pp. 29-32. **Available from:** https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497 01aa75ed71a1.0006.01/DOC_3&format=PDF. [10 March 2023].

Punda Y, Shevchuk V & Veebel V 2019, 'Is the European migrant crisis another stage of hybrid war?', *Sõjateadlane (Estonian Journal of Military Studies)*, vol. 13, pp. 116–119. Available from: https://www.kvak.ee/sojateadlane/. [26 August 2024].

Recommended readings

Council of the European Union 2002, *Plan for the management of the external borders of the Member States of the European Union,* doc, 10019/02, pp. 11-27. Available from: https://data.consilium.europa.eu/doc/document/ST%2010019%202002%20INIT/EN/pdf. [09 March 2023].

Council of the European Union 2002, *Plan for the management of the external borders of the Member States of the European Union, doc, 10019/02,* pp. 11-27. Available from: https://data.consilium.europa.eu/doc/document/ST%2010019%202002%20INIT/EN/pdf. [09 March 2023].

European Commission 2002, *Communication from the Commission to the Council and the European Parliament - towards integrated management of the external borders of the member states of the European Union*, COM/2002/0233 final, pp. 6, 12-22**.** Available from**:** EUR-Lex-52002DC0233 - EN (europa.eu). [06 February 2023].

Estonian Academy of Security Sciences 2022, *Impact of Events in Belarus on the Safety and Security of the Baltic States*. Available from: https://digiriiul.sisekaitse.ee/handle/123456789/2853. [26 August 2024].

EU Monitor 2024, *Legal provisions of COM (2021)891 - Amendment of Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders.* Available from: https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vloruvttc5ze. [27 August 2024].

European Commission 2021, *Von der Leyen on Belarus: The EU has the will, the unity and the resolve to face this crisis*. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ac_21_6254. [27 August 2024].

Hall, B, Fleming S & Shotter, J 2021, 'How migration became a weapon in a 'hybrid war'', *Financial Times*. Available from: https://www.ft.com/content/83ece7e4-cc71-45b5-8db7-766066215612. [27 August 2024].

Presidency Conclusions 2001, *European Council Meeting in Laeken 14 and 15 December 2001*, p. 13. Available from: https://www.consilium.europa.eu/media/20950/68827.pdf. [16 February 2023].

Mac Dougall, D 2023, *Russia using 'hybrid warfare' tactics to push migrants over Finnish border,* Euronews. Available from: https://www.euronews.com/2023/11/14/finland-says-russia-is-helping-migrants-make-their-way-over-the-eastern-border. [27 August 2024].

Session 3. Countering information advocacy and influence activities

Session aim: The session aims to create opportunities for students to develop skills to critically evaluate actions countering information advocacy and influence activities and to analyse psychological aspects related to radicalisation and different forms of extremism on social media

Session duration: 55 independent learning hours, 5 contact learning hours

Learning environment(s) and requirements

eLearning environment and classrooms for contact learning

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Planning and management of information advocacy and influence activities
2. Nonviolent struggle and *modus operandi* of radical organisations
3. Psychological protection against radicalisation and different forms of extremism
4. State and non-state actors' activities related to hybrid threats

Learning activities

During independent learning hours, students will work at home using the Moodle course and will be assisted by the module lecturers. Students can contact the lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is mandatory to read the entire reading list and go through all eLearning tools. After that, students will participate in two forum discussions about:

- actions countering information advocacy and influence activities;
- psychological aspects related to radicalisation and different forms of extremism on social media.

In case the student did not participate in forum discussions, s/he will take online test before contact week.

In the contact week, essential contents delivered previously in the independent learning phase will be discussed in depth in a set of lectures/seminars.

Essential reading

Daukšas, V., Fridman, O., Urbanavičiūtė, K., Venclauskienė, L. 2024, *War on All Fronts: How the Kremlin's Media Ecosystem Broadcasts the War in Ukraine*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/war-on-all-fronts-how-the-kremlins-media-ecosystem-broadcasts-the-war-in-ukraine/301. [27 August 2024].

Hodos, P. N. 2022, *Playing to Extremes: Russia's Choices to Support Western Political Extremists and Paramilitary Groups*. International Journal of Intelligence and CounterIntelligence. https://doi.org/10.1080/08850607.2022.2109449. [27 August 2024].

Jokinen, J., Normark, M. & Fredholm, M. 2022, *Hybrid threats from non-state actors: A taxonomy*. Hybrid CoE Research Report No. 6 (June 2022). Available from:

https://www.hybridcoe.fi/publications/hybrid-coe-research-report-6-hybrid-threats-from-non-state-actors-a-taxonomy/. [27 August 2024].

Monaghan, S. 2022, *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice*. Hybrid CoE Paper No. 12 (March 2022). Available from: https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/. [27 August 2024].

Recommended readings

EU Code of conduct on countering illegal hate speech online 2019, Brussels: European Commission. Available from: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en [6 October 2024].

EU Code of practice on disinformation 2022, Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation [6 October 2024].

Europol Annual EU Terrorism Situation and Trend Reports (TE-SAT). European Union Agency for Law Enforcement Cooperation. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

Extremism, Radicalisation & Mental Health: Handbook for Practitioners 2019, Product of the RAN Centre of Excellence and the RAN H&SC Working Group. Available from: https://home-affairs.ec.europa.eu/system/files/2019-11/ran_h-sc_handbook-for-practitioners_extremism-radicalisation-mental-health_112019_en.pdf [10 November 2024].

Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training 2022, Brussels: European Commission. Available from: https://op.europa.eu/en/publication-detail/-/publication/a224c235-4843-11ed-92ed-01aa75ed71a1/language-en [6 October 2024].

Loik, R. and Madeira, V. 2021, *European Union Strategy and Capabilities to Counter Hostile Influence Operations*. In: H. Mölder; V. Sazonov; A. Chochia; T. Kerikmäe (Ed.). The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood, pp. 247−264. Switzerland: Springer Nature.

Palmertz, B. 2021, *Influence operations and the modern information environment*. In: Hybrid Warfare: Security and Asymmetric Conflict in International Relations. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm. London: I.B. Tauris, Bloomsbury Collections. http://dx.doi.org/10.5040/9781788317795.0014

Pamment, J. 2022, *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/a-capability-definition-and-

assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255 [11 September 2024].

Pape, R. 2024, *The Return of Political Violence*. A Conversation with Robert Pape. The *Foreign Affairs* Interview (November 7, 2024). Available from: https://www.foreignaffairs.com/podcasts/return-political-violence [7 November 2024].

per Concordiam. Journal of European Security and Defense Issues. *Beyond Propaganda: Exposing Falsehoods and Fake News*. Volume 9, Issue 2, 2019. Available from: https://perconcordiam.com/archives/

per Concordiam. Journal of European Security and Defense Issues. *Strategic Communications: Winning the Information War*. Volume 10, Issue 2, 2020. Available from: https://perconcordiam.com/archives/

Report on FIMI Threats 2024, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence. EU External Action Service. Available from: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Strategic Framework for Countering Terrorism and Targeted Violence 2019, Department of Homeland Security (September 2019). Available from: https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

Sörensen, S. 2024, *Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/enhancing-organisational-capability-a-tailored-approach-with-red-team-vs-blue-team-adapted-workshops/299 [6 October 2024].

Wardle, C. & Derakshan, H. 2017, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe report DGI(2017)09. Strasbourg: Council of Europe. Available from: https://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf [6 October 2024].

Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm. London: I.B. Tauris, Bloomsbury Collections. http://dx.doi.org/10.5040/9781788317795.0014

Session 4. Management and leadership in the context of hybrid challenges

Session aim: The session aims to create opportunities for students to develop skills to manage and lead human and challenges and threats based on modern theories, considering professional ethics, fundamental rights and principles of

Session duration: 123 independent learning hours and 27 contact learning hours (of which 18 hours for assessment)

Learning environment(s) and requirements

eLearning environment, classrooms for contact learning and simulation centre

Learner resources

PCs and/or mobile devices with the latest versions of browsers

Session topics

1. Modern theories and concepts of management and leadership
2. Professional ethics
3. Equal treatment of diverse groups
4. Principles of management and leadership for encountering modern security challenges and threats
5. Leadership and management in case of hybrid crises. Solving ethical dilemmas and following principles of equal
6. Strategic management of civilian human resources, balancing organisational goals in case of modern crises and
7. Strategic management of modern technical resources (military, paramilitary, civilian)
8. Strategic communication in case of hybrid crises following principles of professional ethics
9. Hybrid threats' impact on decision-making

Learning activities

During independent learning hours, students will work at home using the Moodle course and will be assisted by the mod lecturers using the Moodle course to discuss any issues related to the contents in the forums.

Students will have access to the eLearning classroom where selected readings and eLearning tools will be available. It is list and go through all eLearning tools. After that, students are expected to complete a self-assessment test (a multipl concepts of management and leadership. The self-assessment tasks will serve as a prerequisite for participating in the will be provided in Moodle.

In the contact week, essential contents covered during the independent learning phase will be discussed in depth in a se exercise will take place (18 hours).

Essential reading

Clegg, S, Crevani, L, Uhl-Bien, M, Todnem, R 2021, 'Changing leadership in changing times', *Journal of Change Managem* from: https://doi.org/10.1080/14697017.2021.1880092 [7 September 2023].

Deverell, E & Olsson E-K 2010, 'Organizational culture effects on strategy and adaptability in crisis management', *Risk M* 134. Available from: https://link.springer.com/article/10.1057/rm.2009.18. [24 November 2023].

Fagerberg, J 2009, *Innovation: A Guide to the Literature*, The Oxford Handbook of Innovation, Oxford Academic. Availabl https://doi.org/10.1093/oxfordhb/9780199286805.003.0001. [27 November 2023].

Hoffjann, O 2022, 'Between strategic clarity and strategic ambiguity – oscillating strategic communication', *Corporate C Journal*, vol. 27, no. 2, pp. 284-303. Available from: https://doi.org/10.1108/CCIJ-03-2021-0037. [30 November 2023].

Maak, T, Pless, N.M, Wohlgezogen, F 2021, 'The fault lines of leadership: Lessons from the global Covid-19 Crisis', *Journ* 1, pp. 66-86. Available from: https://doi.org/10.1080/14697017.2021.1861724. [9 September 2023].

McAuliffe, D & Chenoweth, L 2008, 'Leave no stone unturned: The inclusive model of ethical decision making', *Ethics an* 49. Available from: http://dx.doi.org/10.1080/17496530801948739. [10 September 2023].

McKinsey & Company 2022, *What is diversity, equity, and inclusion?*. Available from: https://www.mckinsey.com/featur explainers/what-is-diversity-equity-and-inclusion. [8 September 2023].

Moilanen, T & Salminen, A 2006, *Comparative study on the public-service ethics of the EU member states. A report from EUPAN*. Available from: https://vm.fi/documents/10623/307711/Comparative_Study_on_the_Public_Service_Ethics_of_the_EU_Member_State 5388-4d1c-9199-59b4f3e567a9/Comparative_Study_on_the_Public_Service_Ethics_of_the_EU_Member_States_public 2023].

Verhage A, Noppe J, Feys, Y & Ledegen, E 2018, 'Force, stress, and decision-making within the Belgian police: the impact decision-making', *Journal of Police and Criminal Psychology*, vol. 33. Available from: https://doi.org/10.1007/s11896-018

8.4.5 Delivery Timetable for Module 4

Module 4	**February 10 - April 10, 2026**
Phase	**Dates**
Independent learning phase - Reading mandatory literature and studying e-learning materials - Taking self-assessment test (a multiple-choice test) about the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies; - 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; - Taking self-assessment test (a multiple-choice test) about modern theories and concepts of management and leadership.	February 10 - March 30, 2026
Experiential learning phase **Assessment:** Solving a case study that addresses the appearance of hybrid threats at the European Union's external border	April 1 - 3, 2026
Contact learning phase **Assessment:** - Tabletop exercise	April 6 - 10, 2026
Reassessments	April 17, 2026 - deadline for liquidation of student debts

8.5 Master's Exam. Theoretical-analytical Essay

Pre-requisite Modules:	Module 1, Module 2, Module 3 and Module 4		ECTS Credits 15
Contact learning hours	**Independent learning hours**	**Experiential learning**	**Total**
90	300	0	390

8.5.1 Aim of the Master's exam and learning outcomes to be assessed

During the master's exam, students prove the maturity of their theoretical and professional preparation and their ability to apply the acquired knowledge. The student will be required to prepare a theoretical-analytical essay that addresses the specific needs of their speciality. This entails working with scientific sources and presenting a well-structured analysis of the study in the proper form.

Successful completion of the Master's exam indicates that the student has achieved the goals set by the curriculum. It demonstrates the student's professional maturity and their capability to apply theories, professional skills, and acquired competence from the course of study.

Upon completion of the Master's exam, the student will be able to:

- formulate and present the problem related to hybrid threats;
- create a systematized and evidentiary solution to the (identified) problem;
- use relevant literature to solve the problem, citing sources accurately
- synthesize theoretical approach, using scientific methods;
- employ appropriate social science data collection and analysis methods;
- present their research and proposed solutions in an argumentative and convincing manner, adhering to academic standards and practices.

8.5.2 Assessment strategy

The Master's exam is composed of writing a theoretical-analytical essay and defending the essay. Students can choose the topics for the essay from a provided list or propose their own topics. If the student chooses a topic not from the list, they must coordinate it with the assigned academic staff members. The writing process will be guided by a supervisor.

Students may also opt for a preliminary defence of their essay. To do so, the essay must meet the requirements of the guidelines for the preparation and formatting of student papers, along with the assessment criteria described in the table below. Feedback on the essay will be provided based on the established requirements pointing out any shortcomings.

Students must submit the essays by the designated deadline, which is, approximately three weeks before the defence.

During the defence, essays will be evaluated by the defence committee. A positive grade is achieved if each subsection of the essay is graded at least with the grade "E". The final grade will be the average of the grades of the subsections. If a student receives a grade “F” in at least one subsection, the final grade will be “F” (fail).

Students who defend an essay with a negative grade will have the opportunity to eliminate all the identified deficiencies and defend the essay again within one month.

Phase	Dates
Independent learning - Writing a theoretical-analytical essay	April 13 – May 26, 2026
Contact learning phase - Preliminary defence of the essay	May 27 – 29, 2026 June 1, 2026 – deadline for submitting the essay
Assessment: - Defence of the essay	June 18 -19, 2026

ANNEX 1 Assessments

Module 1 Assessments and assessment criteria

The learning outcomes to be assessed	Assessment methods	Assessment criteria
critically analyse hybrid threats in the context of global, European and national security evaluate the security strategies aiming to ensure sustainable security concepts in the contemporary hybrid threats environment	Written analysis	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The measures from the security strategies to overcome the impact of the hybrid threat(s) are analysed. - The hybrid threat(s), related to the strategy, and models of its(their) appearance are clearly defined. - The evaluation of measures of the security strategy reflects their suitability to ensure sustainable security concepts in the contemporary hybrid threats environment. - The results of the analysis are presented logically and comprehensibly. The author has presented their own views. - The terms used in the analysis are clearly explained. - Selection and interpretation of sources are sufficient and demonstrate critical interpretation skills. - The conclusions and proposals are formulated and correspond to the stated task. - The format of the analysis corresponds to the guidelines for the preparation and formatting of student papers. - The analysis is structured, and the structure corresponds to the purpose of the work. - The sources used are cited. Sentence structure and spelling are correct. The work is mostly written in scientific language (use of unscientific language is allowed to an extent that does not affect the comprehensibility of the work). The volume of the paper is 2000 - 3000 words.
discuss international and European Union policies and legal frameworks responding to hybrid threats, considering provisions of	Online test with open-ended questions (using all the materials)	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The answer to each question is clear and sufficient. - The answers are provided within a predetermined time.

The learning outcomes to be assessed	Assessment methods	Assessment criteria
fundamental rights		
critically analyse tendencies of contemporary warfare regarding hybrid threats	Case study. Group work and presentation	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The theoretical concepts of a case study are critically evaluated. The causes and consequences of the problem in a case study are analysed. - The background of a case study is explained by using information from 3-4 different sources. The author has explained how reliable they are and why. - The conclusions are clearly justified. All questions are properly addressed. Recommendations are relevant. - Presentation is structured based on the assessment criteria. Important information is presented using visual means. Effective application of relevant vocabulary. The duration of the presentation is 10-15 minutes. - The feedback given to peer groups is constructive and essential. - The questions about the peers' case study are appropriate and presented orally. - The answers to the questions are relevant and sufficient.
critically analyse cases of information warfare and their impact on fundamental rights	Case study. Group work and presentation	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The theoretical concepts of a case study are critically evaluated. The causes and consequences of the problem in a case study are analysed. - The background of a case study is explained by using information from 3-4 different sources. The author has explained how reliable they are and why. - The conclusions are clearly justified. All questions are properly addressed. Recommendations are relevant. - Presentation is structured based on the assessment criteria. Important information is presented using visual means. Effective application of relevant vocabulary. The duration of the presentation is 10-15 minutes. - The feedback given to peer groups is constructive and essential. - The questions about the peers' case study are appropriate and presented orally. - The answers to the questions are relevant and sufficient.
independently and creatively identify problems related to hybrid	Drafting a scientific essay	**Distinctive assessment** Assessment criteria for scientific essay are: - Identifying problem(s)

The learning outcomes to be assessed	Assessment methods	Assessment criteria
threats and develop and design solutions to respond to hybrid threats using different research strategies and methods in social science research		- Content (Theoretical part. Evidence from existing literature) - Research methodology - Presentation and analysis of research results. Formulating the conclusion - Formatting the essay More detailed assessment criteria are given in the table below.
Requirements and formation of the final grade:	A positive grade is achieved if each learning outcome is graded at least with the grade "E" or “Pass”. The final grade of the module is the grade of the scientific essay.	

Scientific essay grading criteria

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
Identifying problem(s). Formulating hypothesis or research questions. The aim of the essay	**The problem** related to hybrid threats is formulated but is general and vague, lacking a clear definition of the phenomenon under investigation. **The research questions and/or hypotheses** are formulated in general and loose terms, partially aligned with the research problem and theory.	**The problem** related to hybrid threats is formulated in a way that partially defines the investigated phenomenon but lacks strong links to the actuality and novelty of the work. **The research questions and/or hypotheses** are formulated in general and loose terms but are broadly consistent with the research problem and theory.	**The problem** related to hybrid threats is formulated in a way that defines the phenomenon under investigation and is generally associated with the actuality and novelty of the work. **The research questions and/or hypotheses** are specifically formulated and generally correspond to the research problem and theory.	**The problem** related to hybrid threats is formulated concretely and is clearly related to the actuality and novelty of the work. **The research questions and/or hypotheses** are specifically formulated and clearly aligned with the research problem and theory.	**The problem** related to hybrid threats is formulated concretely and linguistically precisely and clearly defines the phenomenon under study, which is appropriately and comprehensively associated with the actuality and novelty of the work. **The research questions and/or hypotheses** are formulated specifically and linguistically accurately, clearly

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	The aim of the research is formulated as an achievement but is diffuse and partially aligned with the title and research problem.	**The aim** of the research is general, formulated as an achievement and generally corresponds to the title of the work and the research problem.	**The aim** of the research is specific, formulated as an achievement and generally corresponds to the title of the thesis and the research problem.	**The aim** of the research is specific and realistic, formulated as an achievement and in accordance with the title of the work and the research problem.	aligned with the research problem and theory. **The aim** of the research is specific, realistic and linguistically accurate, formulated as an achievement and clearly aligned with the title of the paper and the research problem, giving the research a clear focus.
Content (Theoretical part)	**The theoretical part** of the work is partially related to the topic and forms a loosely connected referential review. For example,	**The theoretical part** of the work is mainly related to the topic, and it contains little analysis and generalization.	**The theoretical part** of the work is relevant to the topic and includes analysis and generalization but lacks	**The theoretical part** of the work is relevant to the topic, noticeably analytical and generalizing, and a	**The theoretical part** of the work is topical, systematic, comprehensively analytical and generalizing, with a

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	one source is cited page by page or the references follow each other without transitions. A minimum of 5 relevant scientific sources have been used, but the text of the theoretical part is dominated by numerous non-scientific and partially relevant sources (general textbooks, manuals, documents, laws, etc.).	A minimum of 5 topical scientific sources have been used, but the text of the theoretical part is sometimes dominated by non-scientific topical sources (general textbooks, manuals, documents, laws, etc.).	a synthesis by the author. A minimum of 5 relevant research sources have been used. The work uses non-scientific sources relevant to the topic (general textbooks, manuals, documents, laws, etc.), but they do not dominate.	connected complete text. More than 5 relevant scientific sources have been used, including international scientific sources. Non-scientific sources (general textbooks, manuals, documents, etc.) have not been used in the theoretical part of the work, if it is not necessary based on the topic of the work. If these sources are used reasonably, their share does not exceed the	well-connected complete text. More than 5 relevant scientific sources have been used, including international scientific sources. Non-scientific sources (general textbooks, manuals, documents, etc.) have not been used in the theoretical part of the work, if it is not necessary based on the topic of the work. If these sources are used reasonably, their share does not exceed

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
				share of scientific sources.	the share of scientific sources.
Research methodology	**The methodology part** slightly justifies the research process's data collection and data analysis methods. When justifying the choice of methodology, reference is made to individual scientific methodology textbooks or teaching aids in the native language. With the selected research methods, it is possible to partially answer the research	**The methodology part** in general terms justifies the research process's data collection and data analysis methods. When justifying the choice of methodology, reference is made to several scientific methodology textbooks or teaching aids in the native language. With the chosen research methods, it is generally possible to answer the research	**The methodology part** justifies the research process's data collection and data analysis methods. When justifying the choice of methodology, reference is made to native language scientific methodology textbooks or teaching aids and individual international methodological scientific sources. With the chosen research methods, it is	**The methodology part** clearly justifies the research process's data collection and data analysis methods. When justifying the choice of methodology, mostly international methodological research sources are cited. The chosen research methods are appropriate to answer the research problem	**The methodology part** expertly justifies the research process's data collection and data analysis methods, analysing the suitability and limitations of the chosen methods. When justifying the choice of methodology, reference is made to international methodological scientific sources. The chosen research methods are the most suitable to answer the

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	problem and achieve the goal of the work.	problem and achieve the goal of the work.	possible to answer the research problem and achieve the goal of the work.	and achieve the purpose of the work.	research problem and achieve the goal
Presentation and analysis of research results. Formulating the conclusion	**Presentation of the results:** the research results are sometimes difficult to follow, as there is no clear structure and the use of well-thought-out illustrative tools (tables, figures, quotations, etc.). **Analysis of the results:** the work contains a small amount of analysis (interpretation) of the results and their	**Presentation of the results**: the research results are generally traceable, though sometimes there is a lack of a clear structure and the use of well-thought-out illustrative tools (tables, figures, quotations, etc.). **Analysis of the results**: the work contains a small amount of analysis (interpretation) of the results and their	**Presentation of results:** the research results are traceable, and the use of illustrative tools (tables, figures, quotations, etc.) is well thought out. **Analysis of the results**: the work includes a comprehensive analysis of the results and their interpretation and relation to the theory. The answers to the research problem,	**Presentation of the results**: the research results are easy to follow, and the use of illustrative tools (tables, figures, quotations, etc.) is well thought out. **Analysis of results**: the paper includes a thorough analysis, interpretation, and application of the theory to the results, providing specific	**Presentation of the results**: the research results are well-observable and systematically presented, and the use of illustrative tools (tables, figures, quotations, etc.) is skilfully thought out. **Analysis of the results**: the work includes a thorough analysis and interpretation of the results, associating

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	association with theory. In general, the answers to the research problem, hypothesis(es) and/or research questions have been partially found. The goal of the work has been achieved. **Conclusions** and suggestions are weakly related to the results of the study.	relation to the theory, in general, the answers to the research problem, hypothesis(es) and/or research questions have been found. The goal of the work has been achieved. **Conclusions** and suggestions are partly related to the results of the study.	hypothesis(es) and/or research questions have been found. The goal of the work has been achieved. **Conclusions** and suggestions are related to the results of the study and are applicable.	answers to the research problem, hypothesis(es) and/or research questions. The objective of the paper has been achieved. **Conclusions** and suggestions are clearly related to the results of the study and are applicable.	them with theory and a critical approach, giving specific and logically argued answers to the research problem, hypothesis(es) and/or research questions. The goal of the work has been achieved. **Conclusions** and proposals are applied, clearly related to the results of the study and contain, among other things, recommendations on the implementation of the results and further research directions

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
Formatting the essay	The length of the essay, from the introduction to the list of sources, is 10-15 pages. The essay mostly has a comprehensible structure, and the different parts of the work are partially connected. The format of the paper generally corresponds to the guidelines for the preparation and formalization of student papers. The sources used are cited, but there are several minor inaccuracies in the	The length of the essay, from the introduction to the list of sources, is 10-15 pages. The essay has an understandable structure, and the different parts of the work are generally connected. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are cited, but there are a few minor inaccuracies in the	The length of the essay, from the introduction to the list of sources, is 10-15 pages. The essay has an understandable structure, the parts of which are related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited and the source entries are correct. The sentence structure and	The length of the essay, from the introduction to the list of sources, is 10-15 pages. The essay has an understandable and logical structure, the parts of which are clearly related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited and the entries are correct. The sentence	The length of the essay, from the introduction to the list of sources, is 10-15 pages. The essay has an understandable and logical structure, the parts of which are clearly related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited and the entries are correct. The sentence

Grading criteria	Grade E criterion Pass Work that just only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject; evidence of limited additional reading/research/work	Grade D criterion Work of fair quality Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Grade C criterion Work of good quality. Above average performance, with a good working knowledge of subject matter. Evidence of sufficient reading/ research/ work	Grade B criterion Work of very good quality. Performance is typified by a very good working knowledge of subject matter. Evidence of a considerable amount of reading/ research/ work	Grade A criterion Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	references and source entries. Sentence structure and spelling are mostly correct, but there are some errors. Non-scientific language is used throughout, but the work is generally comprehensible.	references and source entries. The sentence structure and spelling are correct. In several places, non-scientific language is used, but the work is understandable.	spelling are correct. The work is mostly written in scientific language, with non-scientific language used in some places.	structure and spelling are correct. The work is written in scientific language.	structure and spelling are correct. The work is written in very good scientific language.

Module 2 Assessments and assessment criteria

The learning outcomes to be assessed	Assessment methods	Assessment criteria
explain the specifics of modern crimes of hybrid nature and criminal procedure concepts and their connection with the principles of fundamental rights explain the risks related to cybersecurity and business continuity and infringement of fundamental rights	Online test with open-ended questions (using all the materials)	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The answer to each question is clear and sufficient. - The answers are provided within a predetermined time.
identify problems, recommend, and elaborate tools and methods of protection against hybrid threats by working in a team and benefiting from team learning processes	Case study. Group work and presentation	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The theoretical concepts of a case study are critically evaluated. The causes and consequences of the problem in a case study are analysed. - The background of a case study is explained by using information from 3-4 different sources. The author has explained how reliable they are and why. - The conclusions are clearly justified. All questions are properly addressed. Recommendations are relevant. - Presentation is structured based on the assessment criteria. Important information is presented using visual means. Effective application of relevant vocabulary. The duration of the presentation is 10-15 minutes. - The feedback given to peer groups is constructive and essential. - The questions about the peers' case study are appropriate and presented orally. - The answers to the questions are relevant and sufficient.
critically analyse the importance of prevention and countering hybrid	Written analysis	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The importance of relevant tools and means of cooperation for prevention and countering hybrid threats are analysed.

threats using relevant tools and means of cooperation		- The results of the analysis are presented logically and comprehensibly. The author has presented their own views. - The terms used in the analysis are clearly explained. - Selection and interpretation of sources are sufficient and demonstrate critical interpretation skills. - The conclusions and proposals are formulated and correspond to the stated task. - The format of the analysis corresponds to the guidelines for the preparation and formatting of student papers. - The analysis is structured, and the structure corresponds to the purpose of the work. - The sources used are cited. Sentence structure and spelling are correct. The work is mostly written in scientific language (use of unscientific language is allowed to an extent that does not affect the comprehensibility of the work). The volume of the paper is 1000 - 2000 words.
Requirements and formation of the final grade:	A positive grade is achieved if each learning outcome is graded at least with the grade “Pass”.	

Module 3 Assessments and assessment criteria

Learning outcomes to be assessed	Assessment methods	Assessment criteria
explain tools for fostering resilience of the state and non-state actors to hybrid threats explain the role of protection of fundamental rights in preparation for responding to hybrid threats, including in cooperation with civil-military and other stakeholders	Online test with open-ended questions (using all the materials)	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The answer to each question is clear and sufficient. - The answers are provided within a predetermined time.
selectively identify and present good practices related to the protection of critical infrastructure and strategic objects	Written analysis	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - The reasons why the analysed infrastructure is considered critical, or the object is strategic are presented. - The possible hybrid threats threatening the infrastructure/object are described and justified. - The ways to protect infrastructures and mitigate hybrid threats are identified. - The good practices related to the protection of similar critical infrastructure and/or strategic objects are identified and discussed. - The results of the analysis are presented logically and comprehensibly. The author has presented their own views. - The terms used in the analysis are clearly explained. - The conclusions and proposals are formulated and correspond to the stated task. - The format of the analysis corresponds to the guidelines for the preparation and formatting of student papers. - The sources used are cited. Sentence structure and spelling are correct. The work is mostly written in scientific language (use of unscientific language is allowed to an extent that does not affect the comprehensibility of the work). The volume of the paper is 1000 - 2000 words.

Requirements and formation of the final grade:	A positive grade is achieved if each learning outcome is graded at least with the grade “Pass”.

Module 4 Assessments and assessment criteria

Learning outcomes to be assessed	Assessment methods	Assessment criteria
critically analyse the European Union's approach to internal and border security management evaluate the role of fundamental rights in the European Union's internal and border security management	Case study	**Non-distinctive assessment (fail/pass)** **Threshold criteria:** - All relevant components of a European Union IBM case study are listed and explained in the context of the current situation. - The underlying causes and potential consequences of each stage of the problem in the case study are analysed. - The background of a case study is explained by using various types of intelligence information from 3-4 different sources. The explanation includes the reliability of the sources and justification for their use. - The link between principles of risk analyses based on CIRAM and situational awareness is presented. - The tools for obtaining and maintaining situational awareness are relevant and justified. - The decisions about primary activities and operational activities are relevant, justified and compliant with the protection of fundamental rights. - The conclusions are clearly justified. All questions are properly addressed. Recommendations are relevant. - The presentation is structured based on the assessment criteria. Important information is presented using visual means. Effective application of relevant vocabulary. The duration of the presentation is 10-15 minutes. - Feedback given to peers' groups is constructive and essential. - The questions about the peers' case study are relevant and on the topic. - The answers to the questions are relevant and sufficient.
explain the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies critically evaluate actions countering	Tabletop exercise	**Non-distinctive assessment (fail/pass)** **Threshold criteria for each case:** - The assessment of the situation is based on European Union policies and legal framework related to hybrid threats and models of their appearance. - The proposed solutions for cooperation with third countries (if it is applicable), international organizations and agencies are appropriate and compliant with European Union's external dimension in countering hybrid threats.

information advocacy and influence activities analyse and interpret psychological aspects related to radicalisation and different forms of extremism on social media propose combined approaches for management and leadership for encountering modern security challenges and threats based on modern theories, considering professional ethics, fundamental rights, and principles of equal treatment of diverse groups apply strategic communication skills in a hybrid context based on ethical values and evaluate the results employ appropriate tools and techniques to strategically manage civilian, human, and technical resources and make decisions in case of hybrid crises, and critically evaluate their peers' problem-solving performance		- The list of responsible parties is complete, and their responsibilities and management methods are clearly defined. - The tools and techniques to strategically manage civilian, human, and technical resources are appropriate and balance organisational goals with stakeholders' expectations. - The applied management and leadership tools and methods are appropriate for the situation, based on modern theories. - The method of strategic communication has been selected based on the situation and the specific characteristics of the media landscape. The message delivered to the right target groups is well thought through, clear and supports ethical values. - The decisions and solutions of the case are clearly justified. The recommendations for measures to prevent and counter hybrid threats are relevant. - All provided solutions and analyses consider fundamental rights, professional ethics, and the protection of vulnerable groups. - Presentation is structured based on the assessment criteria. Important information is presented using different visual means if applicable. Effective usage of relevant vocabulary. The duration of the presentation is 20-25 minutes. - The feedback given to peers' groups is constructive and essential. - The questions about the peers' case study are relevant, on the topic and presented orally. - The answers to the questions are relevant and provide sufficient information.
Requirements and formation of the final grade:	A positive grade is achieved if the student meets all the assessment criteria.	

Master's Exam. Assessment criteria

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
Upon completion of the Master's exam, the student will be able to:	Work that only meets the passing (threshold) standards. Performance demonstrates an understanding of the basic concepts of the subject. Evidence of limited additional reading/research/work	Work of fair quality. Considerable but incomplete understanding of the subject matter. Evidence of a fair amount of reading/ research/ work	Work of good quality. Above-average performance, with a good working knowledge of the subject matter. Evidence of sufficient reading/ research/ work	Work of very good quality. Performance is typified by a very good working knowledge of the subject matter. Evidence of a considerable amount of reading/ research/ work	Work of excellent quality. Superior performance showing a comprehensive understanding and application of the subject matter. Evidence of considerable additional reading/research/work
	Identifying problem(s). Formulating hypothesis or research questions. The aim of the essay				
formulate and present the problem related to hybrid threats	**The problem** related to hybrid threats is formulated but is general and vague, lacking a clear definition of the phenomenon under investigation. **Research questions and/or hypotheses** are formulated in general and loose terms, partially aligned with the research problem and theory.	**The problem** related to hybrid threats is formulated in a way that partially defines the investigated phenomenon but lacks strong links to the actuality and novelty of the work. **The research questions and/or hypotheses** are formulated in general and loose terms but are broadly consistent with the research problem and theory.	**The problem** related to hybrid threats is formulated in a way that defines the phenomenon under investigation and is generally associated with the actuality and novelty of the work. **The research questions and/or hypotheses** are specifically formulated and generally correspond to the research problem and theory.	**The problem** related to hybrid threats is formulated concretely and is clearly related to the actuality and novelty of the work. **Research questions and/or hypotheses** are specifically formulated and clearly aligned with the research problem and theory.	**The problem** related to hybrid threats is formulated concretely and linguistically precisely and clearly defines the phenomenon under study, which is appropriately and comprehensively associated with the actuality and novelty of the work. **Research questions and/or hypotheses** are formulated specifically and linguistically accurately, clearly aligned with the research problem and theory.

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
	The aim of the research is formulated as an achievement but is diffuse and partially aligned with the title and research problem.	**The aim** of the research is general, formulated as an achievement and generally corresponds to the title of the work and the research problem.	**The aim** of the research is specific, formulated as an achievement and generally corresponds to the title of the thesis and the research problem.	**The aim** of the research is specific and realistic, formulated as an achievement and in accordance with the title of the work and the research problem.	**The aim** of the research is specific, realistic and linguistically accurate, formulated as an achievement and clearly aligned with the title of the paper and the research problem, giving the research a clear focus.
	Theoretical part				
synthesize theoretical approach, using scientific methods; use relevant literature to solve the problem, citing sources accurately;	**The theoretical part** of the work is partially related to the topic and forms a loosely connected referential review. For example, one source is cited page by page or the references follow each other without transitions. A minimum of 15 relevant scientific sources have been used, but the text of the theoretical part is dominated by numerous non-scientific and partially relevant sources (general textbooks, manuals, documents, laws, etc.).	**The theoretical part** of the work is mainly related to the topic, and it contains little analysis and generalization. A minimum of 15 topical scientific sources have been used, but the text of the theoretical part is sometimes dominated by non-scientific topical sources (general textbooks, manuals, documents, laws, etc.).	**The theoretical part** of the work is relevant to the topic and includes analysis and generalization but lacks a synthesis by the author. A minimum of 15 relevant research sources have been used. The work uses non-scientific sources relevant to the topic (general textbooks, manuals, documents, laws, etc.), but they do not dominate.	**The theoretical part** of the work is relevant to the topic, noticeably analytical and generalizing, and a connected complete text. More than 15 relevant scientific sources have been used, including international scientific sources. Non-scientific sources (general textbooks, manuals, documents, etc.) have not been used in the theoretical part of the work if it is not necessary based on the topic of the work. If these sources are used reasonably, their share	**The theoretical part** of the work is a topical, systematic, comprehensively analytical and generalizing, with a well-connected complete text. More than 15 relevant scientific sources have been used, including international scientific sources. Non-scientific sources (general textbooks, manuals, documents, etc.) have not been used in the theoretical part of the work if it is not necessary based on the topic of the work.

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
				does not exceed the share of scientific sources.	If these sources are used reasonably, their share does not exceed the share of scientific sources.
	Research methodology				
employ appropriate social science data collection and analysis methods	**The methodology part** slightly justifies the research process's data collection and data analysis methods When justifying the choice of methodology, reference is made to individual scientific methodology textbooks or teaching aids in the native language. With the selected research methods, it is possible to partially answer the research problem and achieve the goal of the work.	**The methodology part** in general terms justifies the research process's data collection and data analysis methods When justifying the choice of methodology, reference is made to several scientific methodology textbooks or teaching aids in the native language. With the chosen research methods, it is generally possible to answer the research problem and achieve the goal of the work.	**The methodology part** justifies the research process's data collection and data analysis methods When justifying the choice of methodology, reference is made to native language scientific methodology textbooks or teaching aids and individual international methodological scientific sources. With the chosen research methods, it is possible to answer the research problem and achieve the goal of the work.	**The methodology part** clearly justifies the research process's data collection and data analysis methods. When justifying the choice of methodology, mostly international methodological research sources are cited. The chosen research methods are appropriate to answer the research problem and achieve the purpose of the work.	**The methodology part** expertly justifies the research process's data collection and data analysis methods, analysing the suitability and limitations of the chosen methods. When justifying the choice of methodology, reference is made to international methodological scientific sources. The chosen research methods are the most suitable to answer the research problem and achieve the goal.

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
	Presentation and analysis of research results. Formulating the conclusion				
create a systematized and evidentiary solution to the problem	**Presentation of the results:** the research results are sometimes difficult to follow, as there is no clear structure and the use of well-thought-out illustrative tools (tables, figures, quotations, etc.). **Analysis of the results:** the work contains a small amount of analysis (interpretation) of the results and their association with theory. In general, the answers to the research problem, hypothesis(es) and/or research questions have been partially found. The goal of the work has been achieved. **Conclusions** and suggestions are weakly related to the results of the study.	**Presentation of the results**: the research results are generally traceable, though sometimes there is a lack of a clear structure and the use of well-thought-out illustrative tools (tables, figures, quotations, etc.). **Analysis of the results**: the work contains a small amount of analysis (interpretation) of the results and their relation to the theory. In general, the answers to the research problem, hypothesis(es) and/or research questions have been found. The goal of the work has been achieved. **Conclusions** and suggestions are partly related to the results of the study.	**Presentation of results:** the research results are traceable, and the use of illustrative tools (tables, figures, quotations, etc.) is well-thought-out. **Analysis of the results**: the work includes a comprehensive analysis of the results and their interpretation and relation to the theory. The answers to the research problem, hypothesis(es) and/or research questions have been found. The goal of the work has been achieved. **Conclusions** and suggestions are related to the results of the study and are applicable.	**Presentation of the results**: the research results are easy to follow, and the use of illustrative tools (tables, figures, quotations, etc.) is well-thought-out. **Analysis of results**: the paper includes a thorough analysis, interpretation, and application of the theory to the results, providing specific answers to the research problem, hypothesis(es) and/or research questions. The objective of the paper has been achieved. **Conclusions** and suggestions are clearly related to the results of the study and are applicable.	**Presentation of the results**: the research results are well-observable and systematically presented, and the use of illustrative tools (tables, figures, quotations, etc.) is skilfully thought out. **Analysis of the results**: the work includes a thorough analysis and interpretation of the results, associating them with theory and a critical approach, giving specific and logically argued answers to the research problem, hypothesis(es) and/or research questions. The goal of the work has been achieved. **Conclusions** and proposals are applied, clearly related to the results of the study, and contain, among other things, recommendations on the implementation of

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
					the results and further research directions.
	Formatting the essay				
present their research and proposed solutions in an argumentative and convincing manner, adhering to academic standards and practices	The length of the essay, from the introduction to the list of sources, is 35-40 pages. The essay mostly has a comprehensible structure, and the different parts of the work are partially connected. The format of the paper generally corresponds to the guidelines for the preparation and formalization of student papers. The sources used are cited, but there are several minor inaccuracies in the references and source entries. The sentence structure and spelling are mostly correct, but there are some errors. Non-scientific language is used throughout, but the work is generally comprehensible.	The length of the essay, from the introduction to the list of sources, is 35-40 pages. The essay has an understandable structure, and the different parts of the work are generally connected. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are cited, but there are a few minor inaccuracies in the references and source entries. The sentence structure and spelling are correct. In several places, non-scientific language is used, but the work is understandable.	The length of the essay, from the introduction to the list of sources, is 35-40 pages. The essay has an understandable structure, the parts of which are related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited, and the source entries are correct. The sentence structure and spelling are correct. The work is mostly written in scientific language, with non-scientific language used in some places.	The length of the essay, from the introduction to the list of sources, is 35-40 pages. The essay has an understandable and logical structure, the parts of which are clearly related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited, and the entries are correct. The sentence structure and spelling are correct. The work is written in scientific language.	The length of the essay, from the introduction to the list of sources, is 35-40 pages. The essay has an understandable and logical structure, the parts of which are clearly related to each other. The format of the paper corresponds to the guidelines for the preparation and formatting of student papers. The sources used are correctly cited, and the entries are correct. The sentence structure and spelling are correct. The work is written in very good scientific language.

Learning Outcomes	Grade E criterion Pass	Grade D criterion	Grade C criterion	Grade B criterion	Grade A criterion
	Defending				
present their research and proposed solutions in an argumentative and convincing manner, adhering to academic standards and practices	The defence speech has been presented within the specified time, and a general overview of the essay has been given. The presentation style is uncertain, and the slides are read off. The visually presented information is generally relevant and facilitates the understanding of the work, but it is sometimes difficult to follow. The Commission's questions have been answered partially comprehensibly and appropriately, but there are significant shortcomings.	The defence speech has been presented within the specified time, and an overview of the essay has been given. The presentation style is sometimes uncertain, and the slides are largely read off. The information presented visually is generally relevant and facilitates the understanding of the work/following of the defence speech. The Commission's questions have been generally answered in a comprehensible and appropriate way, but there are several shortcomings.	The defence speech has been presented within the specified time, and an overview of the essay has been given. The presentation style is confident. The information presented visually is relevant and facilitates the understanding of the work/following of the defence speech. The visually presented information is supplemented during the presentation. The Commission's questions have been answered comprehensibly and appropriately. The student demonstrates a good mastery of the topic and there are only a few minor deficiencies or inaccuracies.	The defence speech has been presented within the specified time, and a systematic overview of the essay has been given. The presentation style is confident and academic. The information presented visually is relevant and facilitates the understanding of the work/following of the defence speech. The visually presented information is supplemented during the presentation. The Commission's questions have been answered in a comprehensible, appropriate, and specific way. The student demonstrates versatile mastery of the subject	The defence speech has been presented within the specified time, and a systematic overview of the essay has been given. The presentation style is confident, academic, and convincing. The information presented visually is relevant and facilitates the understanding of the work/following of the defence speech. The visually presented information is freely supplemented during the presentation. The Commission's questions have been answered in a comprehensible, appropriate, and specific way. The student demonstrates versatile and systematic mastery of the subject.

ANNEX 2 Mandatory reading

Module 1. Phenomena of Hybrid Threats

Session 1. Hybrid threats: concept, definitions and wider interpretations

Bargués, P., Bourekba M., Colomina, C.(eds.) 2022, *Hybrid threats, vulnerable order* CIDOB *report # 08* CIDOB. Available from: https://www.cidob.org/en/publications/publication_series/cidob_report/cidob_report/hybrid_threats_vulnerable_order. [30 August 2023].

Cassam, Q., 2023, *Conspiracy Theories.* Soc 60, 190–199, 2023, Available from: https://link.springer.com/article/10.1007/s12115-023-00816-1. [3 January 2024].

Council of Europe (2016), *Legal challenges related to hybrid war and human rights obligations,* Committee on Legal Affairs and Human Rights, Rapporteur: Mr Boriss Cilevičs. Available from: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en [20 February 2024].

Countering Hybrid Threats 2022, Available from: https://defence-industry-space.ec.europa.eu/system/files/2022-03/Factsheet%20-%20Countering%20Hybrid%20Threats.pdf [21 February 2024].

Douglas, K. M., Sutton, R. M., 2023, *What are conspiracy theories? A definitional approach to their correlates, consequences, and communication*. Annual review of psychology, 74, 271-298, Available from: https://www.annualreviews.org/doi/abs/10.1146/annurev-psych-032420-031329. [24 January 2024].

European Commission 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats,* JOIN(2016) 18 final, 6 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 [20 February 2024].

European Commission 2020*, Identifying Conspiracy Theories.* Available from: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en. [12 January 2024].

Giannopoulos, G., Smith, H., Theocharidou, M. 2020, *The Landscape of Hybrid Threats: A Conceptual Model – Public Version*, (The European Commission and the European Centre of Excellence for Countering Hybrid Threats, 26 November 2020), Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305. [1 August 2023].

Heap, B. (ed.) 2019 Strategic Communications Hybrid Threats Toolkit. Applying the principles of NATO Strategic Communications to understand and counter grey zone threats. Nato Strategic Communications Centre of Excellence, p. 10. Available from: https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf [24 June 2024].

Hybrid CoE (2024), *Hybrid threats as a concept.* Available from: https://hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [20 February 2024].

Giannopoulos, G., Smith, H., Theocharidou, M. 2021, The Landscape of Hybrid Threats: A conceptual model, Publications Office of the European Union, Luxembourg. Available from: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [24 June 2024].

Sunstein, C. R., Vermeule, A., 2009, *Conspiracy theories: Causes and cures.* Journal of political philosophy, 17(2), 202-227 [online]. Available from: http://www.ask-force.org/web/Discourse/Sunstein-Conspiracy-Theories-2009.pdf [19 June 2023].

Uziębło, J. J. 2017, *United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats,* EU Diplomacy Papers 5/2017, College of Europe. Available from: https://www.coleurope.eu/sites/default/files/research-paper/edp-5-2017_uzieblo.pdf?download=1 [23 February 2024].

Session 2. Hybrid threats and security strategies

Bardhan, P., 2022. A World of Insecurity: Democratic Disenchantment in Rich and Poor Countries. Harvard University Press.

European Commission 2015, *The European Agenda on Security*, Communication No. COM(2015) 185 final, 28 April 2015. Available from: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52015DC0185 [24 February 2024].

European Commission 2020, *EU Security Union Strategy*, Communication No. 2020 COM(2020) 605 final, 24 July 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605 [24 February 2024].

European Council 2003, „A Secure Europe in a Better World" European Security Strategy, 12 December 2003. Available from: https://op.europa.eu/en/publication-detail/-/publication/d0928657-af99-4552-ae84-1cbaaa864f96/ [24 February 2024].

European Council 2010, *Internal security strategy for the European Union: Towards a European security model*, 25-26 March 2010, Available from: https://www.consilium.europa.eu/media/30753/qc3010313enc.pdf [24 February 2024].

Fukuyama, F., 2022. Liberalism and Its Discontents. Farrar, Straus and Giroux.

Šlapkauskas, V., 2022. Theoretical and Methodological Aspects of the Definition of, and Research into, Security of a Small State // Europe Alone: Small State Security without the United States / edited by Schultz D, Pūraitė A, Giedraitytė V. Lanham: Rowman & Littlefield International.

Session 3. Policy and regulation

Deppe, C. 2023, Disinformation in Cognitive Warfare, Fimi, Hybrid Threats. The Defence Horizon Journal. October 16, 2023. Available from: https://tdhj.org/blog/post/disinformation-cognitive-warfare-hybrid/ [30 June 2024].

European Commission 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM (2020) 605 final, pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [31 August 2023].

European Commission 2018, *Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats.* JOIN/2018/016 final. Document 52018JC0016, Available from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016 . [31 August 2023].

FAQ: Joint Framework on countering hybrid threats, 2016. Available from: https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250 [31 August 2023].

Fogt, M. 2021, 'Legal Challenges or "Gaps" by countering hybrid warfare – building resilience in jus ante bellum', *Southwestern Journal of International Law,* Vol. XXVII:1, Available from: https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf [25 February 2024].

Office of the United Nations High Commissioner for Human Rights 2008, Human Rights, Terrorism and Counter-terrorism. United Nations, Geneva. Available from: https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet32EN.pdf [30 June 2024].

Sari, A. 2020, Hybrid threats and the law: Concepts, trends and implications. Hybrid CoE Trend Report 3. April 2020. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Hybrid-CoE-Trend-Report-3.pdf [30 June 2024].

Session 4. Warfare in the context of hybrid threats

Adamsky, D. 2018, *From Moscow with coercion: Russian deterrence theory and strategic culture. The Journal of Strategic Studies*, Vol. 41, No. 1–2, pp. 33–60. Available from: https://doi.org/10.1080/01402390.2017.1347872 https://ir101.co.uk/wp-content/uploads/2018/10/adamsky-2018-from-moscow-with-coercion-russian-deterrence-theory-and-strategic-culture.pdf [30 June 2024].

Apetroe, A.C. 2016, Hybrid warfare: from "war during peace" to "neo-imperialist ambitions". The case of Russia. *Modelling the New Europe*. Issue No. 21, pp. 97-101. Available from: https://www.academia.edu/39885308/Online_journal_No_21_December [30 June 2024].

Clark, M. 2021, *The Russian military's lessons learned in Syria. Military learning and the future of war series.* Institute for the Study of War. January pp. 1-52. Available from: https://www.understandingwar.org/sites/default/files/The%20Russian%20Military's%20Lessons%20Learned%20in%20Syria_0.pdf [30 June 2024].

Coffey, L. 2019, How to Defeat Hybrid Warfare Before It Starts. *Defense One*, January 21, 2019. Available from: https://www.defenseone.com/ideas/2019/01/howdefeat-hybrid-warfare-it-starts/154296/. [30 June 2024].

Cordesman, A. H. 2020, Chronology of Possible Russian Gray Area and Hybrid Warfare Operations, *Center for Strategic and International Studies*, December 8, 2020, p. 15, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf. [30 June 2024].

Darczewska, J. 2014, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study.* May 2014. Centre for Eastern Studies Warsaw (OSW). Point of View, No 42, pp.1-26. Available from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf [30 June 2024].

Dobbs et al. 2020, *Grey-zone activities and the ADF*. A Perry Group Report. pp. 3-4. Available from: https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf). [30 June 2024].

Herta, L., M. 2016, Russia's hybrid warfare – why narratives and ideational factors play a role in international politics. *Modelling the New Europe*. 2016, Issue No. 21, pp.53-54. Available from: https://www.academia.edu/39885308/Online_journal_No_21_December . [30 June 2024].

Kravchenko, M. 2018, *Inventing Extremists. The Impact of Russian Anti-Extremism Policies on Freedom of Religion or Belief*. United States Commission on International Religious Freedom. Available from: https://www.uscirf.gov/sites/default/files/Inventing%20Extremists.pdf [30 June 2024].

Lele, A. 2014, Asymmetric Warfare: A state vs non-state conflict, *Oasis*, No 20, pp.97-111. Available from: https://www.redalyc.org/pdf/531/53163822007.pdf. [30 June 2024].

Leonaitė, E. & Žalimas, D. 2016, The Annexation of Crimea and Attempts to Justify It in the Context of International Law. *Lithuanian Annual Strategic Review. 2015-2016*. Volume 14. Military Academy of Lithuania. DOI: 10.1515/lasr-2016-0001.

Magnuson, S., Keay, M., Metcalf, K. 2022, Countering Hybrid Warfare: Mapping Social Contracts to Reinforce Societal Resiliency in Estonia and Beyond. *Texas National Security Review*. Volume 5, Issue 2 (Spring 2022). Available from: https://tnsr.org/wp-content/uploads/2022/01/TNSR-Vol-5-Issue-2-Magnuson-et-al.pdf. [30 June 2024].

Maternowski, C. & Malhotra, A. 2023, *Cutting through the Haze: Gray Zone Operations and Contemporary Threats*. The Canadian Army Journal. Available from: https://natoassociation.ca/wp-content/uploads/2023/08/Cutting-through-the-Haze-Summer-2023.pdf [30 June 2024].

Oates, S. 2016. Russian Media in the Digital Age: Propaganda Rewired. *Russian Politics*, *1*(4), 398-417. https://doi.org/10.1163/2451-8921-00104004.

Rácz, A. 2015, *Russia's hybrid war in Ukraine. Breaking the Enemy's Ability to Resist*. FIIA report No 43. 2015, The Finish institute on international affairs. pp. 1-101. Available from: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf [30 June 2024].

The Committee to Protect Journalists 2022, Understanding the Laws Relating to "fake news" in Russia. *Thomson Reuters Foundation*. Available from: https://cpj.org/wp-content/uploads/2022/07/Guide-to-Understanding-the-Laws-Relating-to-Fake-News-in-Russia.pdf [30 June 2024].

Uzman, G. 2017, Is hybrid warfare really new? Ankara Üniversitesi *SBF Dergisi*, 72(3). September 2017. pp. 525-540. Available from: https://dergipark.org.tr/tr/download/article-file/345212. [30 June 2024].

Session 5. Information warfare

Barclay, D. A., 2018, *Fake News, Propaganda, and Plain Old Lies: How to Find Trustworthy Information in the Digital Age*, Rowman & Littlefield.

Bhatti, A. M., Mehmood, N. 2024, American Strategic Narrative - A Success Story or an Archetypal Rhetoric, Routledge Open Research. Available from: https://routledgeopenresearch.org/articles/3-23 [5 June 2024].

Binder, J. F., & Kenyon, J., 2022, *Terrorism and the internet: How dangerous is online radicalization?*. *Frontiers in psychology*, 6639. Available from: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.997390/full?utm_source=Email_to_authors_&utm_medium=Email&utm_content=T1_11.5e1_author&utm_campaign=Email_publication&field&journalName=Frontiers_in_Psychology&id=997390. [14 November 2023].

Confucius Institutes 2019, *Hybrid Threats: Confucius Institutes*, NATO Strategic Communication Centre of Excellence, 6 June 2019. Available from: https://stratcomcoe.org/cuploads/pfiles/confucius_institutes.pdf. [20 June 2023].

European Commission, 2018, *Final report of the High Level Expert Group on Fake News and Online Disinformation*. Available from: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation [9 December 2023].

Darczewska, J. 2014, *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study.* Centre for Eastern Studies Warsaw. Point of View, No 42, pp.1-26. Available from: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf .[26 August 2023].

European Commission, 2019, *Action Plan Against Disinformation: Report on progress,* June 2019, Available from: https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf [26 August 2023].

Fedasiuk, R. 2022, *How China's united front system works overseas,* The Strategist, Australian Strategic Policy Institute, 13 April 2022. Available from: https://www.aspistrategist.org.au/how-chinas-united-front-system-works-overseas/. [20 June 2023].

Giles, K.; Sherr, J.; Seaboyer, A. 2018, *Russian reflexive control*. Royal Military College of Canada. pp.1-71. Available from: https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control. [29 August 2023].

Gunton, K., 2022, The Impact of the Internet and Social Media Platforms on Radicalisation to Terrorism and *Violent Extremism*. Privacy, Security and Forensics in The Internet of Things (IoT). Available from: https://books.google.lt/books?hl=lt&lr=&id=4n1fEAAAQBAJ&oi=fnd&pg=PA166&ots=nCVvihlRZS&sig=ez0z5QzZDZqCYLtFgHqfRMmzDlA&redir_esc=y#v=onepage&q&f=false [2 January 2024].

Kedem, M. 2023, Beyond Illusion | Addressing the Cybersecurity Impact of Deepfakes and Synthetic Media. *SentinelOne blog*. December 12, 2023. Available from: https://www.sentinelone.com/blog/beyond-illusion-addressing-the-cybersecurity-impact-of-deepfakes-and-synthetic-media/. [30 June 2024].

Läänemets, M. 2022, *China's Strategic Narratives and Soft Power Engagements as a Means of Influence*. Available from: https://assets.nationbuilder.com/menleuropa/mailings/1419/attachments/original/Geopol-report_China_final_22.03.2022.pdf?1649242620. [20 June 2023].

Nissen, T. E. 2016, *Social Media's Role in 'Hybrid Strategies'*. NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/cuploads/pfiles/tomas_nissen_article_12-09-2016.pdf. [30 June 2024].

Periodic insight 2022, *Disinformation narratives about the war in Ukraine,* No 14. 21/10/2022 to 22/11/2022. https://edmo.eu/wp-content/uploads/2022/07/Periodic-insight-n.14-Disinformation-narratives-about-the-war-in-Ukraine.pdf [31 September 2023].

Pomerantsev, P. & Weis, M. 2014, The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. *The Interpreter*, The Institute of Modern Russia, Available from: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf. [30 June 2024].

Posetti, J., Matthews, A., 2018, *A short guide to the history of 'fake news' and disinformation.* International Center for Journalists, 7(2018), 2018-07. Available from: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf [17 October 2023].

Prus, J. 2015, *Russia's Use of History as a Political Weapon*. Policy papers, No. 12 (114), p. 1-8. Available from: https://www.files.ethz.ch/isn/191038/PISM%20Policy%20Paper%20no%2012%20(114).pdf. [30 June 2024].

Roeder, O. 2018, *Why We're Sharing 3 Million Russian Troll Tweets*, FiveThirtyEight. Available from: https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/. [29 August 2023].

Thiele, R. 2020, *Artificial Intelligence – A key enabler of hybrid warfare*. Hybrid CoE Working Paper 6. March 2020. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf. [30 June 2024].

Session 6. Common response to hybrid threats and strategies for tackling them

Aho, A., et al., 2023, Hybrid threats: A comprehensive resilience ecosystem. April 20, 2023. The European Centre of Excellence for Countering Hybrid Threat Available from: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ [28 June 2024].

European Commission. 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM(2020) 605 final,27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [14 July 2022].

European Commission, 2023, *Communication from Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and Committee of the Regions. Towards a more resilient, competitive and sustainable Europe* COM/2023/558 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0558&qid=1708862129657 [10 February 2024].

European Union, 2022, *Countering Hybrid Threats,* European Union, March 2022. Available from: https://www.eeas.europa.eu/sites/default/files/documents/2022-03-28-countering-HybridThreats_NewLayout.pdf [3 September 2023].

Hybrid threats: a comprehensive resilience ecosystem, 2023, Publications Office of the European Union, Luxembourg, doi:10.2760/37899. Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf [12 September 2023].

Keršanskas, V., 2020, Deterrence: Proposing a more strategic approach to countering hybrid threats. The European Centre of Excellence for Countering Hybrid Threat. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf [28 June 2024].

Monaghan, S., 2022, Hybrid CoE Paper 12: Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. March 31, 2022. The European Centre of Excellence for Countering Hybrid Threat. Available from: https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/ [28 June 2024].

Sanz-Caballero, S. , 2023, *The concepts and laws applicable to hybrid threats, with a special focus on Europe*. Humanit Soc Sci Commun 10, 360, 2023. Available from:. https://doi.org/10.1057/s41599-023-01864-y [3 Febuary 2024].

Session 7. Research strategies and methods

ASA 2021, *Ethical guidelines for good research practice*. Association of Social Anthropologists of the UK (ASA). https://www.theasa.org/ethics/

Šlapkauskas, V & Zuzevičiūtė, V. 2022, Between Security and Safety - Outlines for the Contours of Research in Search of a Holistic Approach // Europe Alone : Small State Security without the United States / edited by David Schultz, Aurelija Pūraitė, Vidmantė Giedraitytė. Lanham: Rowman & Littlefield International, Chapter 18. ISBN 9781538167281. eISBN 9781538167298. p. 403-422.

Module 2. Prevention and Cooperation in Countering Hybrid Threats

Session 1. Crimes of a hybrid nature

Aleksi Aho; Catarina Midões; Arnis Šnore., 2020, Hybrid threats in the financial system, Hybrid CoE Working Paper 8, Hybrid CoE, Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf. [3 February 2025].

Bachmann, S.D. and Gunneriusson, H., 2014. Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global risk and security. *The Journal on Terrorism and Security Analysis*.

Communication from the Commission to the European parliament, the European council, the Ccouncil, the European economic and social committee and the Committee of the regions on the EU security union strategy, COM/2020/605 final, Bruxelles, 24.7.2020.

Council decision (EU, Euratom) 2020/2053, of 14 December 2020 on the system of own resources of the European Union and repealing Decision 2014/335/EU Euratom, Official Journal of the European Union L 424/1, 15.12.2020

Consolidated version of The treaty on European Union, Official Journal of the European Union C 202/13, 7.6.2016.

Consolidated version of The treaty on the functioning of the European Union, Official Journal of the European Union C 202/47, 7.6.2016.

European Commission 2023, *Joint Communication to the European Parliament, the Council and the European Economic and Social Committee on the fight against corruption.* JOIN(2023)12 final. Available from: https://commission.europa.eu/document/download/b6888f6a-45ed-4af7-b85a-6712dfe8952c_en?filename=JOIN_2023_12_1_EN.pdf. [1 February 2024].

European Commission 2023, *Proposal for a directive of the European Parliament and of the Council on combating corruption, replacing Council Framework Decision 2003/568/JHA and the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and amending Directive (EU) 2017/1371 of the European Parliament and of the Council.* COM (2023) 234 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0234. [1 February 2024].

European Commission 2020a, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.* COM (2020) 605 final, pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [13 January 2024].

European Commission 2020b, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.* COM(2020)

795 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795. [13 January 2024].

European External Action Service 2023, *Missions and Operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

European External Action Service 2022, *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security*. Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en. [20 September 2023].

European Parliament and the Council of the European Union 2021, *Regulation (EU) 2021/784 of the European Parliament and of the Council* of *29 April 2021on addressing the dissemination of terrorist content online.* (OJL 172, 17.5.2021). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784. [13 January 2024].

European Parliament and the Council of Europe 2022, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065 [13 January 2024].

European Union Agency for Fundamental Rights 2021, *Report. Directive (EU) 2017/541 Combatting Terrorism. Impact on Fundamental Rights and Freedoms. Luxembourg: Publications Office of the European Union.* Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-directive-combating-terrorism_en.pdf. [13 January 2024].

Europol 2023, *European Union Terrorism Situation and Trend Report*. Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

Faleg, G (ed) 2022, *The EU's Civilian Headquarters: Inside the control room of civilian crisis management*. European Union Institute for Security Studies EUISS, Chaillot Paper 175, Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/eus-civilian-headquarters. [10 September 2023].

Huss, O, Beke, M, Wynarski, J, & Slot, B 2023, *Handbook of good practices in the fight against corruption.* Publications Office of the European Union. doi:10.2837/575157.

Informal Ecofin, 2019. *Resilience of financial market infrastructure and the role of the financial sector in countering hybrid threats,* EU2019.FI Available from: https://valtioneuvosto.fi/documents/11707387/15400298/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf/29565728-f476-cbdd-4c5f-7e0ec970c6c4/Hybrid+Threats+Informal+ECOFIN+final+Issues+Note+2019-09-09_S2.pdf. [3 February 2025].

Institute for Economics & Peace 2024, *Global Terrorism Index 2024: Measuring the Impact of Terrorism*, Sydney. Available from: http://visionofhumanity.org/resources. [26 February 2024].

Johnson III, B.M., 1992, Executive Order 12,333: The permissibility of an American assassination of a foreign leader. *Cornell Int'l LJ*, 25, p.401.

Lakhani, S, White, J & Wallner, C 2022, *The gamification of (violent) extremism. An exploration of emerging trends, Future threat scenarios and potential P/CVE solution,.* Luxembourg: Publications, Office of the European Union. Available from: https://home-affairs.ec.europa.eu/system/files/2022-09/RAN%20Policy%20Support-%20gamification%20of%20violent%20extremism_en.pdf. [13 January 2024].

MacLachlan, K 2019, *Corruption as Statecraft.* s.l.: Transparency International.

Missiroli, A., 2024, From hybrid warfare to'cybrid'threats-and back? Concepts, challenges, responses. In *Addressing Hybrid Threats* (pp. 40-56). Edward Elgar Publishing.

Pisoiu, D & Renard, T 2022, *Responses to returning foreign terrorist fighters and their families*, RAN Manual, 2nd Edition, Radicalisation Awareness Network. Available from: https://home-affairs.ec.europa.eu/document/download/7cbeded1-383c-4b58-b74b-88ececeb93f0_en?filename=ran_manual_responses_returning_foreign_terrorists_and_their_families_en.pdf. [13 January 2024].

Ranstrop, M 2019, *Islamist Extremism. Practical Introduction, RAN Factbook,* RAN Centre of Excellence.

Schmitt, M.N., 1992, State-sponsored assassination in international and domestic Law. *Yale J. Int'l L.*, 17, p.609.

Sternkenburg, N 2019, *Far-right extremism. Practical introduction. RAN Factbook,* The RAN Centre of Excellence. Available from: https://home-affairs.ec.europa.eu/system/files/2019-12/ran_fre_factbook_20191205_en.pdf. [13 January 2024].

Zengel, P., 1991, Assassination and the law of armed conflict. *Mil. L. Rev.*, 134, p.123.

Session 2. International criminal law and legal tools for tackling hybrid threats

Council Decision 2014/145/CFSP of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. Available from: https://eur-lex.europa.eu/eli/dec/2014/145(1)/oj. [11.December 2024.]

Dinstein, Y., 2017, *War, aggression and self-defence*. Cambridge University Press.

Hufbauer, G.C., Schott, J.J., Elliott, K.A. and Oegg, B.,2010, *Economic sanctions: New directions for the 21st century*. Peerson Institute for International Economics.

Johnson, L. D. 2022, United Nations Response Options to Russia's Aggression: Opportunities and Rabbit Holes, *Just Security*, 1.

Kempees, P., 2021., *Hard Power' and the European Convention on Human Rights*. International Studies in Human Rights. Brill.

Piper, D.C. 1972, The Legal Control of the Use of Force and the Definition of Aggression. *Ga. J. Int'l & Comp. L.*, 2, p.1.

Ruys, T. 2010, *'Armed attack'and Article 51 of the UN Charter: evolutions in customary law and practice* (Vol. 74). Cambridge University Press.

Sari, A. 2020, *Hybrid threats and the law: Concepts, trends and implications*. Hybrid Centre of Excellence Trend Report, 3.

Vasiliev, S. 2022, Aggression against Ukraine: Avenues for Accountability for Core Crimes, EJIL:Talk, 3 March 2022.

Session 3. Prevention of hybrid threats

European Union Agency for Cybersecurity (ENISA) 2020, *Threat landscape for cybersecurity 2020*. Available from: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020. [4 April 2024].

Ganguly, A, R, Bhatia, U, Flynn, S, E 2018, *Critical infrastructures resilience: Policy and engineering principles,* Routledge, New York.

Hurst, W & Shone, N 2024, Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation, Title of host publication Management and Engineering of Critical Infrastructures, Academic Press, Cambridge, pp. 265-286.

Institute for Security Governance, Naval Support Activity Monterey 2018, *Comprehensive approach to countering hybrid threats,* Available from: https://instituteforsecuritygovernance.org/documents/113018911/119118404/P319283_EM%26R_Comprehensive+Approaches+to+Counter+Hybrid+Threats.pdf/d8c4e29b-6a28-95b1-f3fc-333c438c88e2?t=1617292238514. [22 April 2024].

Lerner, J S, Li, Y, Valdesolo, P & Kassam, K S 2015, 'Emotion and decision making', Annual Review of Psychology, vol. 66, pp. 79-823. Available from: Emotion and Decision Making | Annual Reviews. [28 April 2024].

Matlary, J H 2015, *Resilience as a strategic concept*, Routledge, London.

Nelson, A, Rekhi, S, Souppaya, M & Scarfone, K 2024, *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 Community Profile*, NIST Special Publication 800-61 Revision 3 2024. Available from: https://csrc.nist.gov/pubs/sp/800/61/r3/ipd. [28 April 2024].

Session 4. Cybersecurity and cyber incident management

Anderson, R & Moore, T 2009, 'Information security: Where computer science, economics, and psychology meet', *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, vol. 367, no. 1898, pp. 2717-2727.

Cichonski, P, Millar, T, Grance, T & Scarfone, K 2016, *Computer security incident handling guide*, National Institute of Standards and Technology, Special Publication 800-61, Revision 2. Available from: Computer Security Incident Handling Guide (nist.gov). [02 April 2024].

Christou, G 2016, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, London.

Libicki, M C, Ablon, L & Webb, T 2015, *The defenders dilemma: Charting a course toward cyber security*, RAND Corporation, Santa Monica.

National Intelligence Council 2012, Global trends 2030: *Alternative worlds. National Intelligence Council*. Available from: Global trends 2030: alternative worlds - Atlantic Council. [2 April 2024].

Taddeo, M & Floridi, L 2021, *The Debate on the Moral Responsibilities of Online Service Providers, Centre of Digital Ethics*. Available from: The Debate on the Moral Responsibilities of Online Service Providers by Mariarosaria Taddeo, Luciano Floridi :: SSRN. [2 April 2024].

United Nations System 2013, *United Nations plan of pction on disaster risk reduction for resilience*, New York, USA. Available from: https://www.preventionweb.net/files/33703_actionplanweb14.06cs1.pdf. [23 April 2024].

Universal Declaration of Human Rights, Article 19. Available from: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf. [4 April 2024].

Session 5. International cooperation

Bertolini, M., Minicozzi, R., Sweijs, T. 2023, *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies, pp. 10-13, 17-18. Available from: https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/. [17 January 2025].

Billing, F., Feldtmann, B. 2024, *The Role of Criminal Law Approaches Against Hybrid Attacks*, Bergen Journal of Criminal Law and Criminal Justice, Volume 12, Issue 2, pp. 2-3, 6, 18-19, 21-22, 24. Available from: https://boap.uib.no/index.php/BJCLCJ/article/view/4440. [23 January 2025].

Bratko, A., Zaharchuk, D., Zolka, V. 2021, *Hybrid warfare – a threat to the national security of the state*. Revista de Estudios en Seguridad Internacional, Vol. 7, No. 1, pp. 151, 152, 158. Available from: http://dx.doi.org/10.18847/1.13.10. [12 December 2024].

Brown, C. S. D. 2015, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, International Journal of Cyber Criminology, Vol 9 Issue 1 January – June, pp. 65-66, 86, 97. Available from: https://zenodo.org/records/22387. [20 January 2025].

Convention on Cybercrime Budapest, 23.XI.2001. Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention. [23 January 2025].

Council of the European Union 2022, *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security. Available from: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.* [14 January 2024].

European Commission 2018, *Joint communication to the European Parliament and the Council, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018JC0016. [14 January 2024].

European Commission 2016, *Joint Framework on countering hybrid threats - a European Union response.* JOIN/2016/018 final. Document 52016JC0018, p. 2. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [12 December 2024].

European Commission 2020, *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN (2020) 18 final, p. 4. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [6 December 2024].

Gaiser, L. 2019, *Nato - EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework*. National Security and the Future, 20(1-2), pp. 17-18, 20. Available from: https://hrcak.srce.hr/231815. [13 December 2024].

Khmyrov, I., Khriapynskyi, A., Aliieva, P., Kopotun, I., Svoboda, I. 2024, *International experience of advanced countries in state management of countering hybrid threats*. № 36. Universidade Portucalense, Porto, pp. 373-377. Available from: https://revistas.rcaap.pt/juridica/article/view/36758. [12 December 2024].

Laitinen, M., Armstrong-Smith, S. 2022, *Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations*. Cyber Security: A Peer-Reviewed Journal Vol. 5, 3, pp. 190, 196-197, 202-203. Available from: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.henrystewartpublications.com/sites/default/files/CSJ5.3Tackling%20cybercrime%20and%20ransomware%20headonDisrupting%20criminal%20networks%20and%20protecting%20organisations.pdf. [20 January 2025].

Oancea, R., Gligorea, I., Raţiu, A., Dragomir, I. 2024, *Cybersecurity*, in: *Hybrid Warfare Reference Curriculum*, Volume I, Compulsory Lectures, Edited by Zoltán Jobbágy – Edina Zsigmond, Ludovika University Press, Budapest, 2024, pp. 149-150. Available from: https://csnsc.uk/hybrid-warfare-reference-curriculum-volume-i/. [6 December 2024].

Olech, A. K. 2021, *Cooperation between NATO and the European Union against hybrid threats with a particular emphasis on terrorism*. Instytut Nowej Europy, pp. 2-3, 7. Available from: https://ine.org.pl/en/cooperation-between-nato-and-the-european-union-against-hybrid-threats-with-a-particular-emphasis-on-terrorism/. [12 December 2024].

Wigell, M., Mikkola, H., Juntunen, T. 2021, *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament Coordinator: Policy Department for External Relations Directorate General for External Policies of the Union PE 653.632. May 2021, pp. 1, 4. Available from: http://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf. [12 December 2024].

Module 3. Increasing resilience and bolstering societal and institutional capabilities to hybrid threats

Session 1. Common resilience-building approach against hybrid threats

Council of Europe, 2023, REYKJAVÍK DECLARATION - United around our values. p.p. 7, 10, 15. Available from: https://rm.coe.int/4th-summit-of-heads-of-state-and-government-of-the-council-of-europe/1680ab40c1. [12 December 2024].

Council of the European Union, 2022, How the EU responds to crises and builds resilience, Available from: https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/, [03 December 2024].

European Commission, 2018a, *Communication from the commission to the European Parliament, the council, the European economic and social Committee and the committee of the regions*. *Tackling online disinformation: a European Approach. p.p. 3-16.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236. [15 December 2024].

European Commission, 2018b, *Joint communication to the European Parliament, the European council, the council, the European economic and Social committee and the committee of the regions. Action Plan against Disinformation*. p.p. 1-12. Available from: https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf. [15 December 2024].

European Commission, Directorate-General for Communications Networks, Content and Technology 2018, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office of the European Union. Available from: https://data.europa.eu/doi/10.2759/739290. [12 July 2024].

European Commission, 2016, *Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response,* JOIN/2016/018 final. p. 3-17. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [15 December 2024].

European Parliament, 2022, *Foreign interference in all democratic processes in the European Union. European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)*. p.p. 13. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022IP0064. [12 December 2024].

European Parliament, 2021, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf, [27 December 2024].

Fiott, D. and Parkes, R., 2019, *Protecting Europe: The EU's Response to Hybrid Threats*. EU Institute for Security Studies.

Giannopoulos, G., Smith, H., Theocharidou, M. 2021, *The Landscape of Hybrid Threats: A conceptual model*, EUR 30585 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. p.p. 11. Available from: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf. [10 December 2024].

Hybrid CoE, *Frequently asked questions on hybrid threats*. p.p. 1-2. Available from: https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf. [12 December 2024].

OSCE, UN, OAS, ACHPR, 2017, *Joint declaration on freedom of expression and "fake news", disinformation and propaganda*. p.p. 1-5. Available from: https://www.osce.org/files/f/documents/6/8/302796.pdf. [12 December 2024].

Smith, B. Lannes, 2024, *"Propaganda"*, Encyclopedia Britannica. Available from: https://www.britannica.com/topic/propaganda [10 December 2024].

Session 2. Fostering the resilience of the state and non-state actors to hybrid threats

Cusumano, E & Corbe, M 2017, *A Civil-Military Response to Hybrid Threats*. Available from: https://link.springer.com/book/10.1007/978-3-319-60798-6. [15 December 2024].

Directive (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). pp. 64-70. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555. [15 December 2024].

Directive (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. pp. 171-176, 182-187.

Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557. [15 December 2024].

ENISA, 2017, *Public Private Partnerships (PPP), Cooperative models.* pp. 7, 11-14. Available from: https://op.europa.eu/hr/publication-detail/-/publication/597dee0f-2285-11e8-ac73-01aa75ed71a1. [20 December 2024].

EUCPN 2019, Policy on Community-oriented policing in the EU. Brussels. Avalabe at: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://eucpn.org/sites/default/files/document/files/POLICY%20PAPER%202019%20COP_ENG_LR.pdf. [December 30 2024].

European Commission, 2020, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS* on the EU Security Union Strategy, pp. 6-7. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605, [15 December 2024].

European Commission, 2023, Proposal for a COUNCIL RECOMMENDATION on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance, COM/2023/526 final. pp. 8-9,11-15. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023DC0526. [15 December 2024].

European Parliament, 2023, *SECURITY IMPLICATIONS OF CHINA-OWNED CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION*, pp. 8, 15-19. Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf. [12 December 2024].

Hufnagel, S., 2015, Transnational Policing and Regulation: The Effect of Shared Fundamental Rights on the Formalisation of Cross-Border Police Cooperation. *EJPS*, p.204.

Hybrid CoE, *Frequently asked questions on hybrid threats*. pp. 1-2. Available from: https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf. [12 December 2024].

Juntunen, T., Wigell, M. & Mikkola, H., 2021, Best Practices in the whole-of-society approach in countering hybrid threats. Available at: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632. [December 30 2024].

Linkov, I. and Trump, B., 2019, *The Science and Practice of Resilience*. New York: Springer International.

Niinistö, S 2024, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness Report*. Available from: https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf. [2 December 2024].

OECD 2019, *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris., pp. 14-17, 50-56. Available from: *https://doi.org/10.1787/02f0e5a0-en*. [20 December 2024].

Sanz-Caballero, S., 2023, The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanit Soc Sci Commun 10, 360. Available at: https://doi.org/10.1057/s41599-023-01864-y. [December 30 2024].

Sučić, I. & Karlović, R., 2017, Community policing in support of social cohesion Community. In: Bayerl et.al. Policing - A European Perspective: Strategies, Best Practices and Guidelines. Cham: Springer. 7-20.

Session 3. Protection of critical infrastructure

MANDATORY READING

Council of the European Union 2022, *Council recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure – Adoption,* 15454/22. Available from: https://data.consilium.europa.eu/doc/document/ST-15454-2022-INIT/en/pdf. [4 April 2024].

European Commission 2023*, Hybrid threats. A comprehensive resilience ecosystem.* Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf?cv=1. [4 April 2024].

Liang, Q & Xiangsui, W 2020, *Unrestricted warfare: China's master plan to destroy America*, Albatross Publishers, Prague, Czech Republic.

Singer, P W & Brooking, E T 2018, *Likewar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, Massachusetts, US.

Module 4. Management and Leadership in the Context of Hybrid Threats and Hybrid Crises

Session 1. European Union's external dimension in countering hybrid threats

Council Conclusions 2022, *Council conclusions on a Framework for a coordinated EU response to hybrid campaigns*. Available from: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/. [10 October 2023].

European External Action Service 2023, *Missions and Operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

European External Action Service 2022, *A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security*.

Available from: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en. [20 September 2023].

European External Action Service 2021, *Crisis management and response*. Available from: https://www.eeas.europa.eu/eeas/crisis-management-and-response_en. [25 October 2023].

European Council 2022, *How the EU responds to crises and builds resilience*. Available from: https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/. [20 October 2023].

Faleg, G (ed) 2022, *The EU's Civilian Headquarters: Inside the control room of civilian crisis management*. European Union Institute for Security Studies EUISS, Chaillot Paper 175, Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/eus-civilian-headquarters. [10 September 2023].

North Atlantic Treaty Organisation 2023, *Eighth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*. Available from: https://www.nato.int/cps/en/natohq/official_texts.htm?keywordquery=EU-NATO%20relations&search=true. [2 September 2023].

Permanent Structured Cooperation 2023, *Permanent Structured Cooperation*. Available from: https://www.pesco.europa.eu/. [25 October 2023].

Rehrl, J (ed) 2021, *Handbook on CSDP. The Common Security and Defence Policy of the European Union*. 4th Ed. Federal Ministry of Defence of the Republic of Austria.

Rühle, M & Roberts, C 2021, *Enlarging NATO's toolbox to counter hybrid threats*. Available from: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html. [16 October 2023].

Zandee, D, van der Meer, S & Stoetman, A 2022, *Countering hybrid threats: Steps for improving EU-NATO cooperation,* Clingendael Report, Netherlands Institute of International Relations. Available from: https://www.clingendael.org/pub/2021/countering-hybrid-threats/. [2 September 2023].

Session 2. Border and security management

Council of the European Union 2009, Updated EU Schengen Catalogue *External borders Control Return and readmission Recommendations and best practices* (7864/09), pp. 13-15. Available from: https://data.consilium.europa.eu/doc/document/ST-7864-2009-INIT/en/pdf. [10 March 2023].

European Commission 2016, *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response.* JOIN/2016/018 final, Document 52016JC0018, p. 2. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [21 January 2023].

European Commission 2020, *Communication from the Commission to the European Parliament, the European Council, the council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strateg,* COM(2020) 605 final,

pp. 1, 6, 15-16, 27. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from =EN. [13 December 2022].

European Commission 2022, *Developing a multiannual strategic policy for European integrated border management in accordance with Article 8(4) of Regulation (EU) 2019/1896. Policy document,* COM (2022) 303 final*,* Article 3. Available from: EUR-Lex - 52022DC0303 - EN - EUR-Lex (europa.eu). [21 November 2022].

European Commission 2023, *Communication from the Commission to the European Parliament and the Council establishing the multiannual strategic policy for European integrated border Management*. COM(2023) 146 final. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:f7b5247b-c296-11ed-a05c-01aa75ed71a1.0001.02/DOC_1&format=PDF [11 April 2023].

European Commission 2023, *Annexes to the Communication from the Commission to the European Parliament and the Council establishing the multiannual strategic policy for European integrated border Management*. COM(2023) 146 final*.* Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0146&from=EN [11 April 2023].

European Commission 2024, *Managing migration responsibly*. Available from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/story-von-der-leyen-commission/managing-migration-responsibly_en. [27 August 2024].

European Parliament 2024, Legislative train 05.2024. Available from: https://www.europarl.europa.eu/legislative-train/carriage/revision-of-the-schengen-borders-code/report?sid=8101. [27 August 2024].

European Parliament and the Council of the European Union 2019, *Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624*, Recitals 1-5, 9-57, Article 3. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN. [27 January 2023].

Official Journal of the European Union 2016*, Consolidated versions of the Treaty on European Union and the Treaty on the functioning of the European Union*, (2016/C 202/01), pp. 29-32. **Available from:** https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b49701aa75ed71a1.0006.01/DOC_3&format=PDF. [10 March 2023].

Punda Y, Shevchuk V & Veebel V 2019, 'Is the European migrant crisis another stage of hybrid war?', *Sõjateadlane (Estonian Journal of Military Studies)*, vol. 13, pp. 116–119. Available from: https://www.kvak.ee/sojateadlane/. [26 August 2024].

Session 3. Countering information advocacy and influence activities

Daukšas, V., Fridman, O., Urbanavičiūtė, K., Venclauskienė, L. 2024, *War on All Fronts: How the Kremlin's Media Ecosystem Broadcasts the War in Ukraine*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/war-on-all-fronts-how-the-kremlins-media-ecosystem-broadcasts-the-war-in-ukraine/301. [27 August 2024].

Hodos, P. N. 2022, *Playing to Extremes: Russia's Choices to Support Western Political Extremists and Paramilitary Groups*. International Journal of Intelligence and CounterIntelligence. https://doi.org/10.1080/08850607.2022.2109449. [27 August 2024].

Jokinen, J., Normark, M. & Fredholm, M. 2022, *Hybrid threats from non-state actors: A taxonomy*. Hybrid CoE Research Report No. 6 (June 2022). Available from: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-6-hybrid-threats-from-non-state-actors-a-taxonomy/. [27 August 2024].

Monaghan, S. 2022, *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice*. Hybrid CoE Paper No. 12 (March 2022). Available from: https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/. [27 August 2024].

Session 4. Management and leadership in the context of hybrid challenges

Clegg, S, Crevani, L, Uhl-Bien, M, Todnem, R 2021, 'Changing leadership in changing times', *Journal of Change Management*, vol 21 no. 1, pp. 1-13. Available from: https://doi.org/10.1080/14697017.2021.1880092 [7 September 2023].

Deverell, E & Olsson E-K 2010, 'Organizational culture effects on strategy and adaptability in crisis management', *Risk Management*, vol. 12, no. 2, pp. 116-134. Available from: https://link.springer.com/article/10.1057/rm.2009.18. [24 November 2023].

Fagerberg, J 2009, *Innovation: A Guide to the Literature*, The Oxford Handbook of Innovation, Oxford Academic. Available from: https://doi.org/10.1093/oxfordhb/9780199286805.003.0001. [27 November 2023].

Hoffjann, O 2022, 'Between strategic clarity and strategic ambiguity – oscillating strategic communication', *Corporate Communications: An International Journal*, vol. 27, no. 2, pp. 284-303. Available from: https://doi.org/10.1108/CCIJ-03-2021-0037. [30 November 2023].

Maak, T, Pless, N.M, Wohlgezogen, F 2021, 'The fault lines of leadership: Lessons from the global Covid-19 Crisis', *Journal of Change Management*, vol. 21, no. 1, pp. 66-86. Available from: https://doi.org/10.1080/14697017.2021.1861724. [9 September 2023].

McAuliffe, D & Chenoweth, L 2008, 'Leave no stone unturned: The inclusive model of ethical decision making', *Ethics and Social Welfare*, vol. 2, no. 1, pp. 38-49. Available from: http://dx.doi.org/10.1080/17496530801948739. [10 September 2023].

McKinsey & Company 2022, *What is diversity, equity, and inclusion?*. Available from: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-diversity-equity-and-inclusion. [8 September 2023].

Moilanen, T & Salminen, A 2006, *Comparative study on the public-service ethics of the EU member states. A report from the Human Resources Working Group EUPAN*. Available from: https://vm.fi/documents/10623/307711/Comparative_Study_on_the_Public_Service_Ethics_of_the_EU

_Member_States_publication+131206.pdf/524e908b-5388-4d1c-9199-59b4f3e567a9/Comparative_Study_on_the_Public_Service_Ethics_of_the_EU_Member_States_publication+131206.pdf. [7 September 2023].

Verhage A, Noppe J, Feys, Y & Ledegen, E 2018, 'Force, stress, and decision-making within the Belgian police: the impact of stressful situations on police decision-making', *Journal of Police and Criminal Psychology*, vol. 33. Available from: https://doi.org/10.1007/s11896-018-9262-4. [5 December 2023].

ANNEX 3 Recommended reading

Module 1. Phenomena of Hybrid Threats

Session 1. Hybrid threats: concept, definitions and wider interpretations

Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. 2019, *Hybrid Threats. A Strategic Communications Perspective*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/pdfjs/?file=/publications/download/2nd_book_short_digi_pdf.pdf?zoom=page-fit [24 June 2024].

Bajarūnas, E., Keršanskas, B. 2018, *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome.* Lithuanian Annual Strategic Review, Volume 16, Issue 1 (pp. 123–170). https://doi.org/10.2478/lasr-2018-0006 Available from: https://journals.lka.lt/journal/lasr/article/152/info. [1 August 2023].

Bekkers, F., Meessen, R., Lassche, D. 2019, *Hybrid Conflicts: the New Normal?* TNO: Innovation for Life. Available from: https://www.tno.nl/publish/pages/7427/tno-2019-hybride.pdf [20 February 2024].

Berdal, M. 2011, The "New Wars'" Thesis Revisited. *The Changing Character of War*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:osobl/97801 99596737.003.0007. [24 June 2024].

Butter, M., 2020, *„Conspiracy theories in films and televisions shows",* Available from: https://tobias-lib.ub.uni-tuebingen.de/xmlui/bitstream/handle/10900/121641/Butter.%20Conspiracy%20Theories%20in%20Films%20and%20Television%20Shows.pdf?sequence=1&isAllowed=y. [22 November 2023].

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., Deravi, F., 2019, *Understanding conspiracy theories.* Political psychology, 40, 3-35 [online]. Available from: https://onlinelibrary.wiley.com/doi/full/10.1111/pops.12568. [12 July 2023].

Hanssen, M. (2018). Russian Hybrid Warfare: A Study of Disinformation. *Journal of Strategic Studies*. Available from: https://css.ethz.ch/en/services/digital-library/articles/article.html/1c93c122-e11f-45d4-afde-c5e17a3185fb. [24 June 2024].

Räikkä, J., 2018, *Conspiracies and conspiracy theories: An introduction*. Argumenta, 6, 1-12 [online]. Available from: https://www.argumenta.org/wp-content/uploads/2018/05/1-Argumenta-Juha-Ra%CC%88ikka%CC%88-Conspiracies-and-Conspiracy-Theories.pdf. [10 July 2023].

Sanz-Caballero, S. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, vol. 10, 360. Available from: https://www.nature.com/articles/s41599-023-01864-y. [1 February 2024].

United Nations Secretary-General 2019, *Developments in the field of information and telecommunications in the context of international security*. Report No. A/74/120, 24 June 2019. Available from: https://digitallibrary.un.org/record/3814154?ln=en [20 February 2024].

NATO 2016, *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.* Available from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [22 February 2024].

NATO 2018, *Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018*. Available from: https://www.nato.int/cps/en/natohq/official_texts_156624.htm [22 February 2024].

Session 2. Hybrid threats and security strategies

Bauman, Z., 2017. A Chronicle of Crisis: 2011–2016. Social Europe Editions.

Bauman, Z., 2001. Community. Seeking Safety in an Insecure World. Cambridge: Polity.

Berger, P. L., Luckmann, Th., 2011. The Social Construction of Reality. A Treatise in the Sociology of Knowledge. Open Road Media.

Buzan, B., 2008. People, States and Fear: An Agenda for International Security studies in the Post-Cold War Era. ECPR Press.

Bauman, Z., Donskis, L., 2013. The Loss of Sensitivity in Liquid Modernity. Cambridge: Polity.

Bergson, H., 2006. The Two Sources of Morality and Religion. Macmillan and Company Limited.

Countering Hybrid Threats (2022), Available from: https://defence-industry-space.ec.europa.eu/system/files/2022-03/Factsheet%20-%20Countering%20Hybrid%20Threats.pdf [21 February 2024].

Durkheim, E., 2011 [1925], Moral Education. Translated by E. K. Wilson and H. Schnurer. Mineola, New York: Dover Publications.

Durkheim, E., 1993 [1893], The Division of Labour in Society. Translated by G. Simpson. New York: The Free Press.

European Commission 2016, Joint Framework on countering hybrid threats. A European Union response, Communication No. JOIN(2016) 18 final, 6 April 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [24 February 2024].

European Commission 2017, Action Plan to support the protection of public spaces, Communication No. COM(2017) 612 final, 18 October 2017. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0612. [24 February 2024].

European Commission 2018, Increasing resilience and bolstering capabilities to address hybrid threats, Communication No. JOIN(2018) 16 final, 13 June 2018. Available from: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016. [24 February 2024].

European Commission 2020b, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, Communication No. COM/2020/795 final, 9 December 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1631885972581&uri=CELEX%3A52020DC0795. [24 February 2024].

European Commission 2021, The EU Strategy to tackle Organised Crime 2021-2025, Communication No. COM(2021) 170 final, 14 April 2021. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1670427706474 [24 February 2024].

European Commission, High Representative of the Union for Foreign Affairs and Security Policy 2020) The EU's Cybersecurity Strategy for the Digital Decade. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [24 February 2024].

Etzioni. A. 2004, From Empire to Community: A New Approach to International Relations. New York: Palgrave Macmillan.

Gauvain, M., 2013, Sociocultural Contexts of Development. In Philip David Zelazo (Ed.). The Oxford Handbook of Developmental Psychology, Vol. 2: Self and Other (p.p. 425-444). New York: Oxford University Press.

Hayek, F. A., 1973, Law, Legislation and Liberty, Volume I: Rules and Order. London: Routledge and Kegan Paul [Don Mills: General Publishing].

Maslow, A. H., 1993 [1971]. "Theory Z". The farther reaches of human nature. New York: Arkana.

Rak J. & Bäcker R. (ed), 2022, Neo-militant Democracies in Post-communist Member States of the European Union /. London and New York, Routledge Taylor & Francis Group.

Šlapkauskas, V. 2023. Challenges of Predicting Social Conflicts in the Context of Crises and Hybrid Threats // Research Journal PUBLIC SECURITY AND PUBLIC ORDER, 2023 (33), p. 130-141.

Šlapkauskas V. 2021, The Role of Public Opinions on Society Security: A Socio-Cultural Approach // Research Journal PUBLIC SECURITY AND PUBLIC ORDER, No. 28, pp. 156-165.

Taylor, Ch., 1992. The Ethics of Authenticity. Harvard University Press.

Wolf M. 2023, The Crisis of Democratic Capitalism. By, Penguin Press.

Session 3. Policy and regulation

Bay, S. 2024, *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks*. Hybrid CoE Research Report 12. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-

content/uploads/2024/03/20240319-Hybrid-CoE-Research-Report-12-Countering-hybrid-threats-to-elections-WEB.pdf [30 June 2024].

Cantwell D. 2017, 'Hybrid Warfare: Aggression and Coercion in the Gray Zone', *ASIL Insights* Issue: 14 Volume: 21, Available from: https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone [25 February 2024].

European Centre of Excellence for Countering Hybrid Threats, 2023. Hybrid threats as a Concept. Available from: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [4 September 2023].

European Council, 2023. EU's Strategic Compass for Security and Defence: Articles and reports. Available from: https://consilium-europa.libguides.com/strategic-compass/articles [4 September 2023].

Ferm, T. 2017, *Laws in the era of hybrid threats*. Hybrid CoE Strategic Analysis 3. The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE-SA-3-Ferm.pdf[30 June 2024].

Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue *Addressing Hybrid Threats*, 2018. Available from: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf [4 September 2023].

Haataja, S. (2023) Cyber operations against critical infrastructure under norms of responsible state behaviour and international law, *International Journal of Law and Information Technology*, Volume 30, Issue 4, Winter 2022, Ppp. 423–443, https://doi.org/10.1093/ijlit/eaad006

Joint Staff Working Document, *Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats 16.9.2022 SWD(2022) 308 final.* Available from: https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD_2022_308_6_EN_document_travail_service_conjoint_part1_v5.pdf *[4 September 2023].*

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. 2023, Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, doi:10.2760/37899, JRC129019. Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. [4 September 2023].

Lonardo L. 2021, *EU Law Against Hybrid Threats: A First Assessment.* Available from: *https://www.europeanpapers.eu/en/system/files/pdf_version/EP_eJ_2021_2_19_Articles_SS2_6_Luigi_Lonardo_00514.pdf* [4 September 2023].

McLaughlin, M. 2023, 'Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace', *Opiniojuris.,* Available from: http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/ [25 February 2024].

NATO 2023, *Collective defence and Article 5,* Available from: https://www.nato.int/cps/en/natohq/topics_110496.htm [25 February 2024].

Sanz-Caballero, S. 2023, 'The concepts and laws applicable to hybrid threats, with a special focus on Europe', *Humanities and Social Sciences Communications,* 10:360, https://doi.org/10.1057/s41599-023-01864-y.

Session 4. Warfare in the context of hybrid threats

Amos C. Fox. 2021, *Russian hybrid warfare: A framework*. Journal of military studies. December 2021, Volume & Issue. Volume 10, Issue 1, pp. 60–72. Available from: https://doi.org/10.2478/jms-2021-0004 or https://sciendo.com/article/10.2478/jms-2021-0004?tab=article [30 June 2024].

Bilal, A. 2021, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *Nato Review.* Available from: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html [30 June 2024].

Berkowitz, B. D. 2007, *The New Face of War: How War Will Be Fought in the 21st Century.* Free Press.

Borda. A. Z. (2022) Ukraine war: what is the Budapest Memorandum and why has Russia's invasion torn it up? *The Conversation*. March 2, 2022. Available from: https://theconversation.com/ukraine-war-what-is-the-budapest-memorandum-and-why-has-russias-invasion-torn-it-up-178184 [30 June 2024].

Buchan, P. 2013, Pandours, Partisans, and Petite Guerre: The Two Dimensions of Enlightenment Discourse on War. *Intellectual History Review*, Vol. 23, No. 3, pp. 329–347. Available from: https://doi.org/10.1080/17496977.2012.723338.

Epifanova, A. 2020, Deciphering Russia's "Sovereign Internet Law". Tightening Control and Accelerating the Splinternet. *German Council on Foreign Relations*. January 16, 2020. Available from: https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [30 June 2024].

Galeotti, M. 2018, (Mis)Understanding Russia's two 'hybrid wars'. *Eurozine*. 29 November 2018. Available from: https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/#. [30 June 2024].

Giannopoulos, G., Smith, H. & Theocharidou, M. (eds) 2021, *The Landscape of Hybrid Threats: A Conceptual Model*. Available from: https://dgap.org/sites/default/files/article_pdfs/the_landscape_of_hybryd_threats-eu_publication_office.pdf [30 June 2024].

Hagen, R. A. 2023, *From Battlefield to Bytes: A Deep Dive into Hybrid Warfare*. Available from: https://www.linkedin.com/pulse/from-battlefield-bytes-deep-dive-hybrid-warfare-raymond-andrè-hagen/ [30 June 2024].

Kandrik, M. 2023, *Rethinking Russian Hybrid Warfare. Irregular Warfare Center*. Available from: https://irregularwarfarecenter.org/publications/perspectives/rethinking-russian-hybrid-warfare/ [30 June 2024].

Rumer, E. 2019, *The Primakov (Not Gerasimov) Doctrine in Action*. Carnegie Endowment for International Peace. Available from: https://carnegie-production-assets.s3.amazonaws.com/static/files/files__Rumer_PrimakovDoctrine_final1.pdf [30 June 2024].

Soldatenko, M. 2023, Constructive Ambiguity of the Budapest Memorandum at 28: Making Sense of the Controversial Agreement. *Lawfare*. The Lawfare Institute, February 7, 2023. Available from: https://www.lawfaremedia.org/article/constructive-ambiguity-of-the-budapest-memorandum-at-28-making-sense-of-the-controversial-agreement. [30 June 2024].

U.S. Army Training and Doctrine Command 2007, *Military Guide to Terrorism in the Twenty-First Century*. Handbook. Available from: https://apps.dtic.mil/sti/pdfs/ADA472623.pdf. [30 June 2024].

Watling, J.; Danylyuk, O. V. & Reynolds, N. 2023, *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War*, February 2022 – February 2023. 29 March 2023 Special Report, Royal United Services Institute for Defence and Security Studies. pp.1-39. Available from: https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022. [30 June 2024].

Watling, J. & Reynolds, N. 2022, *The Plot to Destroy Ukraine*. 15 February 2022, Special Report, Royal United Services Institute for Defence and Security Studies, pp.1-19. Available from: https://static.rusi.org/special-report-202202-ukraine-web.pdf. [30 June 2024].

Session 5. Information warfare

MANDATORY READING

A minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session 2018, *Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National Security*., pp. 1-206. Available from: https://www.govinfo.gov/content/pkg/CPRT-115SPRT28110/pdf/CPRT-115SPRT28110.pdf .[29 August 2023].

Adamsky, D. 2019, *Russian Nuclear Orthodoxy. Religion, Politics, and Strategy*. Stanford University press.

Aïmeur, E., Amri, S., & Brassard, G. 2023, Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, *13*(1), 30. https://doi.org/10.1007/s13278-023-01028-5.

Allington, D., 2020, *Conspiracy Theories, Radicalisation and Digital Media*. London: Kings College London. Available from: https://gnet-research.org/wp-content/uploads/2021/02/GNET-Conspiracy-Theories-Radicalisation-Digital-Media.pdf [3 January 2024].

Barnays, E. 1928, Propaganda. Horace Liveright INC. Available from: https://www.voltairenet.org/IMG/pdf/Bernays_Propaganda_in_english_.pdf. [28 August 2023].

Bartlett, J., & Miller, C., 2010, *The power of unreason: Conspiracy theories, extremism and counter-terrorism* London: Demos. pp. 1-54. Available from: http://westernvoice.net/Power%20of%20Unreason.pdf [28 September 2023].

Bennett, L. & Livingston, L. 2020, *The disinformation order: Disruptive communication and the decline of democratic institutions*. European Journal of Communication No. 33(2), April 2020. pp.122-139. Available from: https://journals.sagepub.com/doi/10.1177/0267323118760317 or https://www.researchgate.net/publication/324193884_The_disinformation_order_Disruptive_communication_and_the_decline_of_democratic_institutions .[29 August 2023].

Bennett, L. & Livingston, L. 2020, *A Brief History of the Disinformation Age Information Wars and the Decline of Institutional Authority from Part I - Disinformation in Political and Historical Context.* Cambridge University Press. October 2020. pp.3-40. Available from: https://www.cambridge.org/core/books/disinformation-age/brief-history-of-the-disinformation-age/7F0A2F8BABA0B5CA802EC3AB4F76B818 .[29 August 2023].

Chesney, R., & Citron, D. 2019, Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*. Available from: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war. [30 June 2024].

Cialdini, R. B. 2009, *Influence Psychology of persuasion*. HarperCollins Publishers Ltd. pp.1-263.

Codarin, L., Harth, L., Lulu, J. 2021, *Hijacking the mainstream. CCP influence agencies and their operations in Italian parliamentary and local politics*, Sinopsis, 20 November 2021. Available from: https://sinopsis.cz/wp-content/uploads/2021/11/it0.pdf. [20 June 2023].

Doob, L. W. 1950, *Goebbels' Principles of Propaganda*. Public opinion quarterly. pp. 419-442.

Easton, I. 2022, *The Final Struggle. Inside China's Global Strategy*, Eastbridge Books.

Egelhofer j.l., Lecheler S., 2019, *Fake news as a two-dimensional phenomenon: a framework andresearch agenda.* Annals of the International Communication Assotiation, 2019, VOL. 43, NO. 2, 97–116. Available from: https://www.tandfonline.com/doi/epdf/10.1080/23808985.2019.1602782?needAccess=true&role=button. [5 October 2023].

Evans A. T., Williams H. J. 2022, *How extremism operates online. R*AND Corporation. Available from: https://www.rand.org/pubs/perspectives/PEA1458-2.html. [3 January 2024].

Golovchenko, Y.; Buntain, C.; Eady, G.; Brown, M.; Tucker, J. A. 2016, *Cross-Platform State Propaganda: Russian Trolls on Twitter and YouTube During the 2016 US Presidential Election*, 2020. Available from: https://deliverypdf.ssrn.com/delivery.php?ID=714022009114095071114064083097092126021037057034004075122023003076104018076118122117023061006041103116116084005007121074109122019027055089080083126071087082099081125063047077101073011110011065068095070124085027024107003125071122126019095088107088091083&EXT=pdf&INDEX=TRUE .[29 August 2023].

Helberg, J. 2021, *The Wires of War. Technology and the Global Struggle for Power*, Avi Reader Press.

Kilcullen D 2020, The changing strategic threat Picture, The World of Intelligence. Technology. Apple Podcasts. Available from: https://podcasts.apple.com/au/podcast/the-world-of-intelligence/id1477524651?i=1000477406483 or with transcription https://podcast.janes.com/public/68/The-World-of-Intelligence-50487d09/1db4fe07. [29 August 2023].

Li, E. 2018, The Rise and Fall of Soft Power. Joseph Nye's concept lost relevance, but China could bring it back. *Foreign policy*. 20 August 2018. Available from: https://foreignpolicy.com/2018/08/20/the-rise-and-fall-of-soft-power/. [30 June 2024].

Miao, J. T. 2021, *Understanding the soft power of China's Belt and Road Initiative through a discourse analysis in Europe*. Regional Studies, Regional Science, Vol. 8, Issue 1, pp. 162-177. Available from: https://www.tandfonline.com/doi/full/10.1080/21681376.2021.1921612. [20 June 2023].

Miskimmon, A., O'Loughlin, B., and Roselle, L. 2014, *Strategic Narratives: Communication Power and the New World Order*, London: Routledge.

Mölder, H.; Sazonov, V.; Chochia, A. & Kerikmäe, T. (eds) 2021, *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighbourhood, 2021,* Editors, Springer Nature, pp.1-423.

Olson, S., Prestowitz, C. 2011, *The Evolving Role of China in International Institutions. The U.S.-China Economic and Security Review Commission (prepared by The Economic Strategy Institute)*, January 2011. Available from: https://www.uscc.gov/sites/default/files/Research/TheEvolvingRoleofChinainInternationalInstitutions.pdf. [20 June 2023].

Papkova, I. 2011, *The Orthodox Church and Russian Politics,* Oxford University Press, pp. 1-265.

Rid, I. T. 2020, *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux. pp. 1-528.

Roselle, L., Miskimmon, A., and O'Loughlin, B. 2014, *Strategic narrative: A new means to understand soft power, Media, War & Conflict*, Vol. 7, no. 1, pp. 70-84. Available from: https://www.academia.edu/6682695/Roselle_L_Miskimmon_A_and_OLoughlin_B_2014_Strategic_narrative_A_new_means_to_understand_soft_power_Media_War_and_Conflict_vol_7_no_1_70_84. [20 June 2023].

Sârbu, A., Anca, G. 2023, Using Artificial Intelligence Tools for Obtaining Cognitive Warfare Advantages. *The Defence Horizon Journal*. October 23, 2023. Available from: https://tdhj.org/blog/post/artificial-intelligence-cognitive-warfare-twitter/. [30 June 2024].

United States of America v. Internet Research Agency LLC A/K/A Mediasintez LLC A/K/A Glavset LLC A/K/A Mixinfo LLC A/K/A Azimut LLC A/K/A Novinfo LLC, etc. Indictment. 2018. Available from: https://www.justice.gov/file/1035477/download. [28 August 2023].

Session 6. Common response to hybrid threats and strategies for tackling them

Bajarūnas, E., Keršanskas, B. 2018, Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome. Lithuanian Annual Strategic Review, Volume 16, Issue 1 (pp. 123–170). https://doi.org/10.2478/lasr-2018-0006 Available from: https://journals.lka.lt/journal/lasr/article/152/info [1 August 2023].

Balaban, M., & Mielniczek, P., 2018, *Hybrid conflict modeling. In 2018* Winter Simulation Conference (WSC) (pp. 3709-3720). IEEE. Available from: https://www.researchgate.net/profile/Mariusz-Balaban/publication/330880179_HYBRID_CONFLICT_MODELING/links/5ceb02a092851c4eabc114a2/HYBRID-CONFLICT-MODELING.pdf [12 November 2023].

European Union External Action, 2021, *"Questions and Answers about the East StratCom Task Force"* , October 27, 2021. Available from: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcomtask-force_en#11232 [29 August 2023].

Lasoes N., 2022, *Realising the EU Hybrid Toolbox: opportunities and pitfalls,* December 2022. Available from: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf [26 December 2023].

Moeini, A., Paikin, Z. 2023, IN SEARCH OF A EUROPEAN SECURITY ORDER AFTER THE UKRAINE WAR. The Institute for Peace & Diplomacy. Available from: https://peacediplomacy.org/wp-content/uploads/2023/04/In-Search-of-a-European-Security-Order-After-the-Ukraine-War.pdf [1 February 2024].

Sanz-Caballero, S. 2023, *The concepts and laws applicable to hybrid threats, with a special focus on Europe.* Humanities and Social Sciences Communications, Vol. 10, 360 (2023). Available from: https://www.nature.com/articles/s41599-023-01864-y [1 February 2024].

Wigell, M., Mikkola, H., Juntunen, T., 2021, *Best Practices in the whole-of-society approach in countering hybrid threats. Study Requested by the INGE committee, European Parliament Coordinator,* 2021 May Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf [26 October 2023].

Zandee D., van der Meer S., Stoetman A., 2021, *Countering hybrid threats Steps for improving EU-NATO cooperation*, 2021 October. Available from: https://www.clingendael.org/pub/2021/countering-hybrid-threats/ [26 December 2023].

Session 7. Research strategies and methods

Baldwin J. R., Pingault J.-B., Schoeler T., Sallis H. M., Munafò M. R. 2022, Protecting against researcher bias in secondary data analysis: Challenges and potential solutions. *European Journal of Epidemiology*, 37(1), 1–10.

Gioia, D. 2021, A Systematic Methodology for Doing Qualitative Research. The Journal of applied behavioral science, 2021, Vol.57 (1), p.20-29.

Marx, S, 2023, Mapping as critical qualitative research methodology. International journal of research & method in education, 2023, Vol.46 (3), p.285-29.

McIntyre, D. 2020, *How to think about homeland security. Volume 1, The imperfect intersection of*

national security and public safety. Rowman & Littlefield.

Shared „Dublin“ Descriptors for the Short Cycle, First Cycle, Second Cycle and Third Cycle Awards. 2004, Draft 1.31 working document on JQI meeting in Dublin on 18/10/2004. Viewed on 6 June 2023. Internet access: http://www.unidue.de/imperia/md/content/bologna/dublin_descriptors.pdf.

Urcia, Ivan A. 2021, Comparisons of Adaptations in Grounded Theory and Phenomenology: Selecting the Specific Qualitative Research Methodology. International journal of qualitative methods, 2021, Vol.20, p.16094069211045.

Zyphur, M. J., & Pierides, D. C. 2017, Is quantitative research ethical? Tools for ethically practicing, evaluating, and using quantitative research. *Journal of Business Ethics*, *143*(1), 1–16. https://doi.org/10.1007/s10551-017-3549-8.

Module 2. Prevention and Cooperation in Countering Hybrid Threats

Session 1. Crimes of a hybrid nature

Bértoa, F. C., and Tsutskiridze, L., 2024. *Money Rules: Parties, Oligarchs and Funding Regulation in Post-Soviet Countries*. Taylor and Francis.

Council of the European Union, 2022, *Draft Council conclusions on a framework for a coordinated EU response to hybrid campaigns. Draft Council Conclusions,* 10013/22.

Council of the European Union 2021, *Mini-concept on civilian CSDP support to countering hybrid threats. European External Action Se*rvice*, Written Consultation on the third revision of the Mini-concept on civilian CSDP support to countering hybrid threats,* WK 11851/2020 REV 2.

Darczewska, Jolanta. 2014. *The anatomy of Russian information warfare. The Crimean operation, a case study*. OSW Studies, vol. 42.

Dayspring, S.M., 2015, Toward a theory of hybrid warfare: the Russian conduct of war during peace (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Official Journal of the European Union L 333/164, 27.12.2022.

Demertzis, Maria; Wolff, Guntram B., 2019. Hybrid and cybersecurity threats and the European Union's financial system, Bruegel Policy Contribution, No. 2019/10, Bruegel, Brussels. Available from: https://hdl.handle.net/10419/237635. [3 February 2025].

European Commission 2018, *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council,* JOIN (2018) 16 final. Available from: EUR-Lex - 52018JC0016 - EN - EUR-Lex (europa.eu). [21 November 2022].

European Commission 2016, *Joint Framework on countering hybrid threats a European Union response. Joint communication to the European Parliament and the Council,* JOIN (2016) 18 final. Available from: JOIN_2016_0018_FIN.ENG.xhtml.1_EN_ACT_part1_v8.docx (europa.eu). [21 November 2022].

EUR-Lex 2012, 'Consolidated Version of the Treaty on the Functioning of the European Union', *Official Journal of The European Union,* C 326. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF. [20 September 2023].

Faleg, G & Kovalčíková, N 2022, 'Rising hybrid threats in Africa: Challenges and implications for the EU', Brief no. 3, European Union Institute for Security Studies. Available from: https://www.iss.europa.eu/content/rising-hybrid-threats-africa. [21 November 2022].

Gaglio, I, Guzzon, J, Bartz, K, Marcolin, L, Kryeziu, R, Disley, E & Hulme, S 2023, *Strengthening the fight against corruption: assessing the EU legislative and policy framework.* Publications Office of the European Union. doi:10.2837/22427.

Galeotti, M., 2016, Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?, *Small Wars & Insurgencies*, 27(2), 282-301.

Gilinskiy, Y., 2006, Crime in contemporary Russia. *European Journal of Criminology*, 3(3), 259-292.

Goldfarb, A., 2010, Death of a Dissident: The Poisoning of Alexander Litvinenko and the Return of the KGB. Simon and Schuster.

Gonçalves, C.P., 2019, Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats. In *Cyberspace*. IntechOpen.

Hoogenboom, B., and Hoogenboom, B., 2010, *Blinded by the Light: The Interweaving of (Organised) Crime, White Collar Crime, State Crime and Terrorism*. The Governance of Policing and Security: Ironies, Myths and Paradoxes, pp. 149-168.

Huss, O 2022, *Strategic Corruption as a Threat to Security and the New Agenda for Anti-Corruption.* Available from: https://www.corruptionjusticeandlegitimacy.org/post/strategic-corruption-as-a-threat-to-security-and-the-new-agenda-for-anti-corruption. [1 February 2024].

Kondrushenko, Y., 2019, Responding to Hybrid Warfare: The Case of the Attempted Assassination of Sergey Skripal.

Korauš, Antonín; Jančíková, Eva; Gombár, Miroslav; Kurilovská, Lucia; Černák, Filip., 2024. Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures. Journal of Risk Financial Management. 2024, 17(2), p. 55; Available from: https://doi.org/10.3390/jrfm17020055.

Kostarakos, M., 2023, European Union and NATO Cooperation in Hybrid Threats. In *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies* (pp. 405-423). Cham: Springer International Publishing.

Neville, S.B., 2015, Russia and hybrid warfare: identifying critical elements in successful applications of hybrid tactics (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Schmid, A P 2023, Terrorism prevention: Conceptual issues (Definitions, typologies and theories), In: *Handbook of Terrorism Prevention and Preparedness*, ed. Schmid, A P, The Hague: International Centre for Counter-Terrorism. Available from: https://www.icct.nl/sites/default/files/2023-01/Chapter-2-Handbook-.pdf. [13 January 2024].

Sari, A., 2020, Hybrid threats and the law: Concepts, trends and implications. *Hybrid Centre of Excellence Trend Report*.

United Nations Office on Drugs and Crime (UNODC), 2004. *United Nations Convention Against Corruption.* Available from: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf. [1 February 2024].

Ware, J. 2023, *The third generation of online radicalization*, Program on Extremism at George Washington University. Available from: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/third-generation-final.pdf. [13 January 2024].

White, R.F., 2008, Assassination discourse and political power: The death of Alexander Litvinenko. *Assassination Research*, 5(2), pp.1-8.

Session 2. International criminal law and legal tools for tackling hybrid threats

Casey-Maslen, S. 2024. *Hybrid Warfare Under International Law*. Bloomsbury Academic.

Elliott, K.A. and Uimonen, P.P. 1993, *The effectiveness of economic sanctions with application to the case of Iraq*. Japan and the World Economy, 5(4), pp.403-409.

Elliott, K.A. and Hufbauer, G.C. 1999, Same song, same refrain? Economic sanctions in the 1990's. *American Economic Review*, 89(2), pp.403-408.

Fogt, M.M. 2021, Legal Challenges or Gaps by Countering Hybrid Warfare-Building Resilience in Jus Ante Bellum. *Sw. J. Int'l L.*, 27, p.28.

Fridman, O., 2018, *Russian "Hybrid Warfare": Resurgence and Politicization*. Oxford University Press.

Górka, M. 2023, The Wagner Group as a Tool of Russian Hybrid Warfare. *Polish Political Science Yearbook*, 52(2), pp. 83-98.

Harris, D. J., O'Boyle, M., Bates, E., and Buckley, C. 2023, *Law of the European convention on human rights*. Oxford University Press.

Heller, K. Jon, 2022, Creating a Special Tribunal for Aggression Against Ukraine is a Bad Idea, *Opinio Juris*, 7 March 2022.

Hufbauer, G.C. and Jung, E., 2020, What's new in economic sanctions?. *European economic review*, 130, p.103572.

Lonardo, L. 2021, EU Law against hybrid threats. A first assessment, in European Papers, 2021, vol. 6, pp. 1075–1096.

McDougall, C., 2022, Prosecuting Putin for his Crime of Aggression Against Ukraine: Part Two, *Oxford Human Rights Hub*, 8 March 2022.

Mowbray, A., 2012, *Cases, materials, and commentary on the European Convention on Human Rights*. Oxford University Press.

Regulation EU Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 Amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences.

Rizzotti, M. A., 2019, Russian Mercenaries, State Responsibility, and Conflict in Syria: Examining the Wagner Group under International Law. *Wis. Int'l LJ*, 37, p. 569.

Sanz-Caballero, S., 2023, The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, 10(1), pp. 1-8.

Sari, A., 2020. Hybrid threats and the law. Concepts, trends and implications. In: Hybrid CoE Trend Report 3, Apr 2020, p. 8.

Schabas, W. A., 2015, *The European convention on human rights: a commentary*. Oxford University Press.

United Nations Security Council, 'Resolution 138 on questions relating to the case of Adolf Eichmann, UN Doc S/RES/138(1960).

Van Dijk, P., and Van Hoof, G. J., 2023. *Theory and practice of the European Convention on Human Rights*. Martinus Nijhoff Publishers.

Session 3. Prevention of hybrid threats

Akbar, K A, Halim, S M, Hu, Y, Singhal, A, Khan, L, & Thuraisingham, B 2022, *Knowledge mining in cybersecurity: From attack to defense*, IFIP Annual Conference on Data and Applications Security and Privacy, Cham: Springer International Publishing, Switzerland , pp. 110-122.

Anderson, R & Moore, T 2006, 'The economics of information security', *Science*, vol 314, Issue 5799, pp. 610-613.

Brown, A R 2018, 'Leveraging Artificial Intelligence for Proactive Defense Against Hybrid Threats', *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 4, pp. 567-584.

Choo, K R 2011, 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, vol. 30, no. 8, pp. 719-731.

Garcia, P, Darroch, F, West, L & Brooks-Cleator, L 2020, *Ethical applications of big data-driven AI on social systems: Literature analysis and example deployment use case.* Information, 11(5), 235.

Hoffman, F G 2007*, Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies, Arlington, Virginia. Available from: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. [4 April 2024].

Johnson, J T 2017, *Roadmap for photovoltaic cyber security*, Sandia National Lab, Albuquerque, New Mexico.

Jones, S & Rid, T 2019, 'The cyber-terror trap: How governments respond to mass media scare stories', *International Affairs*, vol. 95, no. 2, pp. 245-266.

Kahneman, D 2011, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York.

Kanamaru, H, Fujita, J & Arai, T 2023, *A Study on the Classification of OT Security Risk Mitigation Measures*, 62nd Annual Conference of the Society of Instrument and Control Engineers (SICE), Tsu, Japan, pp. 274-279.

Keplin, J 2023, '*Building state resilience against hybrid activities*', *Przegląd Bezpieczeństwa Wewnętrznego*, pp. 241-266.

Kjærgaard, K, Karen, K, & Petersen, L 2017, 'Public–private partnerships on cyber security: a practice of loyalty', *International Affairs*, vol. 93, no. 6, pp. 1435–1452. Available from: https://doi.org/10.1093/ia/iix189. [4 April 2024].

Ponemon Institute 2019, *Cost of a Data Breach Report*, Available from: https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258, [4 April 2024].

Rossow, C, Dietrich, C J, Davi, L & van der Walt, C 2017, *Sandnet: Network traffic analysis of malicious software*, In Proceedings of the 2017, Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM), Conference on Computer and Communications Security, pp. 1807-1824.

Smith, J 2019, 'The role of intelligence in proactive defense against hybrid threats', *Journal of Strategic Security*, vol. 12, no. 3, pp. 45-62.

Stohl, M 2019, *The Politics of Cybersecurity: How states and security experts understand, perform and discuss security in the digital age*, Routledge, Oxfordshire.

Sunstein, C R 2018, *#Republic: Divided democracy in the age of social media*, Princeton. Available from: https://doi.org/10.1515/9781400890521. [11 April 2024].

Weimann, G 2015, *Terrorism in cyberspace: the next generation*, Woodrow Wilson Center Press. Available from: https://cris.haifa.ac.il/en/publications/terrorism-in-cyberspace-the-next-generation. [11 April 2024].

Session 4. Cybersecurity and cyber incident management

Anderson, R & Moore, T 2006, 'The Economics of Information Security', *Science*, *314*(5799), pp. 610–613. Available from: http://www.jstor.org/stable/20031627. [22 April 2024].

Birnhack, M 2012, *Reverse engineering informational privacy law*. Volume 15, Yale Journal of Law & Technology, 24. Yale University, New Haven.

Bodeau, D & Dawkins, C 2014, 'The public-private partnership for cybersecurity: Aligning expectations and driving success', *Journal of Cybersecurity*, vol. 3, issue 2, pp. 175-198.

Brenner, SW 2009, *Cyber Threats: The Emerging Fault Lines of the Nation State*, New York, online edn, Oxford Academic. Available from: https://doi.org/10.1093/acprof:oso/9780195385014.001.0001, [4 April 2024].

Choo, KKR 2011, 'The cyber threat landscape: Challenges and future research directions', *Computers & Security*, vol. 30, no. 8, pp. 719-731.

Comfort, L K, Kilkon, K & Zagorecki, A 2001, 'Coordination in rapidly evolving disaster response systems: The role of information', *American Behavioral Scientist*, vol. 44, no. 7, pp. 1032-1045.

Comfort, L K, Kilkon, K & Zagorecki, A 2001, 'Coordination in rapidly evolving disaster response systems: The role of information', *American Behavioral Scientist*, vol. 44, no. 7, pp. 1032-1045.

Curtis, A 2018, *Freedom of information in the digital age*, Routledge, London.

Deibert, R 2013, *Black Code: Inside the Battle for Cyberspace*, McClelland & Stewart, Toronto.

Deibert, R 2019, *Reset: Reclaiming the internet for civil society*, House of Anansi Press, Toronto.

Floridi, L, Cowls, J, Beltrametti, M, Chatila, R, Chazerand, P, Dignum,V, Luetge, C, Madelin, R, Pagallo, U, Rossi, F, Schafer, B, Valcke, P & Vayena, E 2018, 'AI4 People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations ', *Minds & Machines,* vol. 28, pp. 689–707. Available from: https://doi.org/10.1007/s11023-018-9482-5. [22 April 2024].

Greenwald, G 2014, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, New York.

Herath, TC, & Rao, HR 2009, *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness*, Decision Support Syst., 47, pp. 154-165.

Kirwan, G & Power, A 2013, *Cybercrime: The psychology of online offenders*, Cambridge University Press.

Kushner, D 2013, *The Real Story of Stuxnet - IEEE Spectrum*, Available from: https://spectrum.ieee.org/the-real-story-of-stuxnet. [22 April 2024].

Radsan, A J & Murphy, J D 2008, 'Intelligence legalism and the National Security Agency's civil liberties gap', *Stanford Law Review*, vol. 60, no. 3, pp. 549-598.

Simchi-Levi, D, Kaminsky, P, & Simchi-Levi, E 2014*, Designing and managing the supply chain: Concepts, strategies, and case studie*s, McGraw-Hill Education. Available from: (PDF) Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies, David Simchi-Levi Philip Kaminsky Edith Simchi-Levi (researchgate.net). [2 April 2024].

Singer, PW & Friedman, A 2015, *Cybersecurity and cyberwar: What everyone needs to know*, Oxford University Press. Avaliable from: https://whateveryoneneedstoknow.com/display/10.1093/wentk/9780199918096.001.0001/isbn-9780199918096. [23 April 2024].

Solove, D J 2008, *Understanding privacy*, Harvard University Press, United states of America.

Van der Sloot, B 2020, 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 11, 160.

Whitman, M E, & Mattord, H J 2018, *Management of information security* (6th ed.), Cengage Learning, Cheriton House, North Way, Andover, Hampshire.

Session 5. International cooperation

Bachmann, S.-D., Gunneriusson, H. 2015, *Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security*. Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, p. 87. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2506063. [12 December 2024].

Bachmann, S. D., Gunneriusson, H. 2014, *Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Risk and Security*. The Journal on Terrorism and Security Analysis, p. 33. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2252595. [23 January 2025].

Bajarūnas, E. 2020, *Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond*. European View, 19(1), pp. 63. Available from: https://doi.org/10.1177/1781685820912041. [12 December 2024].

Bajarūnas, E., Keršanskas, V. 2018, *Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome*. Lithuanian Annual Strategic Review, 16(1), p. 159. Available from: https://journals.lka.lt/journal/lasr/article/152/info. [12 December 2024].

Balcaen, P., Du Bois, C., Buts, C. 2021, *Sharing the Burden of Hybrid Threats: Lessons from the Economics of Alliances*, Defence and Peace Economics, DOI: 10.1080/10242694.2021.1991128, p. 4. Available from: https://doi.org/10.1080/10242694.2021.1991128. [18 December 2024].

Bendiek, A. 2018, *The EU as a Force for Peace in International Cyber Diplomacy*. Stiftung Wissenschaft und Politik, German Institute for International and Security Affairs, p. 1. Available from: https://www.swp-berlin.org/publikation/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy. [20 January 2025].

Bertolini, M., Minicozzi, R., Sweijs, T. 2023, *Ten Guidelines for Dealing with Hybrid Threats: A Policy Response Framework*. The Hague Centre for Strategic Studies, pp. 7, 12. Available from: https://hcss.nl/report/ten-guidelines-for-dealing-with-hybrid-threats/. [6 December 2024].

Bhardwaja, A., Mangata, V., Viga, R., Halderb, S., Contib, M. 2021, *Distributed Denial of Service Attacks in Cloud: State-of-the-Art of Scientific and Commercial Solutions*. Computer Science Review, p. 24. Available from: https://www.researchgate.net/publication/348097190_Distributed_denial_of_service_attacks_in_cloud_State-of-the-art_of_scientific_and_commercial_solutions?enrichId=rgreq-857443269456ff0c47ac7fc329282664-XXX&enrichSource=Y292ZXJQYWdlOzM0ODA5NzE5MDtBUzoxMTI2NTU4OTcwNDYyMjA4QDE2NDU2MDM5OTcwMDY%3D&el=1_x_2. [20 January 2025].

Cîrdei, I. A., Ispas, L. 2017, *A Possible Answer of the European Union to Hybrid Threats*. Scientific Bulletin, De Gruyter Open, Vol. 22 (Issue 2), p. 73. Available from: https://doi.org/10.1515/bsaft-2017-0009. [12 December 2024].

Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007R0168. [20 January 2024].

Danyk, Y., Maliarchuk, T., Briggs, C. 2017, *Hybrid War: High-tech, Information and Cyber Conflicts*, Connections QJ 16, no. 2, pp. 15-16. Available from: https://doi.org/10.11610/Connections.16.2.01. [20 January 2025].

European Commission 2016, *Joint Framework on countering hybrid threats - a European Union response.* JOIN/2016/018 final. Document 52016JC0018, p. 13. Available from: https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. [17 January 2025].

European Commission 2020, *The EU's Cybersecurity Strategy for the Digital Decade*. JOIN (2020) 18 final, p. 15. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. [17 January 2025].

Filipec, O. 2021, *Preventing Hybrid Threats: From Identification to an Effective Response*. European Studies. 8, p. 19. Available from:

https://www.researchgate.net/publication/354034499_Preventing_Hybrid_Threats_From_Identification_to_an_Effective_Response. [18 December 2024].

Ivanov, I., Shalamanov, V. 2020, *NATO and Partner countries cooperation in countering asymmetric and hybrid threats in South Eastern Europe's cyberspace*. NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Volume 149: Toward Effective Cyber Defense in Accordance with the Rules of Law, p. 11. Available from: https://www.researchgate.net/publication/351702431_NATO_and_Partner_countries_cooperation_in_countering_asymmetric_and_hybrid_threats_in_South_Eastern_Europe's_cyberspace. [17 January 2025].

Microsoft 2022, *Digital Crimes Unit: Leading the fight against cybercrime*. Available from: https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/. [20 January 2025].

Microsoft Digital Defense Report 2024 - The foundations and new frontiers of cybersecurity, p. 95. Available from: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024. [20 January 2025].

Monaghan, S. 2019, *Countering Hybrid Warfare: So What for the Future Joint Force?* PRISM, 8(2), p. 90. Available from: https://www.jstor.org/stable/26803232. [17 January 2025].

Ratsyborinska, V. 2022, *EU-NATO and the Eastern Partnership Countries Against Hybrid Threats (2016-2021)*. National Security and the Future, 23(2), pp. 89-90. Available from: https://doi.org/10.37458/nstf.23.2.3. [12 December 2024].

Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction (recast). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006R1920. [20 January 2024].

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R2219. [20 January 2024].

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA - 32016R0794. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0794. [16 January 2024].

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1726. [18 January 2024].

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1727. [18 January 2024].

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1896. [17 January 2024].

Regulation (EU) 2021/2303 of the European Parliament and of the Council of 15 December 2021 on the European Union Agency for Asylum and repealing Regulation (EU) No 439/2010. Available from: https://eur-lex.europa.eu/eli/reg/2021/2303/oj. [20 January 2024].

Sari, A. 2018, *Blurred Lines: Hybrid Threats and the Politics of International Law - Strategic Analysis January 2018*. Hybrid CoE, p. 8. Available from: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-4-blurred-lines-hybrid-threats-and-the-politics-of-international-law/. [12 December 2024].

Simons, G., Danyk, Y., Maliarchuk, T. 2020, *Hybrid war and cyber-attacks: creating legal and operational dilemmas*, Global Change, Peace & Security, pp. 4, 6. Available from: https://doi.org/10.1080/14781158.2020.1732899. [20 January 2025].

Skopik, F., Pahi, T. 2020, *Under false flag: using technical artifacts for cyber attack attribution*. Cybersecurity, 3:8, pp. 1, 4. Available from: https://doi.org/10.1186/s42400-020-00048-4. [20 January 2025].

Swaminathan, A., Ramakrishnan, B., Kanishka, M., Surendran, R. 2022, *Prediction of Cyber-attacks and Criminality Using Machine Learning Algorithms*, 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, pp. 1, 8. Available from: https://www.researchgate.net/publication/366704973_Prediction_of_Cyber-attacks_and_Criminality_Using_Machine_Learning_Algorithms?enrichId=rgreq-8e82f656e93d9f2843abf2ddff2e0fbd-XXX&enrichSource=Y292ZXJQYWdlOzM2NjcwNDk3MztBUzoxMTQzMTI4MTIyNDI5NzMyNkAxNzA4MTY4OTk1NDEz&el=1_x_2. [20 January 2025].

Taneski, N., Kirkova, R. 2018, *The Concept of Hybrid Threats*, International Journal, Scientific Papers, pp. 1795. Available from: https://eprints.ugd.edu.mk/22011/ [19 December 2024].

Tudorache, P., Bârsan, G. 2024, *Strategies to Counter Hybrid Threats*, in: *Hybrid Warfare Reference Curriculum*, Volume I, Compulsory Lectures, Edited by Zoltán Jobbágy – Edina Zsigmond, Ludovika University Press, Budapest, 2024, pp. 160, 162. Available from: https://csnsc.uk/hybrid-warfare-reference-curriculum-volume-i/. [6 December 2024].

Veena, K., Meena, K., Teekaraman, Y., Kuppusamy, R., Radhakrishnan, A. 2022, *C SVM Classification and KNN Techniques for Cyber Crime Detection*. Wireless Communications and Mobile Computing, Wiley, Volume 2022, pp. 7-8. Available from: https://doi.org/10.1155/2022/3640017. [20 January 2025].

Module 3. Increasing resilience and bolstering societal and institutional capabilities to hybrid threats

Session 1. Common resilience-building approach against hybrid threats

Boin, A & Rhinard, M 2022, "Crisis Management Performance and the European Union: The Case of COVID-19." Journal of European Public Policy, 30 (4): pp. 655–75. doi:10.1080/13501763.2022.2141304.

Council of the European Union, 2021, *The Council adopted conclusions on resilience and crisis response - Consilium*, doc. 14276/21. Available from: https://data.consilium.europa.eu/doc/document/ST-14276-2021-INIT/en/pdf, [03 December 2024].

ECHR, 2022, *European Convention on Human Rights-A living instrument.* p.p. 11. Available from: https://www.echr.coe.int/documents/d/echr/Convention_Instrument_ENG. [12 December 2024].

European Commission, 2024, *Tackling disinformation and information manipulation*. p.p. 1-4. Available from: https://ec.europa.eu/commission/presscorner/api/files/attachment/878789/Tackling%20Disinformation_Factsheet_EN.pdf. [15 December 2024].

European Commission, 2020, *Communication from the commission to the European Parliament, the Council, the European economic and social Committee and the committee of the regions. On the European democracy action plan*, COM/2020/790 final. p.p. 19-27. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:790:FIN. [12 December 2024].

European Parliament, 2021, *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf, [27 December 2024].

European Parliament, 2019, *Online disinformation and the EU's response.* p. 1-2. Available from: https://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf. [12. December 2024].

Grbeša Zenzerović, M., Nenadić, I., 2022, *Jačanje otpornosti društva na dezinformacije: analiza stanja i smjernice za djelovanje – studija*. Zagreb: Agencija za elektroničke medije. Available from: *https://www.aem.hr/wp-content/uploads/2022/09/Studija_dezinformacije_2-izdanje.pdf*. [12 December 2024].

Helbing, D 2013, Globally networked risks and how to respond. Nature, 497 (7447), pp.51-59. Available from: https://www.nature.com/articles/nature12047. [12 July 2024].

Hrvatska enciklopedija, mrežno izdanje. *"Promidžba"*, Leksikografski zavod Miroslav Krleža, 2013. – 2024. Available from: https://enciklopedija.hr/clanak/promidzba. [16 December 2024).

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., 2023, *Hybrid threats: a comprehensive resilience ecosystem*, Publications Office of the European Union, Luxembourg, doi:10.2760/37899, JRC129019. p.p. 8-21. Available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf. [12 December 2024].

Larsson, O., 2013, Sovereign power beyond the state: a critical reappraisal of governance by networks. *Critical Policy Studies*, 7(2), pp.99-114.

NATO, 2024, *NATO's aproach to counter information threats - Public summary.* Available from: https://www.nato.int/cps/en/natohq/official_texts_231905.htm. [18 October 2024].

Nye, JS 2010, Cyber Power, Harvard Kennedy School. Available from: https://www.researchgate.net/publication/236602842_Globally_networked_risks_and_how_to_respond. [12 July 2024].

Van der Meer, T G L A & Jin, Y 2020, Seeking formula for misinformation treatment in public health crises: The effects of corrective information type and source, Health Communication, 35(5), pp.560-575. Available from: https://pubmed.ncbi.nlm.nih.gov/30761917/. [12 July 2024].

Wardle, C & Derakhshan, H 2017, Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. Available from: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policymaking.html. [12 July 2024].

Session 2. Fostering the resilience of the state and non-state actors to hybrid threats

Bauman, Z., 2000, Liquid Modernity. Cambridge: Polity Press.

Di Gregorio, A., 2022, Rule of law crisis and the constitutional 'awareness' of the EU. In *Rule of Law in Crisis* (pp. 152-173). Routledge.

Dunay, P & Roloff, R 2017, *Hybrid Threats and Strengthening Resilience on Europe's Eastern Flank*, Available from: https://www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0. [2 December 2024].

Giddens, A. & Sutton, P. W., 2017, Sociology (8th ed.). Oxford: Polity Press.

Hybrid CoE, 2024, *Hybrid CoE key themes for 2024.* Available from: https://www.hybridcoe.fi/wp-content/uploads/2023/12/Hybrid-CoE-key-themes-for-2024.pdf. pp. 1-4. [15 December 2024].

Joseph, J., 2018, *Varieties of Resilience: Studies in Governmentality*, Cambridge: Cambridge University Press.

Kellerbauer, M., Klamert, M. and Tomkin, J., 2024, *The EU Treaties and Charter of Fundamental Rights: a Commentary*. Oxford University Press.

Mitchell, T., and Harris, K., 2012, *Resilience: A Risk Management Approach*. London: Overseas Development Institute.

Niinistö, S 2024, Outsmart malicious actors to deter hybrid attacks. Available from: https://commission.europa.eu/document/download/934d5577-2d06-4cef-8aa3-8edd2556dd59_en?filename=2024_Niniisto-factsheet_6.pdf. [2 December 2024].

OECD (2023)., *REPORT ON THE IMPLEMENTATION OF THE OECD RECOMMENDATION ON THE GOVERNANCE OF CRITICAL* RISK. p. 27 https://one.oecd.org/document/C(2023)163/en/pdf. [20 December 2024].

Rathnayaka, B., Siriwardana, C., Robert, D., Amara, 2022, *Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review*. International Journal of Disaster Risk Reduction, 2022, pp. 103-123. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2212420922003429?via%3Dihub. [20 December 2024].

Rouet, G. and Pascariu, G., 2019, *Resilience and the EU's Eastern Neighbourhood Countries.*

Tikanmäki, I. & Ruoslahti, H., 2022, How are Hybrid Terms Discussed in the Recent Scholarly Literature?. In: European Conference on Cyber Warfare and Security. Available from: https://www.researchgate.net/publication/361218645_How_are_Hybrid_Terms_Discussed_in_the_Recent_Scholarly_Literature. [December 30 2024].

Tridimas, G. and Tridimas, T., 2017, Public awareness of EU rights and the functions of the European Ombudsman: some unpleasant findings. In *Accountability in the EU* (pp. 74-93). Edward Elgar Publishing.

Wigell, M, Mikkola, H & Juntuen T 2021, *Best Practices in the whole-of-society approach in countering hybrid threats*. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf . [2 December 2024].

Session 3. Protection of critical infrastructure

Adger, W N 2000, 'Social and ecological resilience: Are they related? *Progress in Human Geography*,' vol. 24, no 3, pp.347-364. Available from: https://doi.org/10.1191/030913200701540465. [4 April 2024].

Baldwin, A, D 2020, *Economic Statecraft*, Princeton University Press, Princeton. Available from: https://press.princeton.edu/books/paperback/9780691204420/economic-statecraft. [23 April 2024].

Bascomb, N 2016, *Sabotage: The mission to destroy Hitler's atomic bomb*, Scholastic Incorporated, New York.

Britannica 2024, *Civil Rights*. Available from: https://www.britannica.com/topic/civil-rights. [8 March 2022].

Britt, T W & Oliver, K K 2013, *Morale and cohesion as contributors to resilience*, in Sinclair, RR & Britt TW (Eds.), Building psychological resilience in military personnel: Theory and practice, American Psychological Association, pp. 47-65. Available from: https://doi.org/10.1037/14190-003. [4 April 2024].

Chesley, D L & Amitrano, M 2015, 'Risk and growth, but not as we know them', *Resilience: A journal of strategy and risk*, pp. 1-6. Available from: https://www.pwc.ch/de/publications/2016/pwc_ceo_survey_resilience_e.pdf. [4 April 2024].

Council of Europe 2021, *State of democracy, human rights and the rule of law: A democratic renewal for Europe*, Secretary General of the Council of Europe. pp. 1-46. Available from: https://rm.coe.int/annual-report-sg-2021/1680a264a2. [4 April 2024].

Energy Community 2020, *Annual Implementation Report 2020*, Vienna: Energy Community Secretariat. Available from: https://www.energy-community.org/news/Energy-Community-News/2020/11/23.html. [4 April 2024].

European Commission 2019, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal*. Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN. [4 April 2024].

European External Action Service 2020, *European neighborhood policy and enlargement negotiations*. Available from: https://ec.europa.eu/neighbourhood-enlargement/, [4 April 2024].

European Investment Bank 2020, *European Investment Bank Annual Report 2020*, Luxembourg: European Investment Bank. Avaliable from: https://www.eib.org/en/publications/financial-report-2020. [4 April 2024].

European Union Agency for Cybersecurity 2018, *Capacity building in cybersecurity: A strategy for the European Union*, Publications Office of the European Union, Luxembourg.

European Western Balkans 2019, *Investing in the Western Balkans: Western Balkans Investment Framework Annual Report 2019*. Brussels: European Union.

Macaulay, T 2008, *Critical infrastructure: Understanding its component parts, vulnerabilities, operating risks, and interdependencies*, US: CRC Press Broken Sound Parkway, NW Suite 300, Boca Raton, Florida, US.

Williamson Murray, W & Mansoor, R P 2012, *Hybrid warfare: Fighting complex opponents from the ancient world to the present*, Cambridge University Press, Shaftesbury Road Cambridge, UK.

Module 4. Management and Leadership in the Context of Hybrid Threats and Hybrid Crises

Session 1. European Union's external dimension in countering hybrid threats

Andersson, J J 2023, *European Defence Partnerships: Stronger Together*, European Union Institute for Security Studies EUISS, Brief no. 3. Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/european-defence-partnerships. [20 September 2023].

Andersson, JJ & Cramer, CS 2023, *EUISS Yearbook of European Security*. EU Institute for Security Studies. Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/yearbook-european-security-2023. [10 October 2023].

Boin, A & Rhinard, M 2023, 'Crisis Management Performance and the European Union: The Case of COVID-19'. *Journal of European Public Policy*, vol. 30(4), pp. 655–675. Available from: https://doi.org/10.1080/13501763.2022.2141304. [27 October 2023].

Brethous, M & Kovalčíková, N 2023, *Next level partnership: Bolstering EU–NATO cooperation to counter hybrid threats in the Western Balkans*, EUISS Brief no 2, Luxembourg: Publications Office of the European Union. Available from: https://www.iss.europa.eu/content/next-level-partnership-bolstering-eu-nato-cooperation-counter-hybrid-threats-western-balkans. [3 September 2023].

Council of the European Union, 2022, *Draft Council conclusions on a framework for a coordinated EU response to hybrid campaigns. Draft Council Conclusions,* 10013/22.

Council of the European Union, 2021, *Mini-concept on civilian CSDP support to countering hybrid threats. European External Action Ser*vice*, Written Consultation on the third revision of the Mini-concept on civilian CSDP support to countering hybrid threats,* WK 11851/2020 REV 2.

Countering hybrid threats: EU–NATO cooperation [Policy Podcast]. Available from: https://www.europarl.europa.eu/rss/podcast/eprs-policy-podcast/mp3/2017/hybrid-threats-eu-nato.mp3. [4 September 2023].

Cullen, P, Juola, C, Karagiannis, G, Kivisoo, K, Normark, M, Rácz, A, Schmid, J & Schroefl, J 2021, *The landscape of Hybrid Threats: A Conceptual Model*, Giannopoulos, G, Smith, H and Theocharidou, M (eds), Luxembourg: Publications Office of the European Union. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305. [18 October 2023].

Directorate-General for Research and Innovation (European Commission) 2022, *Strategic crisis management in the EU – Improving EU crisis prevention, preparedness, response and resilience*, Luxembourg: Publications Office of the European Union. https://data.europa.eu/doi/10.2777/517560. [27 October 2023].

European Commission, 2018, *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council,* JOIN (2018) 16 final. Available from: EUR-Lex - 52018JC0016 - EN - EUR-Lex (europa.eu). [21 November 2022].

EUR-Lex. Summaries of EU Legislation 2020, *Crisis Management – Framework for Participation Agreements*. Available from: https://eur-lex.europa.eu/EN/legal-content/summary/crisis-management-framework-for-participation-agreements.html. [26 October 2023].

EUR-Lex 2012, 'Consolidated Version of the Treaty on the Functioning of the European Union', *Official Journal of The European Union,* C 326. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF. [20 September 2023].

European Commission, 2016, *Joint Framework on countering hybrid threats a European Union response. Joint communication to the European Parliament and the Council,* JOIN (2016) 18 final. Available from: JOIN_2016_0018_FIN.ENG.xhtml.1_EN_ACT_part1_v8.docx (europa.eu) [21 November 2022].

European Defence Agency 2023, *Coordinated annual review on defence*. Available from: https://eda.europa.eu/what-we-do/EU-defence-initiatives/coordinated-annual-review-on-defence-(card). [25 October 2023].

European External Action Service 2021, *The Common Security and Defence Policy*. Available from: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en. [20 September 2023].

European External Action Service 2023, *About CSDP structure, instruments and agencies*. Available from: https://www.eeas.europa.eu/eeas/csdp-structure-instruments-and-agencies_en. [23 October 2023].

European External Action Service 2023, *Missions and operations*. Available from: https://www.eeas.europa.eu/eeas/missions-and-operations_en. [20 September 2023].

Faleg, G & Kovalčíková, N 2022, 'Rising hybrid threats in Africa: Challenges and implications for the EU', Brief no. 3, European Union Institute for Security Studies. Available from: https://www.iss.europa.eu/content/rising-hybrid-threats-africa. [10 October 2023].

Jungwirth, R, Smith, H, Willkomm, E, Savolainen, J, Alonso Villota, M, Lebrun, M, Aho, A & Giannopoulos, G 2023, *Hybrid Threats: A Comprehensive Resilience Ecosystem*, Luxembourg: Publications Office of the European Union. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC129019. [10 September 2023].

North Atlantic Treaty Organisation 2023, *EU-NATO task force on the resilience of critical infrastructure 2023, Final assessment report.* Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf. [10 October 2023].

NATO Energy Security Centre of Excellence 2023, *NATO ENSEC COE Official website*. Available from: https://www.enseccoe.org/en. [2 September 2023].

NATO Library 2023, *NATO–EU relations*. Available from: https://natolibguides.info/nato-eu/documents. [20 September 2023].

NATO Strategic Communications Centre of Excellence (NATO StratCom COE) 2020, *NATO Strategic Communications Centre of Excellence Official website*. Available from: https://stratcomcoe.org/. [2 September 2023].

Permanent Structured Cooperation 2023, *About PESCO.* Available from: https://www.pesco.europa.eu/. [20 October 2023].

PreventionWeb 2022, *Strategic crisis management in the European Union*, Science advice for policy by European Academies. Available from: https://www.preventionweb.net/publication/strategic-crisis-management-european-union. [27 October 2023].

The European Centre of Excellence for Countering Hybrid Threats, *Hybrid COE Official website*. Available from: https://www.hybridcoe.fi/. [2 September 2023].

The NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE Official website*. Available from: https://ccdcoe.org/. [2 September 2023].

Session 2. Border and security management

Council of the European Union 2002, *Plan for the management of the external borders of the Member States of the European Union,* doc, 10019/02, pp. 11-27. Available from: https://data.consilium.europa.eu/doc/document/ST%2010019%202002%20INIT/EN/pdf. [09 March 2023].

Council of the European Union 2002, *Plan for the management of the external borders of the Member States of the European Union, doc, 10019/02,* pp. 11-27. Available from: https://data.consilium.europa.eu/doc/document/ST%2010019%202002%20INIT/EN/pdf. [09 March 2023].

European Commission 2002, *Communication from the Commission to the Council and the European Parliament - towards integrated management of the external borders of the member states of the European Union*, COM/2002/0233 final, pp. 6, 12-22**.** Available from**:** EUR-Lex-52002DC0233 - EN (europa.eu). [06 February 2023].

Estonian Academy of Security Sciences 2022, *Impact of Events in Belarus on the Safety and Security of the Baltic States*. Available from: https://digiriiul.sisekaitse.ee/handle/123456789/2853. [26 August 2024].

EU Monitor 2024, *Legal provisions of COM (2021)891 - Amendment of Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders.* Available from: https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vloruvttc5ze. [27 August 2024].

European Commission 2021, *Von der Leyen on Belarus: The EU has the will, the unity and the resolve to face this crisis*. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ac_21_6254. [27 August 2024].

Hall, B, Fleming S & Shotter, J 2021, 'How migration became a weapon in a 'hybrid war'', *Financial Times*. Available from: https://www.ft.com/content/83ece7e4-cc71-45b5-8db7-766066215612. [27 August 2024].

Presidency Conclusions 2001, *European Council Meeting in Laeken 14 and 15 December 2001*, p. 13. Available from: https://www.consilium.europa.eu/media/20950/68827.pdf. [16 February 2023].

Mac Dougall, D 2023, *Russia using 'hybrid warfare' tactics to push migrants over Finnish border,* Euronews. Available from: https://www.euronews.com/2023/11/14/finland-says-russia-is-helping-migrants-make-their-way-over-the-eastern-border. [27 August 2024].

Session 3. Countering information advocacy and influence activities

EU Code of conduct on countering illegal hate speech online 2019, Brussels: European Commission. Available from: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en [6 October 2024].

EU Code of practice on disinformation 2022, Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation [6 October 2024].

Europol Annual EU Terrorism Situation and Trend Reports (TE-SAT). European Union Agency for Law Enforcement Cooperation. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

Extremism, Radicalisation & Mental Health: Handbook for Practitioners 2019, Product of the RAN Centre of Excellence and the RAN H&SC Working Group. Available from: https://home-affairs.ec.europa.eu/system/files/2019-11/ran_h-sc_handbook-for-practitioners_extremism-radicalisation-mental-health_112019_en.pdf [10 November 2024].

Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training 2022, Brussels: European Commission. Available from: https://op.europa.eu/en/publication-detail/-/publication/a224c235-4843-11ed-92ed-01aa75ed71a1/language-en [6 October 2024].

Loik, R. and Madeira, V. 2021, *European Union Strategy and Capabilities to Counter Hostile Influence Operations*. In: H. Mölder; V. Sazonov; A. Chochia; T. Kerikmäe (Ed.). The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood, pp. 247−264. Switzerland: Springer Nature.

Palmertz, B. 2021, *Influence operations and the modern information environment*. In: Hybrid Warfare: Security and Asymmetric Conflict in International Relations. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm. London: I.B. Tauris, Bloomsbury Collections. http://dx.doi.org/10.5040/9781788317795.0014

Pamment, J. 2022, *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/a-capability-definition-and-

assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255 [11 September 2024].

Pape, R. 2024, *The Return of Political Violence*. A Conversation with Robert Pape. The *Foreign Affairs* Interview (November 7, 2024). Available from: https://www.foreignaffairs.com/podcasts/return-political-violence [7 November 2024].

per Concordiam. Journal of European Security and Defense Issues. *Beyond Propaganda: Exposing Falsehoods and Fake News*. Volume 9, Issue 2, 2019. Available from: https://perconcordiam.com/archives/

per Concordiam. Journal of European Security and Defense Issues. *Strategic Communications: Winning the Information War*. Volume 10, Issue 2, 2020. Available from: https://perconcordiam.com/archives/

Report on FIMI Threats 2024, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence. EU External Action Service. Available from: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Strategic Framework for Countering Terrorism and Targeted Violence 2019, Department of Homeland Security (September 2019). Available from: https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

Sörensen, S. 2024, *Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops*. Riga: NATO Strategic Communications Centre of Excellence. Available from: https://stratcomcoe.org/publications/enhancing-organisational-capability-a-tailored-approach-with-red-team-vs-blue-team-adapted-workshops/299 [6 October 2024].

Wardle, C. & Derakshan, H. 2017, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe report DGI(2017)09. Strasbourg: Council of Europe. Available from: https://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf [6 October 2024].

Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm. London: I.B. Tauris, Bloomsbury Collections. http://dx.doi.org/10.5040/9781788317795.0014

ANNEX 4 Cross-reference Tables

Cross-reference Table of Course Learning Outcomes and Module Learning Outcomes

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
Module 1						
critically analyse hybrid threats in the context of global, European and national security						
evaluate the security strategies aiming to ensure sustainable security concepts in contemporary hybrid threats environment						
discuss international and European Union policies and legal framework responding to hybrid threats, considering provisions of fundamental rights						

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
critically analyse tendencies of contemporary warfare regarding hybrid threats						
critically analyse cases of information warfare and their impact on fundamental rights						
independently and creatively identify problems related to hybrid threats and develop and design solutions to respond to hybrid threats using different research strategies and methods in social science research						
Module 2						
explain specifics of modern crimes of hybrid nature and criminal procedure concept and their connection with						

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
principles of fundamental rights						
identify problems, recommend and elaborate tools and methods of protection against hybrid threats by working in a team and benefit from team learning processes						
explain risks related to cybersecurity and business continuity and infringement of fundamental rights						
critically analyse the importance of prevention and countering hybrid threats using relevant tools and means of cooperation						
Module 3						

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
explain tools for fostering resilience of the state and non-state actors to hybrid threats						
explain the role of protection of fundamental rights in preparation for responding to hybrid threats including in cooperation with civil-military and other stakeholders						
selectively identify and present good practices related to the protection of critical infrastructure and strategic objects						
Module 4						
explain the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies						

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
critically analyse the European Union's approach to internal and border security management						
evaluate the role of fundamental rights in European Union's internal and border security management						
critically evaluate actions countering against information advocacy and influence activities						
analyse and interpret psychological aspects related to radicalisation and different forms of extremism on social media						
propose combined approaches for management and leadership for encountering modern security challenges and threats based on modern theories, considering professional						

Course learning outcomes / Module learning outcomes	has a systematic overview and a 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	applies managerial and leadership theories and concepts for dealing with modern security challenges and threats	employs appropriate tools and techniques to strategically manage civilian, human and technical resources, balancing organisational goals with stakeholders' expectations in case of hybrid crises	creates action plans for the prevention of hybrid incidents in the context of ensuring national and regional security	demonstrates the capacity to work in positions requiring strategic thinking, comprehends and copes with challenges and controversies related to hybrid threats, participates in practical (applied) research activities, and is committed to continuous learning and professional development
ethics, fundamental rights and principles of equal treatment of diverse groups						
apply strategic communication skills in a hybrid context based on ethical values and evaluate the results						
employ appropriate tools and techniques to strategically manage civilian, human and technical resources and take decisions in case of hybrid crises and critically evaluate their peers' performance in solving problems						

Cross-Reference Tables of Module Learning Outcomes and Sessions

Module 1							
Sessions / Module learning outcomes	Session 1. Hybrid threats: concept, definitions and wider interpretations	Session 2. Hybrid threats and security strategies	Session 3. Policy and regulation	Session 4. Warfare in the context of hybrid threats	Session 5. Information warfare	Session 6. A common response to hybrid threats and strategies for tackling them	Session 7. Research strategies and methods
critically analyse hybrid threats in the context of global, European and national security	■						■
evaluate the security strategies aiming to ensure sustainable security concepts in contemporary hybrid threats environment		■					■
discuss international and European Union policies and legal framework responding to hybrid threats, considering provisions of fundamental rights			■				
critically analyse tendencies of contemporary warfare regarding hybrid threats				■			■
critically analyse cases of information warfare and their impact on fundamental rights					■		■
independently and creatively identify problems related to hybrid threats and develop and design solutions to respond to hybrid threats using different research strategies and methods in social science research						■	■

Module 2					
Sessions / Module learning outcomes	Session 1. Crimes of a hybrid nature	Session 2. International criminal law and legal tools for tackling hybrid threats	Session 3. Prevention of hybrid threats	Session 4. Cybersecurity and cyber incidents management	Session 5. International cooperation
explain specifics of modern crimes of hybrid nature and criminal procedure concepts and their connection with principles of fundamental rights					
identify problems, recommend and elaborate tools and methods of protection against hybrid threats by working in a team and benefit from team learning processes					
explain risks related to cybersecurity and business continuity and infringement of fundamental rights					
critically analyse the importance of prevention and countering hybrid threats using relevant tools and means of cooperation					

Module 3			
Sessions / Module learning outcomes	Session 1. Common resilience-building approach against hybrid threats	Session 2. Fostering the resilience of the state and non-state actors to hybrid threats	Session 3. Protection of critical infrastructure
explain tools for fostering resilience of the state and non-state actors to hybrid threats			
explain the role of protection of fundamental rights in preparation for responding to hybrid threats including in cooperation with civil-military and other stakeholders			
selectively identify and present good practices related to the protection of critical infrastructure and strategic objects			

Module 4				
Sessions / Module learning outcomes	Session 1. European Union's external dimension in countering hybrid threats	Session 2. Border security and management	Session 3. Countering information advocacy and influence activities	Session 4. Management and leadership in the context of hybrid challenges
explain the European Union's external dimension in countering hybrid threats in collaboration with third countries, international organisations and agencies				
critically analyse the European Union's approach to internal and border security management				
evaluate the role of fundamental rights in the European Union's internal and border security management				
critically evaluate actions countering information advocacy and influence activities				
analyse and interpret psychological aspects related to radicalisation and different forms of extremism on social media				
propose combined approaches for management and leadership for encountering modern security challenges and threats based on modern theories, considering professional ethics, fundamental rights, and principles of equal treatment of diverse groups				
apply strategic communication skills in a hybrid context based on ethical values and evaluate the results				
employ appropriate tools and techniques to strategically manage civilian, human and technical resources, and make decisions in case of hybrid crises, and critically evaluate their peers' problem-solving performance				