Common Module
Hybrid Threats - Protection and Enhanced Resilience of Critical Infrastructure
Module Description

Country	Institution	Common Module	ECTS
DE	**Helmut Schmidt University**	**Hybrid Threats – Protection and Enhanced Resilience of Critical Infrastructure**	**2**

Service(s) **ALL** Language **English**	**Minimum Qualification of Instructors** • EQF-7 (or equivalent experience in public or private sector) in relevant area (Politology, Law, Engineering). • English: Common European Framework of Reference for Languages (CEFR) Level C1 or NATO STANAG Level 3 (SLP 3333).
SQF MILOF	• **Competence area** – Military Service Member. • **Learning area –** Employment of forces – full spectrum operations. • **Organisational level –** Single Arm/Branch - Joint / Multiple Service.

Prerequisites for international participants	**Contents of the Module**
• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. • Non-academic leadership training (sophomore and higher).	• Threats to both military and civilian critical infrastructure. • Risk management strategies to identify critical threats. • Common possible protection methods. • Communication while dealing with non-complete information.

Learning outcomes		
	Know-ledge	• Identify relevant ways to attack critical infrastructure. • Describe aim and fundamental basics of risk management and its application to protect valuable infrastructure assets.
	Skills	• Identify threats to critical infrastructures like power, gas, water, sewage, traffic, logistics or data networks, including to infrastructure dedicated to crisis relief, like police, firefighter, or technical relief agencies. • Practice communication with both military and civilian agencies for crisis relief.
	Respon-sibility & Autonomy	• Make autonomous decisions in coherence with the knowledge about irregular threats to infrastructure. • Experience stress under simulated crisis respond environment.

Verification of learning outcomes:

- **Test**: Multiple choice test of 28 randomised questions on the knowledge acquired at the end of the module.
- **Seminar**: Active participation in the seminar, under supervision of course director and assisting staff, with evaluation at the end of the residential phase.

To pass, the participant has to attend actively in the seminar and achieve the grade pass on the written assignment.

Created by Lars Ole Fichte, PhD / Helmut Schmidt University 13 June 2025
Revised by Col Assoc. Prof. Gell, PhD / Chairman Military Erasmus (EMILYO) Implementation Group 16 June 2025
Issued with the status of "Common" by the Implementation Group 08 July 2025

Module details		
1.1 Online preparation phase: both synchronised and independent preparation blocks to ensure best possible learning experience		
Main Topic	**Recom-mended WH**	**Details**
Introduction	1	• Online synchronised: short reading, watching, analysing, and writing assignments in preparation of the course.
Preparatory assignments	4	• Online independent: preparation of a short presentation to be given by the participant.
Total	**5**	The number of hours for the use of the developed online preparation phase content is up to the module director. He/she may replace the e-learning hours/topics with residential phases.
1.2 Workshop		
Common threats to Infrastructure	3	• Possible threats will be showcased by experts in the field and are going to be discussed in depth afterwards. • Countermeasures and safety precaution will be presented on technical and organisational level for both private and public sectors.
Risk management	3	• Concept of risk management in the context of changing threat situations is taught. • Methodology of impact analysis as the basis of resilient organisations is introduced.
Modern and evolving threats	3	• IED, nuclear, biological, chemical threats: availability, risks, and countermeasures.
Military infrastructure and its protection	2	• High power electromagnetics: availability and limitations. • UAVs as a new player.
Civilian infrastructure and its protection	2	• Protection of naval infrastructure from both electronic interference and attacks with non-military UAVs.
Seminar	(6)	• Participation in a simulation game in an allotted role; simulation is a group exercise to deal with a threat to infrastructure, based on limited knowledge.
Total (incl. point 1.1)	**24**	The detailed number of hours for the respective main topic is up to the course director according to national law or home institution's rules.
2. Additional hours (WH) to increase the learning outcomes		
Self-Studies	36	Separate hours for in-depth studies on an as-required basis. Those hours comprise work of students revisiting course documents and working through additional material provided by course staff, to improve skills and consolidate knowledge.
Total WH	**60**	

Created by Lars Ole Fichte, PhD / Helmut Schmidt University 13 June 2025
Revised by Col Assoc. Prof. Gell, PhD / Chairman Military Erasmus (EMILYO) Implementation Group 16 June 2025
Issued with the status of "Common" by the Implementation Group 08 July 2025

List of Abbreviations:

B1, B2	CEFR Levels
CEFR	Common European Framework of Reference for Languages
ECTS	European Credit Transfer and Accumulation System
EQF	English European Qualifications Framework
ESDC	European Security and Defence College
IED	Improvised Explosive Device
IG	Implementation Group
NATO	North Atlantic Treaty Organization
STANAG	Standardization Agreement
UAV	Unmanned Aerial Vehicle
WH	Working Hour

Created by Lars Ole Fichte, PhD / Helmut Schmidt University 13 June 2025
Revised by Col Assoc. Prof. Gell, PhD / Chairman Military Erasmus (EMILYO) Implementation Group 16 June 2025
Issued with the status of “Common” by the Implementation Group 08 July 2025