EUROPEAN SECURITY AND DEFENCE COLLEGE

Training Catalogue 2024-25

ESDC, Rue d’ Arlon 62, 1046, Brussels
secretariat-esdc@eeas.europa.eu

Foreword

In an era defined by dynamic security challenges and evolving defence landscapes, the European Union's commitment to ensuring peace, stability and security has never been more paramount. The European Security and Defence College (ESDC) stands at the forefront of this mission by providing targeted and cutting-edge training and education that enhances the capabilities and resilience of personnel in the context of the EU's Common Security and Defence Policy (CSDP). The ESDC, an autonomous EU body working under the overall responsibility of the EU High Representative for Foreign Affairs and under the strategic direction of the Member States, is key to ensuring the sustained success of this mission and to build the EU strategic autonomy.

This Training Catalogue has been developed with a vision to support a united, adaptable, and skilled European security and defence community. Each program within this catalogue has been crafted with precision to address the multifaceted nature of current and future security concerns, from crisis management and conflict prevention to cybersecurity and counterterrorism. Our courses integrate academic expertise, practical knowledge, and real-world experiences from an array of European and international institutions, working as a network.

We are committed to fostering a learning environment that promotes collaboration, shared expertise, and a common understanding among Europe's security and defence professionals. By engaging with these programs, participants not only enhance their professional skills but also contribute to building a cohesive and responsive network of EU Member States ready to meet the demands of a changing global environment.

As you explore this catalogue, I invite you to envision the critical role each course plays in safeguarding our common values and ensuring the continued security and prosperity of Europe and its citizens. Together, we can build a more secure and resilient future for all.

Fergal O' Regan
Acting Head of the European Security and Defence College

European Security and Defence College
Doc: ESDC/2024/276
Date: 20 October 2024
Origin: ESDC Secretariat

Contents

Register for an ESDC course – Nomination process

In order to accomplish its mission as defined in the Council Decision that established it[1], the ESDC co-organises a number of training courses in the course of each academic year. As a network college, the ESDC pools and shares resources with its network of EU and international security and defence training institutions. These training providers constitute the network of the ESDC and offer trainings to EU member states, candidate states and third country personnel, under the auspices of the ESDC.

The ESDC Training Catalogue is created every year, detailing when and where each course will take place, along with each course's aim and learning outcomes. The ESDC publishes the catalogue to help interested participants plan ahead. However, dates or even the location of a course may change during the year. Courses may be added or cancelled depending on various factors.

Interested participants should bear in mind that they can only apply for a course once it has been published on the ESDC website (https://esdc.europa.eu/courses/) and on the EEAS Schoolmaster portal (https://goalkeeper.eeas.europa.eu/goalkeeper/search), and the invitation letter has been sent.

Publication of a course usually takes place three months before the start of the course. Applications are not submitted directly, but are filed via the ESDC secure online system ENLIST by designated nominators. A list of relevant ENLIST nominators can be accessed at the ESDC website at http://esdc.europa.eu/nominators/. Nominators will nominate participants to a course, however, registrations are not considered final until confirmed by the ESDC Secretariat on the nomination deadline. In addition, participants are required to complete the necessary personal data in ENLIST. Participants from EU candidate countries or third countries can be nominated by the respective Mission to the EU in Brussels.

It should be highlighted that equal opportunities are given to all EU Member States for participation in our training courses. If a course is also open to candidate or third countries, those other countries will also be treated equally with each other, though EU nominees will have priority over them.

[1] COUNCIL DECISION (CFSP) 2020/1515 of 19 October 2020 establishing a European Security and Defence College, and repealing Decision (CFSP) 2016/2382 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1515

What the ESDC offers

Course list

The ESDC will offer the following courses in the academic year 2024-2025. Further information, such as location, dates and an overview of the learning outcomes for each course, follow in the next section. More detailed information on all ESDC courses, as well as full curricula, can be found on the ESDC webpage, https://esdc.europa.eu/esdc-courses-curricula/. In each curriculum, you will find a more detailed description of the course objectives and a detailed list of learning outcomes.

- High-Level Course
- Training of Trainers
- CSDP Orientation Course
- Strategic Planning Process of Civilian CSDP Missions
- CSDP Capability Planning and Development Course
- Basic Course on Security Sector Reform
- Core Course on Security Sector Reform
- Course on International Law for Military Legal Advisers
- Civilian Aspects of EU Crisis Management
- Advanced Course for Political Advisers in CSDP Missions and Operations
- A Comprehensive Approach to Gender in Operations
- European Armament Cooperation
- European Armament Cooperation
- Challenges of Space for CSDP
- Mediation, Negotiation and Dialogue Skills for CSDP
- Comprehensive Protection of Civilians
- CSDP Course on Building Integrity-Reducing Corruption
- Cross-Cultural Competence in CSDP Missions and Operations
- Pre-Deployment Training for CSDP Missions and Operations
- The Challenges of Securing Maritime Areas for the European Union
- EU Integrated Crisis Management
- EU Addressing and Facing Hybrid Threats and Challenges
- Monitoring, Mentoring and Advising in EU Crisis Management
- Disaster Relief in CSDP Context
- From Conflict Analysis to Integrated Action: Generating Strategies for Intervention
- Contracting in International Operations Course
- HEAT - Hostile Environment Awareness Training
- Vehicle Safety and 4x4 Driving
- Advanced Modular Training (AMT) for CSDP Strategic Crisis Management
- Climate Change and Security
- Strategic Communication for Peace, Security and Defence

- EU Logistics Fundamentals/EU Logistics in Operations Courses
- Investigating & Preventing Sexual and Gender-Based Violence in Conflict Environments
- Project Management in Support of CSDP M/O – PM2
- Senior Strategic Course
- Sectoral Qualifications Framework for the Military Officer Profession (SQF-MILOF): Familiarisation Course
- Intelligence Security Challenges and Opportunities in the EU
- Diplomatic Skills for CSDP
- Cultural Property Protection Course
- Advanced Diplomacy for Security and Defence
- European Security and Geo-Economics
- Integrated Border Management (IBM) in CSDP
- Foreign Information Manipulation and Interference
- Modern Leadership in the Context of Law of Armed Conflicts and Open-Source Intelligence
- Team and Conflict Management in Peace Operations
- Challenges of European Cybersecurity
- Computer Security Incident Response Team (CSIRT) Fundamentals
- Cybersecurity Risk Management
- The Role of the EU Cyber Ecosystem in Global Cyber Security Stability
- Cyber Diplomacy Advanced Course
- Critical Entities Resilience, Advanced
- The EU's Cybersecurity Strategy for the Digital Decade
- Cyber Range - Pentester Tools
- Cyber Range - Cybersecurity in Practice
- Course on Cybersecurity and International laws
- Basics of Cybercrime Investigation
- Countering Disinformation with Applied OSINT Techniques
- Cyber Awareness for Trainers
- Open-Source Intelligence (OSINT)
- Cyber Defence Policy at National and International Levels
- Security Operations Centre (SOC) as a Template
- Cyber Threat Management
- Cyber Incident Responder
- Penetration Tester
- Cyber Threat Intelligence
- Intelligence Analysis
- Image Intelligence Analysis (IMINT)
- Maritime Cybersecurity
- Implementation of Cybersecurity Technical Controls

- The Contribution of Cyber in Hybrid Conflict
- Cybersecurity and Smart Cities
- Cybersecurity Educator
- Digital Forensics Investigator
- Hybrid Threats and Intercultural Strategic Communication

E-Learning – Autonomous Knowledge Units (AKUs)

The ESDC enhances each course with asynchronous online e-learning, ensuring participants acquire essential knowledge before attending the in-person sessions. These Autonomous Knowledge Units (AKUs) offer an interactive learning experience, covering material that would otherwise take valuable time during the course. Participants will also complete simple tests to improve their understanding. It is important to note that completing these AKUs is mandatory and a prerequisite for receiving the official ESDC certificate on completing a course. To facilitate participants' e-learning, the ESDC hosts its own online learning management system where, apart from AKUs, all other information on a course is uploaded for participants to find.

Course Details

ESDC Regular Courses

CSDP High-Level Course (Activity No 1) – Modular Course

Location: Brussels, Larnaca, Bucharest, Lisbon

Dates: 23-27/9/2024, 25-29/11/2024, 7-11/4/2025, 23-27/6/2025

Course aim

The Common Security and Defence Policy (CSDP) High-Level Course (HLC) aims to equip senior experts from EU Member States, candidate countries and EU institutions with the skills necessary to lead and advance the CSDP. Participants will gain expertise in policy implementation, crisis management and capability development within the broader framework of the Common Foreign and Security Policy (CFSP). The course emphasises collaboration with diverse stakeholders and deepens participants' understanding of the EU's security and defence architecture, focusing on the integrated approach to CSDP as a key tool of the CFSP. It addresses both current and emerging policies, missions, and operations, while raising awareness of new threats and broader challenges. Delivered through a combination of e-learning and residential modules, the course fosters a shared European security culture and develops a network of future leaders engaged in the strategic dimensions of CFSP/CSDP. Additionally, it promotes the creation of a strong network of experts in this field.

Learning outcomes

The learning outcomes focus on a comprehensive understanding of the EU's CFSP and CSDP, emphasising both knowledge and practical application. Students will explore the long-term objectives of CFSP/CSDP, the role of EU institutions and the capability development processes, while understanding decision-making for missions and crisis management, including the broader impact of issues such as human rights, climate, and cybersecurity. They will evaluate the EU's interests and values, analyse strategic documents, and engage in political decision-making simulations. Additionally, students will explore opportunities for enhanced coordination among EU institutions and external actors, with a focus on improving military and civilian capabilities and addressing the synergies between civilian and military components. By assessing the effectiveness and challenges of the EU's approach to foreign and security policy, they will critically evaluate current and future developments, promote institutional strengths, and engage in dialogue about the future of CFSP/CSDP, considering operational engagement and capability development at both strategic and regional levels.

Target audience

Participants should be senior experts from EU Member States, candidate countries and EU institutions, bodies and agencies (military and civilians, including diplomats, police, and border guard officers) who are either working in key positions or have clear potential to achieve leadership posts, in particular in the field of CFSP/CSDP. Members of academia, NGOs and the business community may apply to participate. The audience should be a well-balanced mix of civilians and military personnel. Course participants must be available for the whole course, which includes e-learning phases and residential modules, and must be ready to contribute with their specific expertise and experience throughout the course. For participation in the HLC, personal security clearance to at least EU CONFIDENTIAL level is mandatory. It is recommended that course participants have already attended the ESDC CSDP Orientation Course.

Course open to

- EU Member States - Institutions
- Candidate countries that have security agreements with the EU
- International organisations
- NGOs

Training of Trainers (Activity No 2)

Location	***Dates***
Brussels, Belgium	*1 April – 14 July 2025*
Brussels, Belgium	*29 July – 2 August 2025*

Course aim

Training drives change and improvement, its impact, if executed effectively, extending well beyond the training session itself. This course is designed to equip participants with the ability to transfer expertise and knowledge to their specific target groups. It emphasises the 'how' of teaching and training rather than just the 'what', focusing on methodology skills that can be applied to various content areas. By providing foundational knowledge in methodology and didactics within a practical framework, the course offers a comprehensive toolbox for effective training.

Learning outcomes

The learning outcomes cover essential aspects of training and teaching methodologies. They include defining the training cycle, methodology, and didactics, and understanding how learning occurs, including different learning styles and types of learners. The outcomes explain the relationship between learning and teaching, communication processes, outcome-based learning, and the principle of constructive alignment. They also address adult learning principles, compare trainer-centred and trainee-centred approaches, and distinguish between passive and participatory teaching methods. Participants will learn how to give and receive constructive feedback, use the JOHARI window for self-awareness, and consider cultural and environmental influences on training. Additionally, they will explore mechanisms for evaluating training, develop learning objectives and lesson plans, apply feedback principles, use media effectively, and demonstrate delivery skills, all while assessing available resources for training.

Target audience

Participants may include both experienced and inexperienced trainers from civilian, police, and military sectors who are involved in learning activities at both national and international levels. Priority is given to individuals from EU Member States, but non-EU citizens and NATO staff are also welcome.

Course open to

- EU Member States - Institutions
- EU candidate countries
- Third countries and international organisations

CSDP Orientation Course (Activity No 3)

Location	***Dates***
Brussels, Belgium	*16-20 September 2024*
Sofia, Bulgaria	*7-11 October 2024*
Lisbon, Portugal	*7-11 October 2024*
Brussels, Belgium	*11-15 November 2024*
Brussels, Belgium	*3-7 March 2025*
Thessaloniki, Greece	*17-21 March 2025*
Rome, Italy	*24-28 March 2025*
Brussels, Belgium	*19-23 May 2025*
Larnaca, Cyprus	*26-30 May 2025*
Warsaw, Poland	*26-30 May 2025*
Madrid, Spain	*9-13 June 2025*
Brussels, Belgium	*16-20 June 2025*

Course aim

The course aims to offer participants a comprehensive understanding of the CSDP, including its institutional framework, current policies, structures, processes, and activities. Participants will also have the opportunity to network with others in the CSDP field. Ultimately, the CSDP Orientation Course seeks to assist EU Member States and EU institutions in training their personnel to operate effectively in CSDP-related roles at both operational and strategic levels.

Learning outcomes

The learning outcomes focus on understanding the EU‘s organisational structure, decision-making processes, and its approach to external conflicts and crises. Participants will explore the objectives of the EU Global Strategy, principles of CSDP missions, and the Civilian CSDP Compact. They will also review the capability development mechanism and national processes, partnerships with third countries, and the EU‘s role in the international community. Additionally, the course covers lessons learned, civilian-military coordination, and the integrated approach in CSDP missions. Participants will analyse when and why CSDP missions are needed, compare lessons identified, and adapt CSDP strategies to future challenges.

Target audience

Participants would normally be entry and mid-level staff from Member States (MS) and EU institutions and agencies, with some previous experience in security policy matters.

Course open to

- EU Member States - Institutions
- EU candidate countries
- Third countries and international organisations

Strategic Planning Process of Civilian CSDP Missions (Activity No 7)

Location: Brussels, Belgium

Dates: 9-13 June 2025

Course aim

The course aims to equip participants with the knowledge and skills needed for strategic planning in civilian CSDP missions, with a focus on EU capabilities within the integrated approach. It emphasises key tools and skills for strategic planning at the EU level, particularly in the context of civilian CSDP.

Learning outcomes

The course aims to provide participants with an understanding of EU and CSDP structures, decision-making, and planning processes within the CFSP. It emphasises the EU integrated approach, covering key planning documents like PFCA and CMC, and highlights the importance of incorporating lessons learned from civilian CSDP missions. Participants will learn about conflict analysis, crisis response, and integrating concerns such as gender, human rights and civilian protection in planning. They will explore sector-specific civilian CSDP areas (e.g. police, rule of law), the security-development nexus and cooperation with international actors. Additionally, they will gain skills in strategic planning, assessing situational threats and drafting planning documents for civilian CSDP missions, while suggesting improvements to enhance the impact of EU missions.

Target audience

Participants should be senior civilian, police and military personnel engaged in planning at strategic level in relevant authorities of the Member States or likely to be deployed to a relevant EU crisis management structure or to a senior post in a CSDP mission or operation.

Course open to

- EU Member States -Institutions

CSDP Capability Planning and Development Course (Activity No 8)

Location: Brussels, Belgium
Dates: 22-25 October 2024

Course aim

This course aims to foster a shared understanding of the EU's civilian and military capability planning and development processes, highlighting the roles of EU Member States, institutions and agencies. It focuses on the EU's capability needs and trends, emphasising efforts to enhance strategic autonomy through the Strategic Compass and Civilian CSDP Compact. The course covers the methodology behind CSDP capability planning, aligned with the Headline Goal Process (HLGP) and Civilian CSDP Compact, and examines the key outcomes. On the defence side, it explores links to national defence planning and EU initiatives (e.g. Capability Development Plan (CDP), CARD, Permanent Structured Cooperation (PESCO), European Defence Fund (EDF)), while on the civilian side, it connects with relevant developments across Member States and EU services.

Learning outcomes

Participants will gain a comprehensive understanding of the military and civilian capability planning and development processes at the EU level, covering strategic, political, legal, and budgetary frameworks. The course explains the roles of major actors, including EU Member States, EDA, EEAS, EUMC and others, in the decision-making process. It explores key EU defence initiatives such as the CDP, PESCO and the EDF, along with the Headline Goal (HLG) process and its products (e.g. requirements catalogue and force catalogue). Participants will also discuss the EU's Defence Technological and Industrial Base (EDTIB) and civilian capability development, including the Civilian CSDP Compact and its commitments. Finally, the course focuses on applying these processes at the national level to support CSDP missions and operations, contributing to EU capability goals.

Target audience

The participants should come from relevant ministries of the EU Member States and the EU institutions and agencies, and will preferably have some basic knowledge of CSDP and some experience in the field of capability planning and development.

Course open to

- EU Member States - institutions

Basic Course on Security Sector Reform (Activity No 10)

Location	***Dates***
Turin, Italy	*24-29 September 2024*
Chisinau, Moldova	*23-25 October 2024*
Tbilisi, Georgia	*24-29 November 2024*
Brussels, Belgium	*3-5 December 2024*

Course aim

This course offers a comprehensive understanding of Security Sector Reform (SSR) as a concept, including its principles and objectives and its role within the EU integrated approach. It emphasises the political dimension of SSR and highlights the importance of inclusive, nationally owned processes. The course provides an overview of the EU-wide strategic framework for SSR, focusing on how SSR support is implemented and coordinated internally and with other relevant actors to meet EU mandates. Additionally, it seeks to build a network of SSR experts, encouraging participants to share insights and lessons learned on the EU's integrated approach to SSR.

Learning outcomes

The course focuses on the foundational principles of SSR as a context-specific, nationally owned, and politically driven process rooted in human rights, democracy, and the rule of law. Participants will learn to define and distinguish between security, the security sector, and SSR, while understanding the importance of a human security approach. The course outlines the holistic implementation of SSR, covering governance, oversight, and the involvement of diverse state and non-state actors. It also emphasises key international policy frameworks, particularly the EU's role in SSR through its strategic framework. Other key topics include gender-responsive SSR, the SSR-DDR nexus, and the role of coordination for coherent EU support. Participants will analyse practical lessons from SSR, apply EU SSR policies in CSDP missions, and advocate for the integration of gender perspectives and the EU's integrated approach to external conflicts.

Target audience

Participants should preferably be involved in the planning, implementation or management of CSDP missions and operations or in the EU Commission projects in support of areas relevant to SSR. Priority is given to personnel from EU Member States.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Core Course on Security Sector Reform (Activity No 11)

Location	***Dates***
Stadschlaining, Austria	*4-10 October 2024*
Brussels, Belgium	*2-5 December 2024*
Vienna, Brussels	*28 March – 03 April 2025*

Course aim

The course aims to enhance participants' knowledge, skills, and competencies in Security Sector Reform (SSR) within the context of the EU's integrated approach, focusing on key EU policies such as the 'EU-wide Strategic Framework in Support of SSR,' the 'Civilian CSDP Compact,' and the 'Strategic Compass for Security and Defence.' It highlights the core components of SSR, the tools and techniques used by practitioners, and the challenges faced by SSR experts. The course will also promote sharing of good practices and provide participants with tools to address future challenges and assess SSR needs. Additionally, it seeks to strengthen a network of SSR experts with a shared understanding of EU SSR principles and actions.

Learning outcomes

Participants will explore key concepts related to human security, the security sector, and SSR and governance. The course covers the evolution of SSR, its principles, and the political nature of the reform process. Emphasis is placed on EU policy frameworks, such as the SSR Strategic Framework, Civilian CSDP Compact, and Strategic Compass, while also introducing relevant UN, OSCE, and NATO policies. The course addresses SSR challenges in post-conflict, fragile environments and highlights cross-cutting issues such as human rights, gender, and good governance.

Participants will develop practical skills in the assessment, design, implementation, and evaluation of SSR missions, translating strategic objectives into operational actions. They will also learn how to navigate the political dimensions of SSR, improve collaboration with national and international actors and identify key success indicators for monitoring SSR programmes. Case studies, exercises, and field examples will deepen their understanding of SSR challenges, approaches, and lessons learned, enhancing their ability to apply this knowledge in practice as SSR practitioners.

Target audience

Participants should preferably be middle- to senior-level civilian or military experts deployed or just about to be deployed in support of a CSDP or bilateral, regional or multilateral mission or operation to support security and justice reform within EU or EU Member State and/or partner-country structures. The course is also open to those involved in programming, programme management and/or in political/policy dialogue in the wider context of SSR, including EU partner countries. Priority is given to personnel from EU Member States and EU institutions.

Course open to

- EU Member States – institutions
- EU candidate countries
- Third countries and international organisations

Course on Recovery and Stabilisation Strategies (Activity No 14)

Location: Stadtschlaining,, Austria

Dates: 8-12 May 2025

Course aim

The aim of the course is to equip participants with a thorough understanding of recovery and stabilisation strategies by identifying operational challenges and providing tools to address them. It promotes co-operation among various actors, including international organisations, governments, civil society, and NGOs, using a "3C" (coherent, coordinated, complementary) approach, particularly fostering collaboration between the UN and EU. The course also provides networking opportunities for peacebuilding professionals.

Learning outcomes

By the end of the course, participants will be able to explain the rationale behind the Common Security and Defence Policy (CSDP) and its role in civilian crisis management, along with understanding the structures, instruments, and decision-making processes of key organizations like the EU, NATO, UN, and OSCE. They will also be able to compare the crisis management approaches of these institutions. The course will emphasize the multi-dimensional nature of peacebuilding, the importance of a whole-of-government approach, and the opportunities and challenges of civil-military interactions.

Participants will gain a solid understanding of key concepts like local ownership, sustainability, human rights, human security, and the protection of civilians. They will be able to analyze conflicts, identify lessons learned, and develop recovery and stabilization strategies, coordinating efforts among various stakeholders. Additionally, they will be equipped to justify international engagement in peacebuilding, apply integrated approaches to strategic recovery planning, and enhance their conflict analysis skills to design more effective recovery and stabilization strategies.

Target audience

Participants will come from EU institutions, EU Member States and EU candidate countries. A limited number of slots will be allocated to participants from NATO, U OSCE structures. Participants may be civilian, military or police staff.

Participants should be working in a post-conflict recovery context at strategic level or be in charge of policy-level programming for long-term stabilisation strategies in peace operations.

Course open to

- EU Member States – institutions
- EU candidate countries
- NATO and OSCE

Course on International Law for Military Legal Advisers (Activity No 15) – Modular course

Location: Vienna, Austria – Seebenstein, Austria – Reichenau, Germany

Dates: 2-6 December 2024, 24-28 March 2025, 5-9 May 2025

Course aim

The Course on International Law for Military Legal Advisers aims to enhance participants' knowledge and understanding of international operational law and international humanitarian law (IHL). Through a practical exercise simulating an EU-led military crisis management operation (CMO), participants will gain insight into the role of a legal adviser in a multilateral context. The course fosters information-sharing, collaboration, and cooperation among military and civilian personnel from different countries, further strengthened by rotating syndicate groups. Additionally, the course helps establish a network of legal advisers, promoting professional cooperation between armed forces and ministries of defence.

Learning outcomes

Participants will learn to identify and address the legal implications of situations during military CMO operations. They will develop the ability to analyse relevant legal questions, interpret and apply applicable laws, and assess potential legal consequences of commanders' decisions. The course emphasises drafting legal solutions, prioritising issues on the basis of urgency, and improving oral legal presentation skills. Participants will also learn how to coordinate within a team of legal advisers, evaluate the problem-solving process, and provide concise legal advice to support commanders' decision-making.

Target audience

Participants should be military lawyers or civilian legal advisers in the armed forces or ministries of defence, particularly those who have been or are to be assigned to military CMO as legal advisers. Participants must be available for the whole course, which includes e-learning and residential modules, and must be ready to actively contribute throughout the course.

Course open to

- EU Member States – institutions
- EU candidate countries
- Third countries and international organisations

Civilian Aspects of EU Crisis Management (Activity No 17)

Location: Brussels, Belgium

Dates: 6-8 May 2025

Course aim

This course aims to cultivate a comprehensive understanding of the civilian dimensions of EU crisis management among personnel from Member States, EU institutions and relevant EU agencies. It seeks to deepen participants' grasp of the EU crisis management decision-making framework and highlight essential CSDP instruments, such as the Civilian Compact, Strategic Compass, and lessons learned initiatives. Additionally, the course will explore contemporary and future trends, challenges, and opportunities in civilian crisis management, emphasising the importance of establishing sustainable partnerships with international organisations, regional entities and local actors. Ultimately, the course is designed to foster a network of experts dedicated to enhancing effectiveness in crisis management.

Learning outcomes

The learning outcomes of this course focus on equipping participants with a comprehensive understanding of EU crisis management. Participants will learn to articulate the EU crisis management decision-making process and analyse the influence of key EUGS concepts such as 'ownership,' 'resilience,' and 'sustainability' on effective crisis management. The course will also cover the roles of various governmental and non-governmental actors, their interoperability within CSDP missions, and the significance of long-term trends in shaping EU policy.

Additionally, participants will explore critical CSDP instruments like the Civilian Compact and the Strategic Compass, as well as the financial mechanisms underpinning EU crisis management missions. They will assess the importance of gender considerations and human rights within CSDP operations and develop strategies for enhancing crisis prevention and management efficiency. Overall, the course aims to foster improved coordination among stakeholders, promote the application of intercultural communication principles in diverse environments and prepare participants to critically analyse and contribute to EU crisis management initiatives.

Target audience

Participants should preferably be mid- and senior-level experts, including civilians and military staff, engaged in fields related to crisis management within the broader framework of CFSP/CSDP. This includes those currently involved in crisis areas or potential future staff for CSDP missions or operations. Priority will be given to participants from EU Member States, although non-EU participants and NATO staff are also welcome.

Course open to

- EU Member States – institutions
- EU candidate countries
- Third countries and international organisations

Advanced course for Political Advisors in CSDP Missions and Operations (Activity No 18) – Modular course

Location: Rome, Italy - Geneva, Switzerland – Vienna, Austria

Dates: 12-16 May 2025, 10-13 June 2025, 7-11 July 2025

Course aim

This course is designed to equip participants with a comprehensive understanding of the roles and challenges faced by political advisers in CSDP missions and operations, at both operational and strategic levels. Participants will explore the core principles of the EU's external action, along with essential skills and methodologies for effective advising in both capitals and field settings. Through practical training exercises, the course aims to enhance participants' existing skills and facilitate the development of professional networks among those in advisory roles.

Learning outcomes

After completing the course, participants will be able to articulate the primary goals of the CSDP and identify its key actors. They will gain insights into crisis management guidelines, the decision-making process, and the specific responsibilities of political advisers. Participants will also learn to use strategic communication tools, understand the dynamics of advising various stakeholders, and apply EU interests and values in their decision-making. Additionally, they will differentiate between types of CSDP missions, assess the pros and cons of the value-based approach', and distinguish between humanitarian and CSDP actions. By practising negotiation and mediation techniques, participants will develop a heightened awareness of the CSDP‘s role in the EU‘s integrated approach and its achievements as a global actor, while also identifying areas for improvement in crisis management procedures.

Target audience

Participants should be working in political advisory positions/departments in Member States, EU institutions and agencies, or CSDP missions and operations. Subject to national decision, they can be academics, civilians, diplomats, members of the business community, military and police. Selection of the course participants is the responsibility of the organisers. The course organisers recommend that course participants have attended the ESDC CSDP Orientation Course.

Course open to

- EU Member States – institutions

A Comprehensive Approach to Gender in Operations (Activity No 21)

Location	***Dates***
The Hague, Netherlands	*25-29 November 2024*
Ljubljana, Slovenia	*10-14 March 2025*
Madrid, Spain	*23-27 June 2025*

Course aim

This course is designed to enhance operational effectiveness by equipping participants with the knowledge and skills necessary to effectively integrate a gender perspective into CSDP and international missions. Aligned with the EU's Strategic Compass, the Civilian CSDP Compact, and the Training Requirements Analysis on Gender Equality for Civilian CSDP, the course focuses on actionable strategies for embedding gender considerations into mission planning and execution.

Learning outcomes

Participants will emerge from the course with a robust understanding of the significance of a gender perspective in peace operations, as well as the challenges and dilemmas faced by decision-makers in the field. They will be able to articulate the core principles of the EU Strategic Compass and the Civilian CSDP Compact, and recognise the relevant international legal frameworks related to gender equality and Women, Peace and Security (WPS). By identifying the diverse security needs of local populations, participants will learn to effectively apply gender analysis in various operational contexts, from border management to Security Sector Reform.

Additionally, participants will develop the skills to translate policy into actionable plans, address sexual and gender-based violence, and create pathways for women's meaningful participation in conflict resolution and reconstruction efforts. They will also learn to assess their own biases and how these may influence their strategic leadership. Ultimately, participants will be equipped to advocate for gender equality within their teams and organisations, ensuring that gender perspectives are integrated throughout the mission lifecycle, thus contributing to more effective and inclusive operations.

Target audience

Participants should be middle-management military and civilian officials, including police and diplomats, from EU Member States, as well as from EU institutions, relevant agencies, missions and operations, who are assigned to or interested in participating in (future) CSDP, NATO, OSCE or UN missions or operations, or who are to be assigned to a position in a fragile state.

Course open to

- EU Member States – institutions
- EU candidate countries
- Third countries and international organisations

European Armament Cooperation – Awareness Level (Activity No 25a)

Location: Brussels, Belgium
Dates: 30 September – 2 October 2024

Course aim

The European Armament Cooperation (EAC) Course aims to enhance mutual understanding of armament cooperation by analysing the armaments sector and identifying its frameworks, stakeholders, tools and processes. Participants will explore the challenges and benefits associated with armament cooperation at the EU level. The course is designed to equip EAC staff and managers with the knowledge and skills necessary to contribute effectively to international armament cooperation projects within the evolving context of the CSDP.

Learning outcomes

After completing the course, participants will be able to identify the key stakeholders in armament cooperation and articulate their roles within this complex sector. They will understand the political and economic environments that shape armament cooperation and describe existing frameworks that govern these interactions. Participants will learn to apply principles of strategic management, use common tools, and recognise best practices and lessons learned in the field.

In addition, the course will cover the essential soft skills needed for effective collaboration, including cultural awareness. Participants will gain insight into relevant European and international legislation, agreements, and treaties, and will be able to explain the structures, processes, and roles of European institutions and other actors in the armaments sector. Finally, they will explore current trends in capability development, research and technology and industrial development, equipping them to contribute meaningfully to armament cooperation initiatives.

Target audience

The course is aimed at personnel working in national and international armament-cooperation-related posts who need to gain solid knowledge in cooperative acquisition and project management, and supports experts for future leadership positions in the wider defence area.

Course open to

- EU Member States – institutions
- Countries that have security agreements with the EU

European Armament Cooperation – Expert Level (Activity No 25b)

Location: Sofia, Bulgaria
Dates: 11-15 November 2024

Course aim

The aim of the EAC Expert-Level Course is to deepen mutual knowledge in armament cooperation through critical analysis of the armaments sector. Participants will explore the frameworks, stakeholders, tools, and processes involved, while understanding the associated challenges and benefits at the EU level. The course is designed to prepare EAC managers to manage international armament cooperation projects 29kilfully and efficiently within the evolving context of the CSDP.

Learning outcomes

Participants will emerge from the course with the ability to clearly explain the key stakeholders in armament cooperation and their roles. They will gain an understanding of the political and economic environments that influence armament cooperation, as well as the existing frameworks governing these activities. The course will cover the principles of strategic management and common tools, enabling participants to identify best practices and lessons learned in the field.

Additionally, participants will learn to interpret and implement a harmonised vocabulary related to armament cooperation, employ essential soft skills and foster cultural awareness. They will also engage with European and international legislation, agreements and treaties, assessing the structures, processes and roles of European institutions and other relevant actors. Finally, participants will analyse current trends in capability development, research and technology, and industrial development, equipping them to effectively contribute to international armament cooperation initiatives.

Target audience

The course is aimed at personnel working in national and international armament-cooperation-related posts who need to gain knowledge in cooperative acquisition and project management, and prepares experts for future leadership positions in the wider defence area.

For participation in the expert level course, prior completion of the Awareness-level course is highly recommended.

Course open to

- EU Member States – institutions
- Countries that have security agreements with the EU

Challenges of space for CSDP (Activity No 27)

Location	***Dates***
Rome, Italy	*21-24 October 2024*
Paris, France	*11-13 February 2025*

Course aim

This course aims to enhance awareness among civilian and military officials from EU institutions, relevant agencies, and Member States regarding the significance of space activities within the framework of the CSDP. Participants will gain a comprehensive overview of international space policies, emphasising the strategic importance of space from a security and defence perspective. The course also facilitates networking among professionals in the space sector and encourages the sharing of national perspectives and strategic analyses, thereby reinforcing common situational awareness of space threats across the EU.

Learning outcomes

By the end of the course, participants will be able to articulate the complexities and extensive challenges associated with space activities, including various threats and risks. They will understand the conceptual framework surrounding European space activities and policies, and recognise the contributions of both the EU Space Programme and national programmes to the European Defence Technological and Industrial Base (EDTIB).

Participants will identify key policies and concepts related to space activities, and recall current trends in space programmes and political initiatives. They will become familiar with the EU institutions and bodies involved in space, along with their roles and coordination efforts. The course will enable them to evaluate the potential impacts of space challenges on the EU and the CSDP, as well as to apply relevant international and national legislation. Furthermore, participants will learn to leverage the EU's strategies and policies related to space issues, demonstrating the EU's capabilities in supporting CSDP missions and operations. They will also assess how space issues affect the EU and its Member States, propose informed views on related political orientations, and recommend a cohesive approach to the EU Space Strategy for Security and Defence.

Target audience

Participants should be mid-ranking to senior officials from EU Member States and EU institutions dealing with strategic and operational aspects of space activities. They should either be working in key positions or have clear potential to achieve leadership positions, in particular within space-programme-conducting services at governance level. Academics and members of the business and private sector community from EU Member States may also be invited to participate.

Course open to

- EU Member States – institutions

Mediation, Negotiation and Dialogue Skills for CSDP (Activity no 28)

Location: Larnaca, Cyprus

Dates: 10-14 March 2025

Course aim

This course aims to enhance participants' negotiation skills and their ability to utilise the mediation process to assist others in preventing, managing, and resolving conflicts. Through practical simulations, participants will have the opportunity to apply their learned skills to relevant international peace-building scenarios, bridging theory and practice effectively.

Learning outcomes

After completing the course, participants will be able to explain alternative dispute resolution techniques, particularly mediation, negotiation, and dialogue, and appreciate their applications within CSDP operations, including internal disputes. They will identify the underlying methodologies and concepts that support these skills and learn specific mediation techniques tailored to various contexts.

Participants will practice essential skills such as generating constructive options, analysing situations, active listening, and facilitating discussions with local stakeholders while navigating intercultural communication challenges. They will learn to manage crises in both professional and personal environments, communicate effectively during adversity, and address issues related to freedom of movement, human rights, and gender in CSDP missions. Additionally, they will apply basic conflict analysis tools to different scenarios and be prepared to play an active role in conflict prevention and crisis management efforts.

Target audience

Participants should be members of the EEAS, public servants from defence, justice, diplomatic services, police and military establishments, or personnel who are already deployed or will be deployed to civilian and military CSDP missions and operations, who wish to become familiar with mediation, negotiation and dialogue skills for CSDP crisis management activities.

Course open to

- EU Member States – institutions
- EU candidate countries
- Third countries and international organisations

Comprehensive Protection of Civilians (Activity No 30)

Location	***Dates***
Menges, Slovenia	*21-25 October 2024*
Stadschlaining, Austria	*18-22 November 2024*
Vienna, Austria	*19-23 May 2025*

Course aim

This course aims to provide participants with a comprehensive and critical understanding of the various dimensions and meanings of the protection of civilians (PoC) in armed conflict and crisis areas. It enhances knowledge of the EU's integrated approach to conflict and crisis management, while promoting information-sharing, collaboration, and cooperation among military, civilian crisis management, humanitarian, and development aid actors within the framework of the CFSP and the CSDP. The course offers an invaluable opportunity for networking and exchanging perspectives with professionals from diverse institutional, geographical and cultural backgrounds, all dedicated to improving PoC in complex environments.

Learning outcomes

By the end of the course, participants will be able to explain the concept of PoC and related terminology, as well as different approaches taken by international actors such as the EU, UN, NATO and the ICRC. They will understand PoC-related legal instruments, including international humanitarian law (IHL), international human rights law and international refugee law, and recognise institutional standards for protection planning and execution.

Participants will identify the roles and responsibilities of various actors, including civilian, police, military personnel, NGOs and development partners during and after armed conflict, and will articulate the challenges faced by these decision-makers in the field. They will develop the skills to plan, execute and supervise effective protection measures for civilians and contribute to international crisis management efforts. Furthermore, participants will be able to produce threat and risk assessments for vulnerable civilian groups and analyse conflict contexts to devise context-sensitive strategies to enhance civilian safety.

They will also summarise the key concepts and principles guiding PoC, recognise the importance of cooperation and networking among actors in this field, and compare lessons learned from previous operations that focused on protection mandates and civilian casualty mitigation.

Target audience

Participants (maximum 30) are selected from EU, UN and other international experts and decision-makers of the armed forces (battalion level and above), police (senior police officers), civil society (heads of substantive section and above), political institutions, civilian administrations and international organisations (heads of division/department and above), with relevant experience in peacekeeping, peace-building or international crisis management.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

CSDP Course on Building Integrity-Reducing Corruption (Activity No 31)

Location: Tbilisi, Georgia

Dates: 7-11 June 2025

Course aim

This course aims to enhance participants' understanding of corruption risks and equip them with the tools to develop measures to mitigate corruption in the context of CSDP missions and operations. By focusing on identifying vulnerabilities and implementing integrity strategies, the course seeks to foster a culture of accountability and transparency within defence and security frameworks.

Learning outcomes

After completing the course, participants will be able to categorise and evaluate corruption risks within the defence and security sector, including areas such as human resource management and public financial management. They will understand the intricacies of corruption risks throughout the procurement cycle and be able to assess civil-military interactions at the political level regarding governance in the defence sector.

Participants will also examine the role of media and strategic communications in combating corruption and will gain insights into the legal frameworks necessary for developing and sustaining integrity strategies aimed at reducing corruption risks. They will learn to identify ethical values and expected behaviours relevant to CSDP missions and operations, as well as methods for building integrity and facilitating organisational change.

Additionally, participants will be equipped to compare lessons learned and best practices in fostering integrity within CSDP missions and operations, thereby enhancing their capability to effectively reduce the risk of corruption in their respective contexts.

Target audience

Participants should be experts (civilians and military personnel) working in areas related to crisis management in the wider context of CFSP/CSDP or already in a post-crisis area. They could also be prospective participants in future CSDP missions and operations. Priority is given to EU Member State personnel deploying to CSDP missions and operations.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Cross-Cultural Competence in CSDP Missions and Operations (Activity No 32)

Location	***Dates***
Kilkis, Greece	*9-13 December 2024*
Kilkis, Greece	*3-7 February 2025*

Course aim

The aim of this course is to equip participants with a comprehensive set of cross-cultural knowledge and skills essential for effective engagement in CSDP missions and operations. Additionally, the course seeks to establish a network of personnel who possess cross-cultural competence, fostering collaboration among diverse cultural backgrounds.

Learning outcomes

By the end of the course, participants will understand the internal diversity and heterogeneity within cultural groups, recognising their own assumptions, stereotypes, and biases. They will appreciate how language and cultural affiliations shape perceptions and experiences. Participants will develop communicative awareness, gaining insights into how different languages and cultural conventions express ideas uniquely.

The course will enhance participants' intercultural competence through education, encouraging them to consider multiple perspectives (multi-perceptivity) and discover information about various cultural affiliations. They will learn to interpret and relate to other cultural practices, beliefs and values, fostering empathy and cognitive flexibility in adapting their thinking to different contexts.

Participants will be trained to deal with communication breakdowns, employ inter-comprehension to bridge language barriers, and act as mediators in intercultural exchanges. They will cultivate openness to learning from diverse cultural perspectives, question preconceived notions of normality, and develop tolerance for ambiguity and uncertainty. Ultimately, participants will be empowered to seek opportunities for engagement and cooperation with individuals from varied cultural backgrounds, enhancing their effectiveness in multicultural environments.

Target audience

Participants would normally be mid- to high-level personnel (civilian, police and military) from Member States and EU institutions and agencies who are assigned to or are interested in participating in CSDP missions and operations.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Pre-deployment Training for CSDP Missions and Operations (Activity No 33)

Location	***Dates***
Brussels, Belgium	*14-18 October 2024*
Brussels, Belgium	*4-8 November 2024*
Brussels, Belgium	*2-6 December 2024*
Brussels, Belgium	*3-7 February 2025*
Brussels, Belgium	*3-7 March 2025*
Brussels, Belgium	*31 March – 4 April 2025*
Brussels, Belgium	*5-9 May 2025*
Brussels, Belgium	*2-6 June 2025*
Brussels, Belgium	*30 June – 4 July 2025*

Course aim

This course aims to fulfil the 2017 EU Policy for CSDP Training requirement that all personnel assigned to CSDP missions or operations receive pre-deployment training as a prerequisite to their deployment. It is designed to complement national mission-preparatory training efforts, serving as a foundational requirement to enhance mission effectiveness. The pre-deployment training (PDT) will be complemented by induction training on arrival in the field, fostering a unified management culture within CSDP missions and ensuring that participants are well prepared to integrate into mission life and become operational quickly.

Learning outcomes

After completing the course, participants will be able to discuss the EU's role in security and defence, particularly in relation to the CFSP and the CSDP. They will identify the objectives of the EU Global Strategy and Strategic Compass, describe the EU integrated approach to external conflict and crisis, and explain the organisational structures and decision-making processes related to CSDP.

Participants will learn about crisis management procedures, cooperation between civilian and military components and the roles of EU delegations and partners on the ground. They will also understand principles of local ownership, sustainability, the Women, Peace and Security (WPS) agenda and human rights mainstreaming in CSDP missions.

In addition, participants will be able to describe the flow of information between headquarters and the field, the roles of mission support at various levels and the command-and-control principles related to duty of care. They will explore the EU's approach to Security Sector Reform (SSR), relevant EU Commission projects, environmental and climate considerations and the protection of cultural heritage within a CSDP context.

The course will enable participants to apply intercultural communication principles, gender analysis, youth-sensitive conflict analysis and the basics of monitoring, mentoring, and advising (MMA). They will also practice mediation, negotiation and dialogue (MND) as conflict resolution tools.

Participants will learn to analyse the necessity of CSDP missions, perform effectively in international and multicultural environments, and integrate gender perspectives into their daily tasks. Additionally, they will be equipped to implement mission mandates aligned with an integrated approach to internal and external security, utilise mission-planning documents, comply with safety regulations, and operate within a command-and-control structure while adhering to the Generic Standards of Behaviour and Code of Conduct.

Target audience

Seconded and international contracted civilian and military staff who have been selected to be deployed to a CSDP mission/operation. This includes staff not from EU Member States and NATO staff contributing to CSDP missions and operations. Subject to availability of seats, the course is open to candidates in Member States working on CSDP mission or operation matters.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

The challenges of securing maritime areas for the European Union (Activity No 36)

Location	***Dates***
Thessaloniki, Greece	*21-24 October 2024*
Toulon, France	*28-30 April 2025*

Course aim

This course aims to equip military officers and civil servants from EU Member States, institutions, and agencies for roles related to maritime security policies, strategies, and operations at the executive staff level. Participants will become familiar with the diplomatic, institutional, legal and operational aspects of the EU Maritime Security Strategy (EUMSS). Additionally, the course seeks to establish a network of practitioners in the maritime security field across EU Member States and institutions.

Learning outcomes

Participants will learn to describe the organisation and principles of EU institutions involved in the EUMSS and outline its main goals and strategic maritime interests. They will identify threats, challenges and risks in maritime areas and summarise the legal frameworks governing EU actions at sea. The course will cover civil and military options under CSDP, assess the strategic impact of EU maritime missions, and evaluate interactions between climate change and ocean dynamics.

Additionally, participants will benchmark maritime security approaches across EU countries, understand the lessons learned from crisis management (e.g. COVID-19), and consider the environmental impacts of EU maritime actions. They will also develop skills needed to actively contribute in international contexts and lead working groups focused on geostrategic studies.

Target audience

The course is designed for and exclusively open to mid- to senior-level staff from EU MS, EU institutions and agencies dealing with or responsible for maritime security and defence issues.

Course open to

- EU Member States - institutions

EU Integrated Crisis Management (Activity No 37)

Location: Helsinki, Finland

Dates: 23-27 September 2024

Course aim

This residential course aims to deepen participants' knowledge and understanding of crisis management within the framework of the EU integrated approach to external conflicts and crises. It fosters interactive collaboration and situational awareness among military and civilian actors, equipping senior officers with the skills necessary to perform their duties effectively under the CSDP.

Learning outcomes

Participants will learn to describe the key principles of the EU's integrated approach to external conflicts and crises, recognising the various phases of the conflict cycle. They will identify relevant EU policies and instruments across multiple sectors, including diplomacy, security and humanitarian aid. The course will emphasise the interconnectedness of local, regional and global issues in crisis prevention and management.

Additionally, participants will understand how to engage with EU Member States and institutions and civil society, and apply the integrated approach to CSDP missions and stabilisation efforts. They will draft strategic responses to crises, analyse options for effective mission planning, and enhance cooperative problem-solving through teamwork. Finally, participants will develop a clear understanding of the EU's institutional framework and demonstrate how to implement the integrated approach in practice.

Target audience

Participants should preferably be senior-level experts (civilian and military personnel, including civil administration and police) currently working or aspiring to work in areas related to crisis management in the wider context of CFSP/CSDP, including EEAS, CSDP missions and operations, EU delegations and the European Commission, or working for other organisations in a crisis area. Priority is given to personnel from EU Member States.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

EU Addressing and Facing Hybrid Threats and Challenges (Activity No 40)

Location	***Dates***
Paris, France	*17-19 December 2024*
Vienna, Austria	*June 2025*

Course aim

The course aims to equip civilian and military officials from EU institutions, relevant agencies, and Member States with the skills and knowledge necessary to engage effectively with security policies, strategies, and missions at a senior-staff level, particularly on hybrid threats. It promotes understanding of the diplomatic, institutional, legal and operational issues related to hybrid threats at the strategic level and facilitates exchange of national perspectives among Member States to enhance common situational awareness across the EU.

Learning outcomes

Participants will learn to identify the diverse nature of hybrid threats and define key concepts associated with them. They will evaluate the strategic risks these threats pose to EU Member States, missions and operations, as well as understand the roles of various EU institutions and agencies involved in addressing these challenges.

The course will cover the integrated approach to developing and implementing security strategies at the EU level, describing the instruments available to counter hybrid threats. Participants will recognise the importance of cooperation and coordination with partners and analyse civil and military options within the CSDP framework. Additionally, they will explore the EU's capability development and technological responses to hybrid threats while understanding the operational constraints related to democracy and the rule of law. Finally, participants will be encouraged to assess EU approaches critically and to propose solutions to related challenges.

Target audience

Participants will preferably be mid-ranking to senior-level officials from Member States and relevant EU institutions and agencies. The audience coming from Member States could include, but is not limited to, participants from various ministries (foreign affairs, defence, economy, interior, research, technology and finance) as well as agencies subordinated to such ministries and relevant members of the private sector. Participants are expected to have a basic knowledge of CSDP.

Course open to

- EU Member States - institutions

Monitoring, Mentoring and Advising in EU Crisis Management (Activity No 43)

Location: TBD
Dates: Spring-Summer 2025

Course aim

The course aims to equip future mission members with the skills essential to establish effective working relationships with local counterparts and contribute to achieving mission mandates. It also provides a unique opportunity for experts from military, police and civilian sectors to share their experiences, successes, challenges and strategies for overcoming obstacles as mentors and advisers.

Learning outcomes

Participants will learn to describe the EU structure and implementation of monitoring, mentoring and advising (MMA) mandates in civilian CSDP missions. They will explore key aspects of MMA, including various tasks and the roles of mentors and advisers, as well as identifying signs of resistance.

The course will cover assessing local capacity for effective knowledge transfer, planning and implementing programmes under an MMA mandate, and developing strategies for building working relationships with counterparts while managing resistance. Participants will also learn motivation techniques, principles for working in cross-cultural environments and adherence to the CivOpsCdr Guidelines for MMA.

Additionally, they will apply methods to build trust, analyse reasons for resistance, and develop negotiation and mediation skills with local and international partners, all while emphasising intercultural communication in multicultural settings.

Target audience

Participants should be senior-level civilian, police and military experts working or expected to serve in civilian or military CSDP missions and operations or in CSDP-related positions at HQ level. Participants should preferably have mentoring and advising components in their line of work (including but not limited to rule of law, justice reform, democratisation, corrections, police reform and Security Sector Reform) and cooperation with local counterparts. Priority is given to participants from EU Member States. However, non-EU citizens as well as NATO staff are welcome.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Disaster Relief in CSDP Context (Activity No 44)

Location: Lisbon, Portugal

Dates: 18-22 November 2024

Course aim

The course aims to unify perspectives and visions in disaster relief, as part of the overall disaster management chain, covering prevention, preparedness, humanitarian assistance, civilian protection and post-disaster reconstruction. It focuses on developing critical capabilities and situational awareness for managing emergency situations, emphasising strategic, operational and tactical planning in response to natural, human-made and climate-driven disasters within the CFSP/CSDP context. The training also addresses future challenges in disaster management, particularly civilian-military coordination, while fostering a network of future experts in the field.

Learning outcomes

Participants will learn to describe the role of disaster relief within the overall disaster management chain and review the EU's emergency management systems, particularly the Union Civil Protection Mechanism. They will understand the significance of humanitarian civil-military coordination in disaster relief and explain the organisation and functioning of EU humanitarian assistance and civil protection.

The course will cover the relevance of EU coordination with international actors such as UN OCHA and the International Red Cross, as well as the impact of various disasters on security. Participants will familiarise themselves with operational mechanisms, including the Emergency Response Coordination Centre (ERCC) and the CSDP coordination tools, and learn about the deployable military disaster relief capability package (DMDRCP).

They will identify the opportunities and challenges of utilising CSDP assets in humanitarian operations, design responses for complex interventions in disaster-affected areas, and implement the EU's integrated approach to disaster management. The course will also promote teamwork and problem-solving, develop a clear understanding of the EU's institutional setup and procedures in disaster relief, and encourage participants to engage with a shared community of disaster management experts.

Target audience

Experts with military, civilian/police, diplomatic or professional backgrounds who plan, execute and/or participate in a range of humanitarian and disaster management activities (disaster preparedness/prevention, humanitarian relief, rescue operations and post-disaster reconstruction and rehabilitation) in the context of CFSP/CSDP, or potential participants in CSDP missions or operations. Priority will be given to personnel from Member States who can be deployed to fact-finding missions in disaster-stricken areas as a team consisting of EEAS/EUMS, ECHO and other staff, and to personnel involved in humanitarian relief, civilian protection and humanitarian disaster assistance (from MS, EU partners and third countries).

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

From Conflict Analysis to Integrated Action: Generating Strategies for Intervention (Activity No 45)

Location: N/A

Dates: 3-7 March 2025

Course aim

The course aims to integrate various perspectives on complex conflict, equipping participants with critical skills to analyse conflict dynamics and assess realistic responses. It provides CFSP/CSDP personnel in crisis situations with conceptual frameworks and analytical tools for effective conflict prevention and crisis management. The course emphasises practical application and interactive learning to enhance the quality and impact of interventions.

Learning outcomes

The course equips participants with essential skills to analyse conflict dynamics and develop realistic responses within the CFSP/CSDP framework. Key outcomes include identifying the EU's conflict analysis elements, understanding the significance of preparedness and conflict sensitivity, and defining factors that drive modern conflicts. Participants will explore various conflict analysis frameworks, apply tools to real-world scenarios, and integrate gender and human rights considerations into their analyses.

Additionally, the course emphasises teamwork for inter-agency operations, assesses the complexities of third-party interventions, and demonstrates the critical role of conflict analysis in shaping effective CSDP missions. By the end, participants will be able to undertake thorough conflict analyses and design informed interventions that maximise positive impact while minimising harm.

Target audience

The course is designed for mid-ranking personnel engaged in CFSP/CSDP missions or prospective participants on future EU crises management initiatives.

Course open to

- EU Member States - institutions
- Eastern Partnership and Western Balkans countries

Contracting in International Operations Course (Activity No 47)

Location: Vienna, Austria

Dates: 23 June – 4 July 2025

Course aim

This two-week course aims to deepen participants' understanding of the comprehensive Civilian Security Operations (CSO) approach within the EU framework. It promotes enhanced information-sharing, collaboration and cooperation among military and civilian stakeholders. Additionally, the course provides a unique opportunity for participants to build a professional network of individuals engaged in CSO, facilitating ongoing dialogue and partnership in this vital area.

Learning outcomes

The course enhances participants' understanding of a comprehensive CSO approach within the EU framework, fostering collaboration among military and civilian actors. Key outcomes include identifying CSO frameworks and stakeholders and the roles of European institutions, as well as assessing trends and principles such as the European Peace Facility (EPF) and the role of networking in CSO.

Participants will develop intercultural awareness, analyse best practices, and distinguish between European and international legislation. Additionally, the course emphasises evaluating the core soft skills necessary for effective CSO implementation, ultimately creating a valuable network of professionals in the field.

Target audience

Participants will be senior experts (civil and military personnel) working in areas related to contractor support to operations (CSO). Priority is given to personnel from EU Member States deploying to CSDP missions and operations.

Course open to

- EU Member States - institutions

HEAT - Hostile Environment Awareness Training (Activity No 48a)

Location	***Dates***
Lisbon, Portugal	*14-18 October 2024*
Lubeck, Germany	*21-25 October 2024*
N/A	*4-8 November 2024*
Lubeck, Germany	*2-6 December 2024*
Lubeck, Germany	*27-31 January 2025*
Gotenica, Slovenia	*16-21 February 2025*
Lubeck, Germany	*7-11 April 2025*
Lisbon, Portugal	*5-9 May 2025*
Soave, Italy	*16-20 June 2025*
Lubeck, Germany	*11-15 August 2025*

Course aim

This course aims to enhance participants' security awareness and situational readiness while serving in missions. It focuses on fostering a safety-conscious mindset, boosting individual and team confidence, and providing practical guidance on how to deter, detect, and respond to potential threats. By equipping staff with essential skills and knowledge, the course seeks to improve overall personal safety and security in challenging environments.

Learning outcomes

Participants will learn to navigate various security scenarios, including: proper conduct while traveling in convoys; approaching checkpoints; and understanding hostage situations. The course covers recognising common arms, practising situational awareness, and managing risks in potentially dangerous environments such as protests or riots. Additionally, participants will develop skills in communication and navigation, and learn first-response techniques for medical emergencies. Emphasis will be placed on fostering a culture of personal and professional security, making informed decisions to mitigate risks, and integrating a gender perspective into threat assessment and risk analysis.

Target audience

Participants should (preferably) be persons deploying to CSDP high-risk missions. Priority is given to personnel selected for CSDP Missions and Operations.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Vehicle Safety and 4x4 Driving (Activity No 48b)

Location	***Dates***
Lubeck, Germany	*17-18 October 2024*
Lubeck, Germany	*28-29 November 2024*
Lubeck, Germany	*23-24 January 2025*
Lubeck, Germany	*3-4 April 2025*
Lubeck, Germany	*7-8 August 2025*

Course aim

This course aims to equip participants with the knowledge and practical skills necessary to operate 4x4 vehicles safely and effectively in remote and challenging driving conditions. It focuses on enhancing the operator's ability to navigate various terrains without technical support, thereby improving both crew safety and operational effectiveness.

Learning outcomes

Participants will gain an understanding of the technical aspects of 4x4 vehicles, including their construction and settings for different terrain conditions. The course covers safe driving behaviour in extreme environments and effective use of recovery equipment. Participants will learn to assess road and terrain conditions, identify safe driving paths, and manage risks associated with vehicle operations. Additionally, they will develop skills in terrain reading and coordinate with team members to enhance overall safety and performance.

Target audience

Participants should be persons deploying to CSDP missions with required self-driving in rough terrain. Priority is given to personnel selected for CSDP Missions and Operations.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Advanced Modular Training (AMT) for CSDP Strategic Crisis Management (Activity No 51) – Modular Course

Location: Brussels, Belgium - Thessaloniki, Greece - Rome, Italy

Dates: 24-28 March 2025, 26-30 May, 30 June – 4 July 2025

Course aim

The aim of this course is to provide civilian and military senior officers with the planning and management skills and knowledge required in order to perform their duties in the CSDP area. AMT builds on the principle that CSDP is a key element of the EU's external action, which reflects the collective toolbox available to the EEAS, EU Commission, and EU Member States.

Course participants will be exposed to relevant aspects of interaction among crisis management structures, by practising and discussing the procedures, key stages and planning tools of crisis management at the strategic level as part of the EU integrated approach to external conflicts and crises. The AMT methodology and structure is experiential and grounded in the diverse experience and expertise of course participants. The course uses a fictitious scenario and crisis management planning methodologies as a platform for developing skills and embedding knowledge, supported by both e-learning and residential classes.

This course requires significant prior knowledge and experience of CSDP. Participants are therefore expected to have substantial prior knowledge of CSDP. Participation in the CSDP Orientation Course and/ or relevant experience in the CSDP domain is highly recommended. AMT takes the form of two modules: EU integrated approach (AMT 1) and CSDP crisis management (AMT 2). The latter is offered with two options: CSDP crisis management at the political-strategic level (AMT 2a) and CSDP crisis management at the strategic level (AMT 2b). AMT 1 is mandatory and, depending on interest, participants must opt for either AMT 2a or AMT 2b. The time gaps between the prerequisite course and two AMT modules should be judiciously planned by the training providers to allow participants to take the recommended e-learning, reflect on major themes, engage in social learning and apply the acquired skills on the job.

Learning outcomes

In Module 1, participants will develop a comprehensive understanding of the integrated approach by examining the entire conflict cycle and the processes employed within the EEAS Crisis Response Mechanism, as well as other EU mechanisms such as those of the Council and Commission. They will learn to analyse conflict situations by identifying root causes and key actors, while formulating potential EU responses that align with existing global and regional strategies. This module also emphasises the theory of change in the context of EU external action and promotes principles that guide the integrated approach, particularly focusing on the security-development nexus and the importance of a conflict-sensitive approach to fragile environments, human rights, and gender issues.

Modules 2a and 2b focus on CSDP crisis management at both political-strategic and strategic levels. In Module 2a, participants will explore crisis response planning, including the roles and responsibilities of relevant bodies, while contributing to planning for potential crises and exit strategies. They will discuss the challenges involved in transferring authority from the political-strategic to the strategic level and work collaboratively as part of a planning team, guided by a senior strategic planner. This hands-on experience will prepare them to navigate the complexities of crisis management.

Module 2b continues this theme at the strategic level, reinforcing the importance of crisis response planning and the roles of various stakeholders. Participants will engage in strategic-level planning and further examine the challenges of authority transfer within CSDP operations. They will gain practical experience working in a planning team under the guidance of a senior planner, equipping them with the skills needed to effectively contribute to crisis management initiatives at both levels within the CSDP framework.

Target audience

The course is open to civilian and senior military (OF-3 and above) personnel earmarked to work or working in CSDP-related posts in Member States, the EEAS crisis management structures, CEUMC Office, CSDP Civilian and Military Missions and Operations, EU institutions and agencies working in the field of external action (e.g. DG ECHO, SATCEN, EDA), EU delegations, EU HQs and other relevant military and civilian institutions at national level.

Course open to

- EU Member States - institutions

Climate Change and Security (Activity No 52)

Location	***Dates***
Sofia, Bulgaria	*1-4 April 2025*
Athens, Greece	*18-20 June 2025*

Course aim

This course aims to build awareness of climate change as a security threat multiplier by providing foundational knowledge on its impacts across global, regional, and local levels. Participants will explore instruments and strategies to reduce climate risks and strengthen resilience, supporting civil and military decision-makers in identifying climate-related hazards and enhancing capabilities for mission planning, adaptation, and peacebuilding efforts. Addressing both present and future challenges, the course also includes an assessment of EU strategic documents and fosters a network of experts in climate diplomacy, disaster relief, and policy development for climate mitigation and adaptation.

Learning outcomes

The course equips participants with the knowledge to analyse key climate change trends, impacts, and security risks, emphasizing the implications for livelihoods, governance, and peace at various levels. It explores EU and international strategies, frameworks, and stakeholders central to climate change mitigation and adaptation, highlighting EU-specific structures for humanitarian and disaster response and resilience-building. Participants will also develop skills to assess the relationship between climate change and security, formulate evidence-based opinions, and propose solutions to improve climate resilience within peacekeeping and peacebuilding contexts.

Additionally, the course fosters a network of future civilian and military experts, empowering them to collaborate effectively on climate-security challenges. Participants will engage in cooperative problem-solving and gain insights that support EU policy development and implementation on climate adaptation, mitigation, and security.

Target Audience

Participants would be mid- to senior-level staff from MS and EU institutions, bodies and agencies. Priority will be given to:

- Personnel from MS who are or will be taking part in climate change mitigation and adaptation policy development and implementation at national level or with EEAS/EUMS, ECHO, CLIMA, NEAR or INTPA level (including EU delegations) or EDA;
- Personnel involved in conflict mediation and risk reduction, civil protection/ disaster relief, and humanitarian assistance;
- education and training experts, faculty advisers, professors, consultants, analysts, etc.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Strategic Communication for Peace, Security and Defence (Activity No 53)

Location: Bucharest, Romania

Dates: 24-26 September 2024

Course aim

This course aims to enhance understanding of the security implications of climate change by providing foundational knowledge about global warming as both a phenomenon and a security threat multiplier. Participants will explore the effects of climate change on international, regional and local peace and security. The course also introduces key instruments for mitigating the risks associated with climate change and equips civil and military decision-makers with the expertise to identify climate-related hazards and threats. By assessing future challenges and EU strategic documents, the training fosters a network of experts in climate change diplomacy, disaster relief and policy development.

Learning outcomes

Participants will learn to explain key trends in climate change, including its causes, risks and impacts, and understand its security implications, such as climate-fragility risks and threats to human security. They will identify effective measures to minimise and address these impacts and describe the relevant international agreements, frameworks and stakeholders involved in climate security. The course will highlight EU strategies and policies on climate change mitigation and adaptation, linking these directly to the CSDP and the European Union’s humanitarian and disaster response mechanisms.

Additionally, participants will develop the ability to analyse the nexus between climate change and security on the basis of the latest research, propose effective responses to enhance resilience in peacekeeping and peace-building efforts, and assess EU strategic documents related to climate change. They will also have opportunities to foster a network of experts in this field and contribute to the development and implementation of climate change policies within the EU framework.

Target audience

Participants should be mid-level professionals in MS and third-country institutions involved in the implementation of CSDP (ministries of foreign affairs, defence, internal affairs and justice). Strategic communications practitioners from the authorities of the MS and from related EU institutions and agencies could also be invited to join the course. Depending on the design of the course, senior decision-makers at the CSDP missions and operations level (StratCom/Political Advisers to the Head of Mission/Commander) could join the training, especially when experts with field experience are invited to contribute their expertise.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

EU Logistics Fundamentals/EU Logistics in Operations Courses (Activity No 54 a and b)

Location: Brussels, Belgium

Dates: 10-14 March, 17-21 March 2025

Course aim

These courses aim to equip participants with in-depth knowledge of EU logistics policies, principles, concepts and standard operating procedures applicable to civilian and military CSDP missions and operations. By focusing on both multinational and national logistics perspectives, the training enhances participants' skills in managing logistics requirements and overcoming challenges. Additionally, the courses emphasise the importance of crisis response planning, with a particular focus on logistics planning and execution at both political-strategic and military-strategic levels. Participants will learn to navigate dependencies and support functions essential for effective logistics management in CSDP operations.

Learning outcomes

The courses focus on enhancing participants' understanding of the EU's logistics frameworks and their application in civilian and military CSDP missions. Participants will discuss the EU Strategic Compass, integrated approaches to conflicts and civilian-military logistics capabilities, alongside the Concept Development Implementation Plan and relevant logistical concepts. The courses emphasise cooperation between civilian and military logistics, addressing challenges faced in crisis management planning and response, and evaluating lessons learned from CSDP logistics training.

Additionally, participants will explore EU synergies with international organisations such as NATO and the UN, focusing on interoperability and innovative logistics solutions. They will assess the structures, stakeholders and challenges of EU civilian-military logistics, evaluate the benefits of PESCO projects, and examine mutual support mechanisms for logistics in CSDP operations. The curriculum also covers the implications of hybrid threats, particularly in the cyber domain, and includes logistics planning and execution processes at both political-strategic and military-strategic levels. Ultimately, participants will be equipped to advise on logistics asset utilisation, foster interinstitutional cooperation, and contribute to logistics decision-making in crisis situations.

Target audience

Civilian and military personnel (OF-1 through OF-5 and OR-7 through OR-9)

Course open to

- EU Member States - institutions

Investigating & Preventing Sexual and Gender-Based Violence in Conflict Environments (Activity No 55)

Location: Boeblingen, Germany
Dates: 30 June – 11 July

Course aim

The course aims to strengthen mission personnel's ability to integrate a gender perspective into their work, focusing on preventing and addressing sexual and gender-based violence (SGBV). Participants will learn to apply this perspective in reporting and preventing SGBV and supporting investigations. Additionally, the course equips participants to design and deliver training sessions on SGBV prevention and investigation in conflict and crisis environments. It emphasises linking the justice chain, from police investigations to courtroom proceedings, while developing participants into trainers who can further educate others in these critical areas.

Learning outcomes

By the end of the course, participants will be able to explain the conceptual and legal framework of SGBV within mission contexts, define key concepts related to the Women, Peace, and Security (WPS) agenda, and understand the EU's integrated approach to gender equality in conflict environments. They will be able to assess training needs, design and conduct SGBV training, and navigate justice-related challenges, including cooperating with potential partners and experts. The course will also provide skills in gender analysis, crime scene management and adult learning principles, enabling participants to support SGBV prevention and investigation efforts while working in intercultural and fragile environments.

Target audience

CSDP personnel (civilian, military, police and diplomatic) committed to working on gender equality and towards accountability for SGBV crimes. Applicants for this course should have a special interest in implementing their training in fragile and (post-)conflict settings inside and outside the mission structure. The course is particularly useful for, but not limited to: personnel in an investigating or advisory role; personnel with a background in the police, military police, gendarmerie or judiciary; experts from other areas; and gender and human rights advisers.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Project Management in support of CSDP M/O – PM2 (Activity No 58)

Location	***Dates***
Thessaloniki, Greece	*5-9 May 2025*
Brussels, Belgium	*30 June – 4 July 2025*

Course aim

This course aims to address the project management needs identified in the annual CSDP lessons reports, especially following the creation of project cells within CSDP missions. The primary goal is to enhance the efficiency and effectiveness of these missions by providing a comprehensive methodological framework, PM², that can be adapted for managing a wide variety of projects. Participants will be equipped with the knowledge, skills and resources necessary to tailor and implement the PM² Methodology, improving their project management capabilities, reporting practices and communication with stakeholders across different authority levels.

Learning outcomes

By the end of the course, participants will have a thorough understanding of the PM² methodology, including its objectives, lifecycle, core elements and artifacts. They will learn to apply selected processes and procedures in project simulations, contributing to problem-solving, decision-making and collaboration in group settings. The course will enable participants to analyse the suitability of the PM² framework for specific projects in a CSDP context, develop strategies to implement the methodology in their own work environment, and make informed decisions during simulated scenarios. Additionally, participants will be able to assess the strengths and weaknesses of applying PM², fostering synergies across processes, and utilising team advantages to enhance project outcomes.

Target audience

The course is aimed at civilian, military and police personnel from EU Member States and from CSDP missions and operations, personnel serving in mission/operation supporting structures, either within the EU bodies or at Member State level, and personnel from Partnership Framework Agreement (PFA).

Course open to

- EU Member States - institutions
- Personnel seconded from third countries to CSDP missions

Senior Strategic Course (Activity No 64) – Modular course

Location: Brussels, Belgium -Berlin, Germany – Paris, France

Dates: 3-5 February 2025, 11-12 March 2025, 26-28 May 2025

Course aim

The CSDP Senior Strategic Course (SSC) aims to foster a professional environment that encourages exchange of ideas and transmission of senior-level knowledge. It promotes networking and critical analysis of strategic topics, rather than relying on traditional presentations. The course is designed to cultivate a common European security culture and strengthen the network of leaders involved in the strategic aspects of CFSP/CSDP. It facilitates both formal and informal high-level interactions, benefiting from participants' unique perspectives, but it does not aim to specifically prepare participants for senior positions.

Learning outcomes

By the end of the course, participants will have a deep understanding of the long-term objectives of CFSP/CSDP, the EU Global Strategy, and the roles of EU institutions in foreign and security policy. They will gain knowledge of military and civilian capability development, decision-making processes for CSDP missions and various aspects of crisis management, such as prevention, preparedness and response. The course also covers key horizontal issues, including human rights, cybersecurity and irregular migration, while exploring the interconnections between CSDP and areas like freedom, security and justice (FSJ). Participants will assess the strengths and weaknesses of current EU policies and capabilities, discuss future CFSP/CSDP developments, and evaluate the EU's operational engagement in relation to strategic objectives, ultimately integrating this knowledge into their professional activities.

Target audience

Participants should be top senior managers/members (equivalent to brigadier/general or equivalent ranks, political and security directors etc.) from defence, security, police, diplomacy and industry (up to five, with a maximum of one per MS) from all EU Member States and from the EU institutions: those who will make decisions on and implement strategy. In addition, selected academics will be invited (up to five, with a maximum of one per MS) and their work will contribute to the substance and the image of EU strategy.

Course open to

- EU Member States - institutions

Sectoral Qualifications Framework for the Military Officer Profession (SQF-MILOF) Familiarisation Course (Activity No 65)

Location	***Dates***
Madrid, Spain	*7-9 October 2024*
Rome, Italy	*January or February 2025*

Course aim

This course aims to familiarise personnel from EU Member States and institutions with the SQF-MILOF package by exploring the implementation roadmaps at the national level. It equips participants with the foundational skills needed to align national military qualifications (NMQs) with the SQF-MILOF framework and the Core Curriculum for Military Officers (MILOF-CORE), fostering understanding and integration across Member States.

Learning outcomes

By the end of the course, participants will be able to discuss the background, objectives and relevance of the SQF-MILOF framework, understanding its role in shaping future military officer competencies. They will compare the European, national and military qualifications frameworks, analyse the connections between SQF-MILOF and MILOF-CORE, and address the challenges of leveling NMQs to SQF-MILOF standards. The course also emphasises the importance of validating informal and non-formal learning for lifelong development, teaching participants how to write learning outcomes and level military qualifications. Additionally, participants will develop the skills to actively contribute to the discussion, promotion and implementation of SQF-MILOF at national level.

Target audience

Personnel working at national level dealing with military qualifications and curriculum developers from training and education providers.

Course open to

- EU Member States - institutions

Intelligence Security Challenges and Opportunities in the EU (Activity No 66)

Location: Brussels, Belgium

Dates: 19-21 November 2024

Course aim

This course is designed to prepare military officers and civil servants from EU institutions, agencies and Member States to take on mid- to senior-level roles in intelligence policies, strategies, missions and operations, with a focus on capabilities development. It aims to deepen participants' knowledge of diplomatic, institutional, legal and operational intelligence issues at the strategic level. The course also addresses future challenges and strategic EU documents in this field, and fosters a network of future civilian and military intelligence experts.

Learning outcomes

By the end of the course, participants will be able to describe the key EU strategies, policies and stakeholders involved in intelligence cooperation, as well as major international intelligence organisations. They will be equipped to address future challenges in the intelligence field, assess strategic documents and summarise integrated technological threats at both operational and strategic levels. Additionally, participants will gain insight into the network of civilian and military intelligence experts within EU institutions and Member States, understand intelligence coordination within the EU and with other nations, and incorporate data protection practices into their daily work.

Target audience

The course is open to civil servants and military personnel from EU Member States and EU institutions, more specifically dealing with operational and strategic aspects of intelligence issues, from defence or security perspectives, and willing to update and deepen their knowledge. Academics and members of the business community from the EU Member States can also be nominated to participate in this course.

Course open to

- EU Member States - institutions

Diplomatic Skills for CSDP (Activity No 67)

Location: Timisoara, Romania

Dates: 17-19 December 2024

Course aim

The basic course on diplomacy for CSDP missions aims to introduce participants to fundamental principles of diplomacy and their relevance to the CSDP/CFSP framework. It provides a critical assessment of the evolving connections between traditional and modern diplomacy, globalisation trends and public diplomacy in the context of CSDP missions. The course also introduces participants to emerging concepts such as digital diplomacy. Ultimately, it supports EU Member States, institutions and agencies in training personnel to operate in CSDP-related fields at both operational and strategic levels.

Learning outcomes

Participants completing the course will acquire a thorough understanding of core diplomatic principles, EU strategic objectives and the EU's role in international strategic competition. They will summarise global players' grand strategies, the objectives of the EU Global Strategy and PESCO diplomacy, while understanding the role of intelligence in diplomacy and partnerships with third countries. Additionally, participants will analyse the EU's role in the international community and its interactions with other international organisations (IOs). The course will also cover lessons learned in CSDP missions, civilian-military coordination, and the integrated approach to CSDP operations. Finally, participants will develop the ability to argue the need for CSDP missions and adapt modern communication trends to diplomatic needs.

Target audience

Participants would normally be entry- or mid-level staff from MS and EU institutions and agencies, with some previous experience in security policy matters. Ideally, the participants should have some experience related to diplomacy or (preferred scenario) have previously attended the CSDP Orientation Course.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Cultural Property Protection Course (Activity No 68)

Location	***Dates***
Krems, Austria	*23-27 September 2024*
Rome, Italy	*17-21 March 2025*

Course aim

This course is designed to provide members of EU institutions, relevant bodies, Member States and EU candidate countries involved in crisis and conflict prevention, management and post-crisis recovery with the knowledge needed to protect cultural property. It fosters collaboration among governments, civil society, international organisations and NGOs to achieve an integrated approach to cultural property protection. Additionally, the course addresses key challenges in cultural property protection, provides tools to overcome them, and promotes cooperation with international actors like the UN and OSCE. A secondary goal is to create a network of professionals in this field.

Learning outcomes

Participants will gain a comprehensive understanding of the legal framework for cultural property protection, including relevant laws and regulations for various situations. They will learn about EU approaches and those of other international organisations such as UNESCO and NATO, comparing national and international concepts for protecting cultural property. The course also covers best practices and lessons learned in cultural property protection and their relevance to CSDP missions, as well as the roles of civil-military interaction in this field. Participants will be able to identify threats to cultural property, collaborate with stakeholders, and apply a holistic approach to protection efforts during crisis and conflict scenarios. Moreover, they will develop the ability to analyse and contribute to cultural property protection within their areas of responsibility, ensuring that cooperation with other actors takes place in a comprehensive protection strategy.

Target audience

The participants will predominantly come from EU institutions, its Member States, EU candidate countries and EU partners. Limited numbers of slots will be assigned to participants from UN and OSCE structures and topic-related training institutions.

Participants should be working in conflict prevention, conflict management and post-conflict recovery and stabilisation contexts related to the protection of cultural heritage at an operational level. Regarding the integrated and holistic approach to the protection of cultural property, participants may be civilian, military or police staff.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Advanced Diplomacy for Peace Security and Defence (Activity No 69)

Location: Brussels, Belgium

Dates: 11-13 November 2024

Course aim

The Advanced Diplomacy Course for Security and Defence aims to deepen participants' knowledge of diplomacy, particularly focusing on the role, significance and necessity of diplomatic skills in the context of CSDP missions. The course emphasises advanced diplomatic techniques, such as negotiation strategies and the traits of a contemporary diplomat, with a specific focus on diplomacy in CSDP environments. Ultimately, the course supports EU Member States and institutions by equipping personnel to work effectively in CSDP-related diplomatic and strategic roles.

Learning outcomes

Participants will enhance their understanding of key diplomatic concepts and principles, particularly in the context of international strategic competition and EU diplomacy. They will assess EU strategic documents from a diplomatic perspective and critically discuss the grand strategies of global and regional players. The course covers topics such as the orientation of EU diplomacy, defence diplomacy, the role of intelligence and cooperation with third countries, emphasising contemporary diplomatic challenges. Participants will also explore both traditional and modern diplomatic trends, learning from lessons and best practices in strategic communication, mediation and negotiation. Additionally, they will analyse the importance of advanced diplomatic knowledge in the CSDP context, apply integrated approaches to CSDP missions, and adapt their skills to sensitive and complex environments.

Target audience

Participants would normally be mid- and high-level staff from MS and EU institutions and agencies, with consistent previous experience in diplomacy, security and defence matters.

Course open to

- EU Member States - institutions

European Security and Geo-Economics (Activity No 71)

Location: Vienna, Austria

Dates: 30 September – 3 October 2024

Course aim

The course aims to provide participants with a comprehensive understanding of geo-economics as an integral part of foreign, security and defence policies. It examines the use of economic instruments in pursuing strategic interests, particularly in the context of great-power competition. The course also explores how the European Union can practise geo-economics while remaining committed to its core values, equipping participants with the knowledge and skills to address economic dimensions in CSDP missions.

Learning outcomes

Participants will gain in-depth knowledge of the EU Global Strategy, its organisational structure, and decision-making processes, particularly regarding geo-economics. They will learn about the EU's integrated approach to partnerships and cooperation with external partners and explore the role of geo-economics in implementing EU strategic objectives. Participants will understand how the EU formulates communication-related policies and identify key actors in the geo-economic landscape within CSDP environments. Additionally, they will evaluate lessons and best practices in geo-economics, assess stakeholders' influence on EU strategies, and analyse conflicts of interest relevant to CSDP. By the end of the course, participants will be equipped to manage the EU's geo-economic interests, compare lessons learned, and effectively communicate strategic objectives aligned with EEAS guidelines.

Target audience

The course is open to both civilian and military (mid-level) personnel, from EU Member States, relevant EU institutions and agencies, and CSDP missions and operations, who either are or will be involved in work on CSDP matters. Candidates should have a special interest in financial and economic issues. The course is particularly intended for personnel working at the interface of security, defence and external relations (including trade, investment and enlargement).

Course open to

- EU Member States - institutions

Integrated Border Management (IBM) in CSDP (Activity No 72)

Location: Kilkis, Greece

Dates: 21-25 October 2024

Course aim

The IBM course is designed to equip military and law enforcement officers, as well as civil servants from EU institutions, relevant agencies, and Member States, with a thorough understanding of the IBM concept and its implementation within both CSDP missions and national frameworks. Through case studies, participants will gain insights into integration levels across different countries and within the EU. The course will also cover the planning process, potential risks, benefits and challenges of integration, providing valuable guidance for managing and improving border management practices.

Learning outcomes

Participants will learn about the legal foundation of border management in the EU and the importance of IBM within the CSDP framework. They will examine lessons learned from EU Member States, identify potential risks, and understand the impact of the security environment on IBM. Participants will gain practical knowledge of border agency structures, roles and responsibilities, along with the use of technology in IBM operations. They will apply risk analysis methods, integrate best practices, and explore strategies for effective IBM planning in CSDP missions. The course will also cover gender perspectives, building integrity and the contribution of military forces to IBM, providing participants with the skills to manage border agencies and apply the knowledge to real-world scenarios.

Target audience

Participants would normally be mid- to high-level personnel (civilian, police and military) from Member States and EU institutions and agencies who are assigned to or are interested in participating in CSDP missions and operations.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Foreign Information Manipulation and Interference (Activity No 76)

Location: Brussels, Belgium

Dates: 18-22 November 2024

Course aim

The Foreign Information Manipulation and Interference (FIMI) course is designed to create an enhanced learning environment that fosters a deep understanding of the manipulation of information and its associated cybersecurity components. The course integrates best practices from the counter-FIMI and cybersecurity fields to uncover the tactics involved in the creation and dissemination of disinformation. By focusing on the emerging link between information manipulation and cyber-attacks, the course aims to expand the knowledge and understanding of experts and practitioners regarding the tools, methods and strategies employed by hostile entities to conduct manipulative activities that threaten values, procedures and political processes at EU level. Additionally, participants will engage with existing methodological frameworks, such as the open-source DISARM, to identify and counter FIMI/disinformation, as well as exploring practical case studies on combating these threats. The course will also set the stage for a better understanding of the impact of current FIMI actions and future developments. The curriculum includes lectures, discussions, problem-solving exercises and mentorship opportunities.

Learning outcomes

Participants will gain insight into the primary challenges to EU security arising from the evolving landscape of FIMI/disinformation and tactics. They will learn to identify elements of the EU's integrated approach to situational awareness, resilience and cooperative responses against FIMI/disinformation. The course will equip participants to map methods that combine information manipulation with cyber-attacks and facilitate shared assessments of these tactics. They will become familiar with the principles of an EU FIMI/disinformation toolbox, which emphasises preventive, cooperative, stability-building, restrictive and supportive measures.

The course will enable participants to identify lessons learned and effective practices in various response options, ranging from diplomatic engagement to crisis mitigation. They will develop mechanisms for resilience that span prevention and recovery phases. Participants will also learn how to mitigate identified risks and vulnerabilities by leveraging existing resources. Through practical exercises and scenario development, they will apply critical thinking, assessment and collaboration skills.

Additionally, participants will gain the ability to use tools and techniques to evaluate manipulative action patterns that may adversely affect EU values, procedures, and political processes. They will learn to use cyber-diplomacy tools and interference mitigation mechanisms effectively. Finally, the course will empower participants to translate their knowledge into practical solutions that can be shared, negotiated and advanced in multi-stakeholder environments.

Target audience

Participants should be mid-level professionals in MS institutions involved in implementing the prevention and countering of disinformation and cybersecurity threats (ministries of foreign affairs, defence, intelligence and internal affairs). Practitioners with expert knowledge in the authorities of the MS and from related EU institutions and agencies could also be invited to join the course. Depending on the design of the course, senior decision-makers could join the course, especially when experts with field experience are invited to contribute their expertise.

Course open to

- EU Member States - institutions

Modern Leadership in the Context of Law of Armed Conflicts and Open-Source Intelligence (Activity No 78)

Location: Thessaloniki, Greece

Dates: 14-18 October 2024

Course aim

The course is designed to equip military and law enforcement officers (OF2-OF4) and civil servants from EU institutions, relevant agencies, and Member States with targeted training to enhance their effectiveness in military command and administration within the Learn, Plan, Apply & Lead framework. Participants will gain an understanding of the key elements of international law (IL) pertaining to armed conflicts, explore the legal framework governing CSDP missions, and analyse the impact of open-source intelligence (OSINT) on decision-making. Additionally, the course will provide opportunities for networking and professional relationship development among participants.

Learning outcomes

Participants will acquire a comprehensive understanding of the legal framework governing CSDP missions and operations concerning international law of armed conflicts, along with foundational knowledge of relevant EU structures and mechanisms. The course will empower them to implement policies and strategies in line with national and international legal standards, while emphasising the role of OSINT in decision-making and operational planning.

Additionally, participants will develop skills for effective communication and collaboration with stakeholders, promoting information-sharing and a common operational picture. They will be trained to navigate civil-military coordination challenges, evaluate the impact of EU actions on capacity-building operations, and foster cooperation within the EU and with external partners. Ultimately, this course aims to prepare participants for roles as mid-level officials in peacekeeping and capacity-building efforts within the CSDP framework.

Target audience

The course is designed for up to 40 participants. EU Member States and European institutions are invited to nominate one participant each at mid- to senior-level rank. The training audience could include, but is not limited to, participants (military and civilian personnel) from various ministries (foreign affairs, defence and interior) as well as national and EU institutions and agencies.

Course open to

- EU Member States - institutions

Team and Conflict Management in Peace Operations (Activity No 81)

Location: N/A
Dates: 2-6 December 2024

Course aim

The Team and Conflict Management course is designed to enhance the effectiveness and performance of teams and their leaders in CMO. It emphasises the importance of cooperation, mutual support and strong interpersonal relationships among team members and supervisors as essential components for fostering resilience and a productive working environment. The course aims to equip participants with vital competencies, such as intercultural communication, conflict management and leadership skills, enabling them to implement the mission's mandate successfully. Participants will have opportunities to test, reflect on and further develop their abilities in leadership, teamwork and conflict resolution.

Learning outcomes

Participants will gain a comprehensive understanding of cultural dynamics and their impact on mission environments, as well as the nature and emotional underpinnings of interpersonal conflicts. They will learn about effective motivation strategies and the characteristics of high-performing teams, while also exploring various leadership styles and their applications within a comprehensive approach. Practical skills will include applying cross-cultural communication techniques, conflict analysis and management tools, and methods for team-building and trust development. Additionally, participants will develop self-reflection practices regarding their leadership and conflict behaviours, ensuring that interactions within diverse communities are respectful and implementing duty of care in multicultural settings. Overall, the course aims to prepare participants to lead and collaborate effectively in complex, diverse environments while managing stress and addressing the needs of team members.

Target audience

The course is geared towards civilian, police and military experts who have worked or will be working in leadership positions in crisis management missions/ operations, as well as HQ staff working in the area of CSDP.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Challenges of European Cybersecurity (Activity No 200)

Location: Budapest, Hungary

Dates: 28-30 April 2025

Course aim

The course is designed to provide participants with a comprehensive understanding of the information society and its complexities, including the various threats posed by cybersecurity issues. It covers essential concepts and principles related to cybersecurity and cyber defence, as well as international cyberspace issues and cyber diplomacy. By offering insights into the technological tools used in this field, the course also aims to foster networking opportunities among professionals working in cybersecurity and cyber defence.

Learning outcomes

Participants will develop an awareness of the extensive and complex nature of the information society, gaining insight into the various cyber threats it faces. They will learn to define key concepts related to cybersecurity and cyber defence, identify the roles of EU institutions and agencies involved in this area, and recognise the challenges at the European level. The course will encourage reflection on emerging trends in cyber threats and the implications for international cyber diplomacy. Participants will also explore both technical and organisational tools for enhancing cybersecurity and consider the potential impacts of cyber threats on public policies and industrial planning. Ultimately, they will assess the challenges of cybersecurity within the European context and evaluate future directions for addressing these issues effectively.

Target audience

Participants should be mid-ranking to senior officials dealing with strategic matters in the field of cybersecurity and cyber defence from EU MS, relevant EU institutions and agencies. They should either be working in key positions or have clear potential to achieve leadership positions, in particular in the fields of cybersecurity or cyber defence.

Course participants must be available for the entire course and should be ready to bring their specific expertise and experience to bear throughout the course.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Computer Security Incident Response Team (CSIRT) Fundamentals (Activity No 204)

Location: Nicosia, Cyprus

Dates: 18-21 February 2025

Course aim

This course focuses on the essential capabilities required for the development, implementation and provision of effective CSIRTs. It combines theoretical knowledge with innovative interactive e-learning methods to deliver foundational knowledge in cybersecurity incident response and a thorough introduction to risk management. Additionally, the course provides a platform for cybersecurity professionals to exchange views and share best practices, enhancing their knowledge, skills, and competencies. By the conclusion of the course, participants will be equipped to assess the potential impacts of cyber incidents on policies and systems and determine appropriate cyber countermeasures. They will also gain specific skills to investigate, analyse and respond to cyber incidents within network environments.

Learning outcomes

Participants will learn to identify key EU institutions and agencies involved in cybersecurity and cyber defence and understand the challenges facing cybersecurity at the European level. They will recognise the scale of the information society and the various cyber threats currently encountered. The course covers incident-handling standards and methodologies, as well as hybrid threats related to cybersecurity. Participants will analyse information related to cyber threat intelligence, assess security incidents, and classify the necessary technical and organisational tools for cybersecurity. Additionally, they will evaluate the potential impacts of cyber threats and incidents on public policies and systems. Ultimately, they will be equipped to apply detection and prevention techniques and develop strategies for effective incident response, including malware analysis and risk management.

Target audience

Participants should be mid-ranking to senior officials dealing with technical and tactical matters in cybersecurity and cyber defence, from EU MS, relevant EU institutions and agencies. They should have backgrounds clearly related to technical and tactical aspects of cybersecurity (Information Technology (IT) or Information Security (IS) professionals).

Course open to

- EU Member States - institutions

Cybersecurity Risk Management (Activity No 205)

Location: Budapest, Hungary
Dates: 14-17 October 2024

Course aim

The Risk Management course aims to develop participants' skills in identifying, analysing, assessing, estimating and mitigating cybersecurity-related risks associated with ICT infrastructures, systems and services. Through effective planning, application, reporting and communication of risk analysis, assessment and treatment, participants will be equipped to manage cybersecurity risks proficiently.

Learning outcomes

Participants will learn to recognise best practices and standards in information security management and understand the roles of key personnel in an effective information security management system. They will gain knowledge of methodologies for conducting risk analysis, as well as defining risk evaluation and treatment options. The course will cover identifying technical controls to reduce risks and documenting information security management policies in alignment with organisational strategies. Additionally, participants will analyse critical assets, identify potential threats and vulnerabilities, and establish comprehensive risk management plans. They will also design and document processes for risk analysis and management, apply appropriate mitigation and contingency actions, and ensure that information security policies are implemented, while managing security risks in relation to organisational information and processes.

Target audience

Participants should be technical experts (civilians or military personnel) who have to take roles in information security management, in particular those with technical responsibilities in IT and networking who need or plan to take information security management roles and responsibilities.

Course open to

- EU Member States - institutions
- EU candidate countries

The role of the EU Cyber Ecosystem in Global Cybersecurity Stability (Activity No 206)

Location: Brussels
Dates: 2nd semester 2024-25

Course aim

This course explores the foundational elements of the EU cyber ecosystem and their role in enhancing global security stability through improved cyber-resilience, trust-building and cooperation among global actors. Aimed at mid-ranking to senior officials, the course provides a platform for exchanging views and sharing best practices on cyber-related topics, thereby enhancing participants' knowledge, skills and competencies. By the end of the course, participants will be better equipped to operate interoperably within the global cyber ecosystem and to cultivate shared perspectives.

Learning outcomes

Participants will gain a comprehensive understanding of EU policies related to cybersecurity and the various entities involved in the EU cyber ecosystem, along with their specific roles. They will define key cybersecurity concepts, recognise different types of cyber threats, and identify challenges at both global and international levels, including those related to cyberspace. The course will also cover hybrid threats and their complexities, the impact of cyber threats on global stability, and potential cooperation opportunities between the EU cyber ecosystem and the global cyber environment. Participants will learn to evaluate the impacts of cyber threats and create synergies between the EU and global cyber frameworks, ultimately selecting appropriate confidence-building measures to foster collaboration in cyberspace.

Target audience

Participants should be mid-ranking to senior officials dealing with aspects in the field of cyber security.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Cyber Diplomacy Fundamentals (Activity No 207a)

Location: Bucharest, Romania

Dates: March – December 2025

Course aim

This course provides participants with a comprehensive understanding of the evolving landscape of cyber external relations, equipping them with the knowledge to identify and implement capacity-building measures that enhance resilience and stability. Participants will explore the necessity of interoperability within the global cyber ecosystem, gain insight into fundamental concepts and current challenges, and learn strategies to strengthen cyber resilience. A key focus will be on understanding and applying the EU's Cyber Diplomacy Toolbox to address emerging threats effectively. Additionally, the course fosters collaboration among junior to mid-ranking officials, enabling them to network, exchange views, and share best practices, ultimately enhancing their knowledge, skills, and competencies in cyber-related matters.

Learning outcomes

Upon completing this course, participants will gain a comprehensive understanding of digital diplomacy and cybersecurity in the context of the EU's foreign policy. They will be able to identify and list the strategies, policies, rules, and norms that shape EU cyber diplomacy, as well as understand the roles of various entities in the EU cyber ecosystem. Participants will be familiar with the nature of cyber and hybrid threats and their significant impact on external relations. They will recognise the key challenges facing global cybersecurity and cyber diplomacy, including issues related to cyberspace governance. Participants will grasp foundational concepts in cybersecurity, cyber defense, cybercrime, and the protection of critical infrastructures. Additionally, they will be equipped to analyse the complexity and impact of cyber issues in the external relations domain, distinguishing how these issues affect global stability and cyber resilience. Learners will also be able to evaluate the potential impacts of cyber threats on the global environment and explore synergies with the EU's cyber ecosystem.

Target audience

The participants should be junior- to mid-level diplomats or representatives of Member State governmental or EU institutions, and any competent state agencies with a role in strategy formulation and implementation in the cyber realm.

Course open to

- EU Member States - institutions
- EU candidate countries

Cyber Diplomacy Advanced (Activity No 207b)

Location: Brussels

Dates: 21-23 January 2025

Course aim

This course is designed to provide participants with an understanding of the geopolitical dynamics of cyberspace, the current threat landscape and the various pillars of cyber diplomacy. This knowledge will enable participants to implement effective cyber policies, engage in regional and multilateral forums, and participate in capacity-building efforts. Throughout this advanced course, participants will gain insights into global cyber governance, challenges, the EU's tools for preventing, deterring and responding to cyber threats, as well as confidence-building measures. The course will also facilitate networking opportunities for mid- to senior-ranking officials, allowing them to share best practices and enhance their knowledge, skills and competencies in cyber diplomacy.

Learning outcomes

Participants will be able to outline key concepts and actors involved in cyber diplomacy and understand the international rules-based order in cyberspace, including the application of international law and norms of responsible state behaviour. They will identify emerging trends and geopolitical challenges, describe the rationale behind confidence-building measures (CBMs) and capacity-building efforts, and recognise the importance of a full-spectrum approach to resilience and cooperation in cyberspace. The course will equip participants to design effective cyber diplomacy strategies, address challenges in external relations, assess the potential impacts of cyber threats, and integrate appropriate norms when implementing CBMs. Additionally, participants will learn to develop and evaluate capacity-building measures, justify various actions according to the Cyber Diplomacy Toolbox, and contribute to the design and implementation of comprehensive cyber strategies.

Target audience

The participants should be mid- to senior-level diplomats or representatives of Member State governmental or EU institutions, and any relevant state agencies involved in the development and implementation of cyber policies or strategies.

Course open to

- EU Member States - institutions

Critical Entities Resilience (Activity No 208a)

Location: Bucharest, Romania

Dates: March-June 2025

Course aim

This course provides an overview of the evolving efforts in Critical Entities Resilience (CER), highlighting interdependencies, emerging risks, and systemic transformations from national to global levels. It equips participants with strategic foresight, explores the integration of advanced technologies like AI and Blockchain, and introduces the latest tools for CER practitioners and policymakers to assess and mitigate risks effectively.

Learning outcomes

This course will provide participants with a comprehensive understanding of the Critical Entities Resilience (CER) framework at the European level, emphasising the interdependencies between critical infrastructures and emerging areas of focus. It explores the factors, attributes, and elements of resilience within complex systems while addressing the evolving security environment, including safety, cyber threats, and systemic vulnerabilities. Participants will analyse emerging risks and governance perspectives, assessing the impact of new technologies on critical infrastructure and the tools available to CER practitioners and policymakers. The course also develops analytical skills to evaluate the systemic effects of technological adoption, regulatory transformations, and public policy shifts. Additionally, it fosters strategic thinking by assessing challenges at both national and European levels and proposing measures to enhance public-private cooperation in strengthening resilience efforts. They will also share knowledge on resilience factors for critical entities and exchange best practices concerning the implementation of CER directives into national legislation.

Target audience

Participants should be mid- to high-level representatives of public authorities, critical entities or critical infrastructure owners/operators (private and state) (critical entities) with responsibilities for developing and implementing security strategies, policies and mechanisms for Critical Entities Resilience. EU Member States, governmental and private companies involved in CER or CI operation are invited to participate.

Course open to

- EU Member States – institutions, bodies and agencies

Critical Entities Resilience Advanced (Activity No 208b)

Location: Lisbon

Dates: 23-27 June 2025

Course aim

This course aims to enhance participants' understanding of Critical Entity Resilience (CER) by exploring the interdependencies and dynamics of critical entities in a complex security environment. Through engaging tabletop exercises, participants will improve strategic foresight in resilience planning and develop a multidisciplinary perspective on governance frameworks for managing security issues in a cross-border context.

Learning outcomes

By the end of the course, participants will be able to describe the interdependencies of critical infrastructures in relation to national, European and global contexts, as well as the regulations governing CER at the European level. They will identify challenges posed by complex security environments and recognise emerging trends that create new risks and vulnerabilities. Participants will explain perspectives on Complex Systems Governance and outline available tools and regulations for CER practitioners and policy-makers. They will classify challenges related to technical, organisational and transborder coordination, analyse the systemic impacts of European and global integration on CER efforts, and categorise the effects of new technologies and challenges such as climate change on public policy regarding CER. In addition, participants will develop a systemic understanding of the security environment grounded in the CER framework, systematise complex systems from this perspective, and design models to address security issues effectively. They will also share knowledge on resilience factors for critical entities and exchange best practices concerning the implementation of CER directives into national legislation.

Target audience

Participants should be mid- to high-level representatives of public authorities, critical entities or critical infrastructure owners/operators (private and state) (critical entities) with responsibilities for developing and implementing security strategies, policies and mechanisms for Critical Entities Resilience. EU Member States, governmental and private companies involved in CER or CI operation are invited to participate.

Course open to

- EU Member States - institutions

The EU’s Cybersecurity Strategy for the Digital Decade (Activity No 209)

Location: Rome, Italy

Dates: 14-16 May 2025

Course aim

This course offers a comprehensive overview of the EU’s Cybersecurity Strategy for the Digital Decade, focusing on its main pillars. It serves as a collaborative forum for participants from Member States and EU institutions to engage with one another, sharing insights on current and future developments at strategic, tactical and operational levels. By facilitating the exchange of views and best practices, the course aims to enhance participants’ knowledge and skills, enabling them to align more effectively with the Strategy’s objectives. Ultimately, attendees will improve their interoperability within the EU cyber ecosystem.

Learning outcomes

By the end of the course, participants will be able to identify the three main instruments of EU action—regulatory, investment, and policy—and recognise the roles of various entities involved in achieving the Cybersecurity Strategy’s objectives. They will define key concepts, analyse the impacts of each of the strategy’s three pillars—resilience, operational capacity, and global cyberspace—and integrate these objectives into related plans. In addition, participants will evaluate potential cyber threats affecting the strategy’s implementation and transform anticipated outcomes into opportunities for synergy within the EU cyber ecosystem, while also selecting appropriate trust-building measures to enhance cooperation.

Target audience

Participants should be officials from MS or EU institutions and agencies who deal with aspects of cybersecurity.

Course participants must be available throughout the course and should be ready to participate in line with their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

Cyber Range - Pentester Tools (Activity No 213)

Location: Warsaw
Dates: 24-26 September 2024

Course aim

This course aims to enhance participants' knowledge and practical skills in identifying potential vulnerabilities and understanding the role of penetration testing in improving cybersecurity. It covers fundamental aspects of the subject such as network reconnaissance, host enumeration, and vulnerability identification, equipping students with knowledge of various applicable tools and techniques. Participants will engage in practical exercises, conducting penetration tests through scenarios on the Cyber Range platform—a sophisticated virtual environment for modeling and simulating cyber scenarios. Ultimately, the course contributes to developing the skills of digital professionals, fostering cyber-resilience, and promoting strategic autonomy within the framework of the CSDP.

Learning outcomes

By the end of the course, participants will be able to describe penetration testing concepts, identify various cyber threats, and list the tools and techniques relevant for different penetration tests. They will learn to recognise potential threats and weaknesses in IT infrastructure, understand the benefits of conducting penetration tests, and perform essential activities such as network reconnaissance, traffic interception and web reconnaissance. Additionally, students will be equipped to conduct penetration tests, reconstruct and evaluate cyber-attacks, assess the impact of identified vulnerabilities, and recommend appropriate countermeasures to mitigate risks to organisations.

Target audience

The course is intended for technical personnel (mid-ranking officials, engineers and technicians) employed in the field of cybersecurity, from MS or EU institutions, bodies and agencies. Attendees should need to learn about cybersecurity threats from a technical perspective. Due to the technical nature of this course, it is recommended that attendees be familiar with the Linux operating system, including use of terminal tools and basic network configuration aspects.

Course open to

- EU Member States - institutions

Cyber Range - Cybersecurity in Practice (Activity No 215)

Location: Warsaw

Dates: 11-13 March 2025

Course aim

This course aims to enhance participants' knowledge and practical skills in securing the IT infrastructures they oversee. Through hands-on execution of prepared scenarios involving virtual machines and networks, students will explore key areas such as reconnaissance, exploitation, Wi-Fi hacking and web pentesting, allowing them to identify vulnerabilities and weaknesses that could grant unauthorised access to target resources. Participants will learn about various cybersecurity tools and their applications in different contexts. Delivered on the Cyber Range, the course provides a unique training environment for simulating complex scenarios, including cyber-attacks, ultimately helping to improve the security of IT infrastructures. This course contributes to the development of digital professionals and fosters cyber-resilience and strategic autonomy in line with the CSDP.

Learning outcomes

By the end of the course, participants will be able to describe penetration testing concepts and procedures, including both offensive and defensive security strategies. They will be able to list applicable tools and techniques for various penetration tests, understand wireless networking standards, and gain knowledge about vulnerabilities such as XSS, CSRF and SQL Injection. Students will perform network reconnaissance, intercept and analyse network traffic, and choose appropriate pentesting tools for Wi-Fi hacking. Additionally, they will conduct web reconnaissance and evaluate coding for security weaknesses, test local networks using appropriate penetration techniques, and assess the potential impacts of identified vulnerabilities on organisations. Overall, participants will be equipped to select and prepare systems and tools for effective penetration testing.

Target audience

The course is intended for technical personnel (mid-ranking officials, engineers and technicians) employed in the field of cybersecurity, from Member States or EU institutions, bodies and agencies. Attendees should need to learn about cybersecurity threats from a technical perspective. Due to the technical nature of this course it is recommended that attendees be familiar with the Linux operating system, including use of terminal tools and basic aspects of network configuration.

Course open to

- EU Member States - institutions

Course on Cybersecurity and International Laws (Activity No 216)

Location: Brussels

Dates: 10-12 February 2025

Course aim

This course explores the application of international law in cyberspace, addressing current geopolitical challenges and offering practical solutions. It covers key legal instruments related to state responsibility, cybersecurity due diligence, trans-boundary data flows (including GDPR) and the human rights implications of AI. Participants will exchange views and best practices, enhancing their knowledge and skills and enabling them to tackle contemporary international law issues in the cyber domain effectively.

Learning outcomes

By the end of this course, participants will understand the norms and sources of international law as they apply to cyberspace and be able to identify state obligations in multi-stakeholder internet governance. They will be able to define key concepts related to cybersecurity in international law, such as attribution, state responsibility and proportionate countermeasures. Participants will also identify various cyber threats and global challenges and articulate normative measures for addressing them. They will gain insights into the implications of AI and hybrid threats for human rights in cyberspace and evaluate the impacts of cyber threats on international law and the peaceful resolution of disputes. Additionally, they will be able to classify cyber incidents and threats within the frameworks of due diligence and GDPR, evaluate their potential impacts, and foster synergies within the EU cyber ecosystem and global cyber environment to enhance cooperation in international law contexts.

Target audience

Participants should be mid-ranking to senior officials dealing with aspects of cybersecurity. Course participants must be available throughout the course and should be ready to contribute knowledge from their specific fields of expertise and experience.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Basics of Cybercrime Investigation (Activity No 217)

Location: Budapest

Dates: 2nd semester 2024-25

Course aim

This course provides an overview of strategic cybersecurity, focusing on the role of cybercrime within current threats. It covers the characteristics and types of and future trends in cybercrime, along with its legal aspects, including material, procedural and international law. Participants will learn about the tasks of international organisations in addressing cybercrime and gain foundational knowledge of digital forensics to enable them to lawfully-record digital data.

Learning outcomes

By the end of this course, participants will be able to outline the principles of European cybersecurity strategies and will understand the responsibilities of law enforcement in response to attacks on public and private organisations. They will become familiar with national and international laws in cyberspace and the basics of digital forensics. Participants will learn to implement investigation practices aligned with international legislation, cooperate with law enforcement on cybersecurity incidents, and report cybercrime information to relevant stakeholders. They will analyse digital evidence and cyber-attack methods, manage cybercrime-related incidents, handle digital evidence lawfully, and decide on appropriate security mitigation measures.

Target audience

Participants should be law enforcement specialists with general knowledge regarding cybercrime and should use IT equipment on a daily basis and want to understand cybercrime from both regulatory and technical perspectives.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Countering Disinformation with Applied OSINT Techniques (Activity No 218)

Location: Chisinau, Moldova-Brussels, Belgium-Athens, Greece

Dates: 1 February – 30 March, 3-7 March, 31 March – 11 April 2025

Course aim

This course aims to enhance the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC by expanding its focus to include training on countering disinformation at both technical and strategic/operational levels. Participants will gain knowledge and skills through structured methods that incorporate advanced open-source intelligence (OSINT) techniques, lab exercises and practical scenarios. The course will also facilitate exchange of knowledge and best practices among personnel dedicated to countering disinformation campaigns. By the end, participants will have improved their effectiveness in large-scale open-source collection and creating more accurate intelligence to combat disinformation.

Learning outcomes

By the end of this course, participants will be able to define disinformation and misinformation and understand key concepts within the EU Cyber Security Strategy. They will explain how social media are exploited to disseminate disinformation, and how to identify its sources and analyse its impact on audiences. Participants will assess the intent and capabilities of disinformation actors, describe various tactics for large-scale information spread, and conduct effective fact-checking and validation. They will perform social network analyses to investigate troll bot networks, set up collection environments for X (ex Twitter), and develop techniques for real-time collection of information on troll networks, ultimately selecting the most appropriate methods for gathering information from open sources.

Target audience

Participants should be officials dealing with aspects of intelligence, security and cybersecurity, from MS and EU institutions and agencies. Course participants must be available throughout the course and should be ready to participate within their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

Cyber Awareness for Trainers (Activity No 259)

Location: Pocking, Germany

Dates: 14-18 August 2025

Course aim

This course aims to train participants as training managers and trainers, standardising cyber-awareness training across EU Member States and institutions. It emphasises networking among individuals to foster collaboration and ultimately supports the implementation of effective cybersecurity awareness programmes within the EU framework.

Learning outcomes

By the end of this course, participants will be able to identify key cyber vulnerabilities and associated risks, understand the role of cyber awareness in enhancing security, and outline the main objectives of training programmes. They will gain skills in designing and implementing effective training by applying essential principles and evaluation techniques. Additionally, participants will learn to assess training needs, navigate barriers and enablers at the organisational level, and create conceptual evaluation frameworks for their cyber-awareness training courses.

Target audience

The target audience for this training programme is civilian or military personnel within an organisation with responsibility for developing, implementing and evaluating cybersecurity awareness programmes in support of wider organisational security objectives.

Course open to

- EU Member States - institutions
- NATO CCD CoE
- Switzerland

Open-Source Intelligence (OSINT) (Activity No 261)

Location: Athens, Greece

Dates: 5-16 May 2025

Course aim

This course is designed to enhance the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC by expanding its focus on technical and strategic/operational training in OSINT. Participants will gain knowledge, skills and competencies through structured information collection methods, hands-on lab exercises and practical scenarios. Additionally, the course serves as a forum for OSINT operators to exchange knowledge and best practices. By the end of the course, participants will be better equipped to collect intelligence from open sources using structured analytical techniques, leading to more accurate assessments to address intelligence questions.

Learning outcomes

By the conclusion of this course, participants will be able to identify the principles and types of OSINT sources, understand key concepts within the EU Cyber Security Strategy, and evaluate webpages effectively. They will also recognise entities involved in the EU Intelligence Framework and comprehend cognitive biases that affect OSINT collection. Participants will learn about internet functionality and computer networks and be able to use various search engines, Boolean operators and OSINT tools effectively. They will develop structured approaches to gathering information from open sources, ensuring they can respond accurately to intelligence inquiries.

Target audience

Participants should be officials dealing with aspects of intelligence, security and cybersecurity, from MS and EU institutions and agencies. Course participants must be available throughout the course and should be ready to participate within their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

Cyber Defence Policy on National and International Levels (Activity No 262)

Location: Tartu, Estonia

Dates: 17-21 March 2025

Course aim

This course aims to equip participants with a conceptual framework for strategic thinking in cyber defence and to enhance their understanding of the integration of cyber considerations into both national and international security policies and strategies. It will provide foundational skills and knowledge to analyse and design effective policy frameworks and strategies for cyber defence. The curriculum offers an integrated overview of contemporary geopolitical affairs and security issues, encouraging participants to think creatively and critically about strategically important topics.

Learning outcomes

By the end of this course, participants will be able to identify key features of the modern security environment and define the role of cyberspace as a crucial enabler in hybrid conflicts. They will understand the military's reliance on communication and information systems, recognise the significance of cyberspace to national security and grasp fundamental technological aspects of cybersecurity. Participants will classify national power instruments in relation to cyberspace effects, analyse strategic cybersecurity issues within the national security landscape, and apply relevant terminology and concepts. They will evaluate cyberspace policies and develop strategic concepts for cyber defence, assess the role of cyber defence in broader security contexts, and identify measures for ensuring national security in the digital era.

Target audience

Participants should be mid-ranking to senior officials from the defence and security sector dealing with strategic aspects of cybersecurity and cyber defence, from EU MS and relevant EU institutions and agencies. They should either be working in key positions or have clear potential to achieve leadership positions, in particular in cybersecurity or defence. Course participants must be available for the entire course and should be ready to bring their specific expertise and experience to bear throughout the course.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Security Operations Centre (SOC) as a Template (Activity No 263)

Location: Bucharest, Romania
Dates: December 2024

Course aim

This course aims to provide participants with up-to-date knowledge on implementing and operating a SOC in alignment with the operational requirements of the NIS2 Directive. It combines theoretical insights with extensive hands-on training, equipping participants with the skills and competencies necessary to work on realistic SOC analysis scenarios. The course fosters a systematic approach to cybersecurity, evidence-based analysis, and the application of best practices from field experts. By the end of the course, participants will learn how to establish and manage a SOC, detect cyber-attacks, and effectively communicate SOC findings.

Learning outcomes

After completing this course, participants will be able to describe the NIS2 Directive and its relevance to incident response, and to understand the theoretical foundations of a SOC. They will be able to analyse the establishment, governance, and operational aspects of a SOC. Participants will be able to explain the five key responsibilities of the Chief Information Security Officer, operate various SOC tools and apply best practices and cybersecurity controls. They will develop skills in network monitoring, recognise cyber-attacks, practice incident response, and conduct digital forensics to collect artifacts, culminating in effective reporting of SOC findings.

Target audience

Participants should be military or civilian officials dealing with cybersecurity tasks, from EU institutions, bodies and agencies and EU Member States.

Course open to

- EU Member States - institutions
- EU candidate countries

Cyber Threat Management (Activity No 264)

Location: Budapest, Hungary

Dates: 7-10 October 2024

Course aim

This course aims to provide participants with in-depth knowledge of the top cyber threats and prepare them to confront both current and emerging cyber threats effectively. It offers insights into the organisational and technical measures that security experts can deploy against the threats analysed. Participants will gain a comprehensive understanding of each threat's potential harm to organisational assets, the vulnerabilities they can exploit, and the security measures necessary to mitigate associated risks.

Learning outcomes

By the end of this course, participants will be able to describe the major cyber threats facing organisations today and to define generic attack methods and techniques. They will understand the stages of cyber-attacks related to specific threats and the importance of both organisational and technical security measures. Participants will also learn about cyber-threat intelligence management practices, analyse various cyber threats and apply frameworks such as MITRE ATT&CK and the Cyber Kill Chain. Additionally, they will analyse vulnerabilities, propose specific security measures, identify and prioritise these measures, and understand the contributions of security measures in combating threats.

Target audience

The course is designed for personnel with an intermediate level of knowledge in cybersecurity. Participants should be technical experts (civilians or military personnel), from MS, EU institutions and agencies.

Course open to

- EU Member States - institutions
- EU candidate countries

Cyber Incident Responder (Activity No 265)

Location: Nicosia, Cyprus

Dates: 1 February-30 March,March-June 2025

Course aim

The aim of this course is to equip participants with the skills to analyse, evaluate and mitigate the impact of cybersecurity incidents while identifying the root causes of these incidents and the malicious actors behind them. This course will enable mid-ranking to senior officials to exchange views and share best practices regarding Security Operations Centres (SOCs) and CSIRTs, enhancing their knowledge, skills, and competencies. By the end of the course, participants will have learned how to employ specific tactics, techniques, procedures and tools effectively to cope with large-scale cyber-attacks within a Windows network/domain.

Learning outcomes

By the end of this course, participants will be able to identify incident-handling tools and communication procedures and describe the incident response process for Windows cyber-attacks. They will be able to outline the steps for effective incident response and understand the operation of Security Operations Centres (SOCs) and best practices for incident response. Participants will discuss relevant cybersecurity laws and regulations, manage and analyse log files, and collect, analyse and correlate cyber-threat information from various sources. They will identify cyber threats using host, network and log analysis, build an incident response plan and use cyber-incident response tools effectively. Additionally, they will apply incident-response steps dynamically, use indicators of compromise to respond to breaches, assess and manage technical vulnerabilities, and evaluate the effectiveness of cybersecurity incident detection and response measures.

Target audience

The participants should be mid-ranking to senior military or civilian officials dealing with cyber-incident response, or SOC and cybersecurity professionals, from EU institutions, bodies and agencies, EU Member States and the Western Balkans.

Course open to

- EU Member States - institutions
- EU candidate countries

Penetration Tester (Activity No 266)

Location: N/A

Dates: November 2024

Course aim

The course aims to equip participants with both fundamental and advanced knowledge of penetration testing, using free and open-source tools, applications and scripts. Designed for mid-ranking to senior officials, the course encourages exchange of insights and best practices among peers, enhancing their skills and competencies in the field. By integrating theoretical lectures with practical labs, the course will give participants the skills necessary to plan and execute penetration tests effectively on systems, applications and services, ultimately improving their ability to identify vulnerabilities in IT systems.

Learning outcomes

Participants will gain a comprehensive understanding of penetration-testing methodologies and categories, distinguishing penetration testing from vulnerability assessments and red/purple teaming. They will learn to identify security measures for operating systems and networks, use open-source tools and apply the five phases of penetration testing. Additional skills include conducting social engineering, information-gathering, ethical hacking and technical analysis. Participants will also develop the ability to communicate findings to stakeholders, document results and ensure compliance with regulatory standards, thereby enhancing their overall cybersecurity assessment capabilities.

Target audience

Participants should be mid-ranking to senior military or civilian officials dealing with penetration testing, and cyber-incident monitoring, or SOC and cybersecurity professionals, from EU institutions, bodies and agencies and EU Member States.

Course open to

- EU Member States - institutions

Cyber Threat Intelligence (Activity No 267)

Location: Brussels, Belgium

Dates: 25-28 September 2024

Course aim

The course aims to enhance understanding of cyber-threat intelligence (CTI) at tactical, operational and strategic levels, fostering a robust security skill set and developing existing competencies. It emphasises raising personnel awareness of actionable threats, empowering organisations to implement protective and detective measures that mitigate potential damage through prevention. Additionally, the course facilitates exchange of insights among mid-ranking to senior officials on CTI topics, enhancing their collective knowledge and skills.

Learning outcomes

By the end of the course, participants will be adept at recognising adversary tactics, techniques and procedures, and applying structured analytical techniques essential for any security role. They will learn about CTI mechanisms, elements and tools, and how to consume and disseminate intelligence effectively. Participants will identify methodologies and incident-handling procedures from a CTI perspective, apply structured analytic techniques and create custom CTI procedures. Furthermore, they will analyse information from diverse sources, produce actionable intelligence and generate formal reports to communicate their findings, ultimately strengthening their organisation's security posture.

Target audience

Participants should be mid-ranking to senior military or civilian officials dealing with CTI and national intelligence, or SOC and cybersecurity professionals, from EU institutions, bodies and agencies and EU Member States.

Course open to

- EU Member States - institutions

Intelligence Analysis (Activity No 268)

Location: Athens. Greece

Dates: 19 – 30 May 2025

Course aim

The course aims to enhance the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC by providing foundational training in the Intelligence Analysis discipline at the strategic and operational levels. It focuses on equipping participants with the knowledge, skills and competencies needed to apply structured intelligence analysis techniques in diverse scenarios. Additionally, the course serves as a forum for all-source analysts to exchange insights and best practices, fostering collaboration within the field. By the end, participants will be proficient in the entire intelligence analysis process, using structured methods to generate accurate and unbiased assessments.

Learning outcomes

Participants will develop a robust understanding of the EU Intelligence Framework, including key entities and foundational principles of intelligence work. They will learn to recognise cognitive biases that can distort analysis and explore cognitive processes related to thinking and memory, enhancing their decision-making skills. The course will emphasise the use of argumentation and structured analytical techniques, such as SWOT analysis and scenario planning, enabling participants to construct logical, persuasive analyses. Additionally, they will practice creating relevant scenarios and indicators, synthesising information from diverse sources and discerning the most accurate data to support their findings. By adopting a systematic approach to answering intelligence questions, participants will be empowered to produce well-supported, actionable intelligence that contributes to their organisations' strategic objectives.

Target audience

Participants should be officials dealing with aspects of intelligence, security and cybersecurity, from MS, EU institutions and agencies. Course participants must be available throughout the course and should be ready to participate within their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

Image Intelligence Analysis (IMINT) (Activity No 269)

Location: Athens, Greece

Dates: 9-20 September 2024

Course aim

This course aims to provide comprehensive training in IMINT at the technical and tactical/operational levels. Participants will learn to identify and analyse targets, utilise ArcGIS and other relevant tools and create IMINT products based on their findings. The course also fosters a collaborative environment for IMINT operators to exchange knowledge and best practices, enhancing their skills and aligning with the objectives of the CSDP. By the end of the course, participants will be proficient in developing reports and products that effectively communicate their analytical insights.

Learning outcomes

Participants will gain a foundational understanding of the principles of IMINT and its role within the intelligence cycle. They will learn to recognise the characteristics of remote sensing and different projections, determining the appropriate projection systems for various applications. Skills will be developed in target analysis, including identifying and categorising targets, applying detection techniques and analysing data using ArcGIS software. Participants will also learn to evaluate the potential impact of targets on operational environments, compose prioritised target lists and adopt a structured approach to answering intelligence requirements through imagery analysis.

Target audience

Participants should be officials dealing with aspects of imagery intelligence, intelligence support to targeting, intelligence surveillance and reconnaissance operations and geospatial intelligence.

Course open to

- EU Member States - institutions

Maritime Cybersecurity (Activity No 270)

Location: Constanta, Romania

Dates: 14-16 April 2025

Course aim

This two-day course provides a comprehensive overview of EU cybersecurity policy drivers, technological tools, and strategies for identifying and managing cyber threats in the maritime sector. Designed to align with the EU's Cybersecurity Strategy for the Digital Decade and the Strategic Compass, it combines expert-led lectures, interactive workshops and real-world case studies. By the end of the course, participants will have gained essential practical knowledge and skills to effectively tackle maritime cybersecurity challenges from both policy and technical perspectives in a technologically advanced and interconnected environment.

Learning outcomes

Participants will develop a solid understanding of EU regulatory frameworks and policy instruments related to maritime cybersecurity, identifying key national and EU entities involved. They will learn the fundamental concepts of the EU Cybersecurity Strategy and gain insights into advanced technological tools and best practices. Skills will be honed in identifying, analysing and managing maritime cyber threats, ensuring that relevant policies and regulations are complied with. Additionally, participants will improve their abilities to collaborate and communicate with stakeholders, navigate simulated cybersecurity crises and recognise their personal and professional responsibilities in ethical decision-making. By applying principles of responsible autonomy, they will be equipped to make informed decisions in complex scenarios while upholding ethical standards.

Target audience

Participants should be officials dealing with aspects of cybersecurity, from coastal MS or EU institutions and agencies. Course participants must be available throughout the course and should be ready to participate in line with their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

Implementation of Cybersecurity Technical Controls (Activity No 272)

Location: Chania, Greece

Dates: Spring 2025

Course aim

This course aims to emphasise the importance of critical security controls and provide a comprehensive understanding of essential cybersecurity functions and incident response. Participants will learn to differentiate performance among various security devices and acquire practical tips for mitigating common threats. Additionally, hands-on training in a lab environment will add to theoretical knowledge and enhance skills in addressing cybersecurity challenges.

Learning outcomes

Participants will gain knowledge of best practices and standards in critical cybersecurity controls, examining methodologies for implementing essential functions and outlining basic incident response procedures. They will explore common tools for managing cyber threats and understand Defence in Depth techniques, including endpoint detection and response, management, monitoring and endpoint investigation. In addition, participants will develop skills in network traffic analysis and recognise the processes associated with implementing effective cybersecurity functions. By familiarising themselves with first-responder protocols for prevalent client-side attacks, they will enhance their ability to respond to incidents effectively and improve their overall cybersecurity posture.

Target audience

Participants should be civilian or military personnel in IT who want to gain essential understanding and practical tools needed to perform actions to successfully mitigate the most common threats in order better to support their organisation's mission.

Prerequisites:

- good work/administration experience in the Linux and Windows environments, especially command line;
- intermediate level of knowledge and experience in IT or networking;
- intermediate level of knowledge of some of these topics: basic information security controls, cryptography concepts, secure communications.

Course open to

- EU Member States - institutions
- EU candidate countries
-

The Contribution of Cyber in Hybrid Conflict (Activity No 274)

Location: Helsinki, Finland

Dates: 25-29 November 2024

Course aim

This course aims to educate participants on the key elements of cyber and hybrid threats, alongside potential responses, while offering a decision-making exercise to deepen their understanding of how to navigate the complexities arising from these threats. Participants will engage in a tabletop exercise that simulates an adversarial context, allowing them to explore the implications of cyber and hybrid attacks in a controlled environment. Additionally, the course fosters networking opportunities and intellectual cross-fertilisation among diverse communities that may not frequently interact.

Learning outcomes

Participants will gain a clear understanding of digital technologies and the terminology related to cybersecurity, cyber defence and threats, and how these elements interact in real-world scenarios. They will familiarise themselves with the EU's institutional landscape and arrangements for addressing cybersecurity and hybrid threats. The course will delve into hybrid threats through a conceptual framework, identifying key actors, domains, tools and threat phases, while also examining their implications in contemporary conflicts, such as the war in Ukraine. Participants will learn to recognise malicious activities in cyberspace, manage cyber considerations in planning responses to hybrid threats and assess their impact on multinational operations. Finally, they will develop the skills to design strategic policy options to effectively counter cyber and hybrid threats and campaigns.

Target audience

The course is for specialist and non-specialist strategic-level mid-to-senior-rank military officers and equivalent civilian officials in (or preparing for) cyber- / hybrid-related practitioner roles in EU institutions, or in Member State ministries (e.g. MoD; MoI; MoFA), relevant agencies, or military HQs, who:

- are involved in developing policies, strategies, concepts or doctrine related to cybersecurity, cyber defence or hybrid threats/campaigns; and/or

- design or deliver professional education courses, individual training courses, or command-post exercises related to cybersecurity, cyber defence, or hybrid threats/campaigns.

Course open to

- EU Member States - institutions

Cybersecurity and Smart Cities (Activity No 275)

Location: Brussels, Belgium
Dates: 2nd semester 2024-25

Course aim

This course aims to educate participants about cybersecurity and IoT security at the city level, particularly in the context of smart cities. It highlights the role of local governments and stakeholders in transforming urban and business activities—such as mobility, transactions and supply chains—through technology. By exploring these dynamics, participants will gain insights into the unique cybersecurity challenges and opportunities that arise in smart city environments.

Learning outcomes

Participants will learn to recognise smart facilities and services within a city and identify the various cyber threats that urban environments face. They will grasp fundamental concepts related to cybersecurity and cyber defence and identify local stakeholders and EU institutions involved in these areas. The course will address emerging trends in cyber threats and international issues, including cyber diplomacy, and outline models and frameworks for assessing cybersecurity. Participants will evaluate the levels of protection of individuals and organisations, understand the potential impacts of cyber threats on smart city growth, and identify challenges that local governments encounter in raising community awareness about cybersecurity. Additionally, they will describe collaborative frameworks among stakeholders for recovering from cyber-attacks, assess safety levels and outline processes that cities should follow to enhance cybersecurity and resilience. Practical applications of safety frameworks at the individual level will also be emphasised.

Target audience

Municipal staff and civil servants working for the national government at local agencies. All those taking part in the course participate in smart city planning and smart service delivery in the urban space, where they are exposed to several types of threats. Priority is given to participants from EU Member States. However, non-EU citizens as well as NATO staff are welcome.

Course open to

- EU Member States - institutions
- EU candidate countries
- NATO

Cybersecurity Educator (Activity No 278)

Location: Podgorice, Montenegro
Dates: 21-25 October 2024, 7-11 May 2025

Course aim

This course aims to provide participants with up-to-date knowledge on behavioural-science-based predictors that enhance the success of cybersecurity training for staff. It will cover strategies to increase motivation and commitment, time-efficient methods for assessing individual cyber risks and individualisation of training measures. Participants will also explore conditions that foster sustainable training effects. Additionally, the course facilitates exchange of views and best practices in cybersecurity awareness interventions, improving participants' knowledge, skills and competencies in this critical area.

Learning outcomes

Participants will learn about emerging trends and key features of social engineering, including the psychological mechanisms that underlie these tactics. They will identify typical challenges and limiting factors in awareness training and explore scientific models that guide effective interventions. Skills will be developed in evaluating the quality of external consultancy offers for awareness programmes and identifying critical elements that contribute to sustainable training outcomes. Participants will assess observable and latent characteristics associated with cyber-resilience and apply intervention mapping as an educational technique. They will also adopt a structured approach to planning, executing and evaluating interventions, create formal reports assessing critical outcome indicators and use empirically validated scientific concepts to ensure the success of their interventions.

Target audience

The participants should be mid-ranking to senior military or civilian officials dealing with information security and cybersecurity, from EU institutions, bodies and agencies, EU Member States and third countries.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

Digital Forensics Investigator (Activity No 279)

Location: Athens, Greece

Dates: 2nd semester 2024-25

Course aim

The aim of this course is to equip participants with the skills necessary to analyse, evaluate and collect artefacts related to cybersecurity incidents while identifying the root causes and malicious actors involved. It facilitates knowledge-sharing among mid-ranking to senior officials regarding security operation centres (SOCs) and CSIRTs. By the end of the course, participants will acquire specific tactics, techniques, procedures and tools essential for managing large-scale cyber-attacks within a Windows network/domain.

Learning outcomes

Participants will learn to describe best practices and standards in digital forensics, as well as methodologies and frameworks used in forensic analysis. They will gain insights into digital forensics procedures, enabling them to select appropriate malware analysis tools and discuss relevant cybersecurity laws and regulations. Skills will be developed in collecting digital artifacts, using malware analysis tools and identifying, analysing and correlating cybersecurity events. Participants will also learn to produce detailed investigation reports, apply forensic investigation policies and document, recover, extract and analyse digital evidence systematically. In addition, they will learn how to preserve digital evidence for authorised stakeholders and inspect environments for signs of unauthorised actions, ultimately presenting their forensic analysis findings effectively.

Target audience

Participants should be mid-ranking to senior military or civilian officials dealing with cyber-incident response and SOC and cybersecurity professionals from EU institutions, bodies and agencies, EU Member States and the Western Balkans.

Course open to

- EU Member States - institutions
- EU candidate countries

Hybrid Threats and Intercultural Strategic Communication (Activity No 280)

Location: Brussels, Belgium

Dates: 7-11 April 2025

Course aim

The aim of this course is to enhance strategic communication skills within the framework of the CSDP. It seeks to improve collaboration among allies from diverse cultures while promoting effective listening techniques for both overt and covert discourse of adversaries and hostile forces. Participants will acquire the tools to analyse narratives and discourses related to FIMI (Foreign Information Manipulation and Interference), artificial intelligence and other hybrid threats.

Learning outcomes

Participants will learn to define intercultural strategic communication and its components, particularly in the context of cognitive warfare dynamics. They will identify applications of cognitive communication and frame semantics in CSDP missions, reflecting on emerging trends in cyber threats, FIMI and AI. The course will outline the EU's approach to countering hybrid threats and the key entities involved in this ecosystem. Participants will develop a strategic thinking approach to communication across diverse cultures, applying both implicit and explicit dialogue skills to uncover underlying meanings. They will learn UN deep-listening techniques and how to analyse story-telling across cultures, including its use by hostile forces. Additionally, participants will select appropriate communication techniques to foster cohesion and use analytical tools to discern speakers' world-views, thereby creating synergies between the EU ecosystem and the hybrid threats landscape.

Target audience

Participants should be mid-ranking to senior officials, either non-experts or dealing with tactical and/or technical aspects of cyber defence, FIMI or other hybrid threats, from MS, relevant EU institutions and agencies. Course participants must be available throughout the course and should be ready to contribute in line with their specific fields of expertise and experience.

Course open to

- EU Member States - institutions

ESDC Pilot Courses

The ESDC also plans to offer the following pilot courses, which, if successful, will become regular ESDC courses.

Pilot Course Title	Dates	Venue
SQF-MILOF Train the Trainers	10-13 March 2025	Sibiu, Romania
The European Gendarmerie Force in Crisis Management Operations	16-27 September 2024	Vincenza, Italy
Women, Peace and Security: Looking at WB and MENA Regions	2-6 December 2024	Thessaloniki, Greece
PSYOPS for Peace, Security and Defence	9-12 December 2024	Rome, Italy
Strategic Security Foresight	4-6 February 2025	Paphos, Cyprus
Sustainable and Resilient Leadership for CSDP	3-7 March 2025	Brussels, Belgium
Advanced Cyber Range Training for Maritime Cyber Resilience	25-28 March 2025	Constanta, Romania
European Union Higher Military Education	31 March – 3 April 2025	Thessaloniki, Greece
Human Security	14-16 April 2025	Brussels, Belgium
Practical Strategies for Mitigating AI-Driven Cyber Attacks	23-25 April 2025	Constanta, Romania
Medical Security (MedSec)	5-10 May 2025	Stockholm, Sweden
Crisis Management in a Multilateral Framework	12-15 May 2025	Sofia, Bulgaria
Advising and Training Mission Operator Fundamentals – A Comprehensive Approach in Defence and Security	3-5 June 2025	Rome, Italy