20 YEARS
European Security and Defence College

European Security and Defence College

Training Catalogue 2026/27

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 Ó Regan
Head of the European Security and Defence College

European Security and Defence College
Doc: ESDC/2026/185
Date: 20 May 2026
Origin: ESDC Secretariat

Contents

Foreword 1
Register for an ESDC course – Nomination process 6
What the ESDC offers 7
Course list 7
E-Learning – Autonomous Knowledge Units (AKUs) 9
Course Details 10
ESDC Regular Courses 10
CSDP High-Level Course (Activity No 1) – Modular Course 10
Training of Trainers (Activity No 2) 12
CSDP Orientation Course (Activity No 3) 13
Capability Planning and Development Course (Activity No 8) 15
Basic Course on Security Sector Reform (Activity No 10) 16
Core Course on Security Sector Reform 17
Course on Recovery and Stabilisation Strategies (Activity No 14) 19
Course on International Law for Military Legal Advisers (Activity No 15) 20
EU-NATO Cooperation (Activity No 16) 21
Civilian Aspects of EU Crisis Management (Activity No 17) 22
Training of eTrainers (Activity No 19) 23
A Comprehensive Approach to Gender in Operations (Activity No 21) 25
Course on European Armament Cooperation (Activity No 25a + 25b) 27
Challenges of space for CSDP (Activity No 27) 28
Mediation, Negotiation and Dialogue Skills for CSDP (Activity no 28) 29
Cognitive Warfare in the new international competition (Activity No 29) 30
Comprehensive Protection of Civilians (Activity No 30) 31
Cross-Cultural Competence in CSDP (Activity No 32) 33
Pre-deployment Training for CSDP Missions and Operations (Activity No 33) 34
Scenario-Based Civil Defence Course (Activity No 34) 36
The challenges of securing maritime areas for the European Union (Activity No 36) 37
EU Integrated Crisis Management (Activity No 37) 38
EU Addressing and Facing Hybrid Threats and Challenges (Activity No 40) 39
Monitoring, Mentoring and Advising in EU Crisis Management (Activity No 43) 40
Disaster Relief in CSDP Context (Activity No 44) 41
HEAT - Hostile Environment Awareness Training (Activity No 48a) 43

Vehicle Safety and 4x4 Driving (Activity No 48b) 45
Advanced Modular Training (AMT) for CSDP Strategic Crisis Management (Activity No 51) – Modular Course 46
The Climate-Environment-Security and Defence Nexus (Activity No 52) 48
Strategic Communication for Peace, Security and Defence (Activity No 53) 50
Investigating & Preventing Sexual and Gender-Based Violence in Conflict Environments (Activity No 55) 52
Project Management in support of CSDP M/O – PM2 (Activity No 58) 53
Energy Security (Activity No 59) 54
Reflective Leadership in Complex Environments (Activity No 62) 55
Senior Strategic Course (Activity No 64) – Modular course 56
Diplomatic Skills for Peace, Security and Defence (Activity No 67) 57
Cultural Heritage Protection Course (Activity No 68) 58
Advanced Diplomacy for Peace, Security and Defence (Activity No 69) 59
Integrated Border Management (IBM) in CSDP (Activity No 72) 60
European gendarmerie forces in crisis management operations (Activity No 75) 61
Foreign Information Manipulation and Interference (Activity No 76) 62
Advanced Research into Hybrid Threats (Activity No 77) 64
Modern Leadership in the Context of Law of Armed Conflicts and Open-Source Intelligence (Activity No 78) 65
Security in the Black Sea region (Activity No 79) 66
Artificial Intelligence, Security and Cooperation in the EU (Activity No 80) 67
Team and Conflict Management in Peace Operations (Activity No 81) 68
PsyOps for Peace, Security and Defence (Activity No 82) 69
Mission Medical Security course (Activity No 83) 70
Women, Peace and Security (Activity No 84) 71
Strategic Leadership in Security and Intelligence Culture (Activity No 85) 73
Medical Advisor (Activity No 86) 74
Crisis Management in Multilateral Frameworks (Activity No 87) 75
Challenges of European Cybersecurity (Activity No 200) 76
Critical Infrastructure in the Context of Digitization (Activity No 202) 77
CSIRT Fundamentals (Activity No 204) 78
Cybersecurity Risk Management (Activity No 205) 79
Cyber Diplomacy Advanced (Activity No 207b) 80
Critical Entities Resilience Advanced (Activity No 208b) 81

The EU's Cybersecurity Strategy for the Digital Decade (Activity No 209) 82
Cyber Range - Pentester Tools (Activity No 213) 83
Data Governance (Activity No 214) 84
Cyber Range - Cybersecurity in Practice (Activity No 215) 85
Course on Cybersecurity and International Laws (Activity No 216) 86
Countering Disinformation with Applied OSINT Techniques (Activity No 218) 87
Chief Information Security Officer (CISO) (Activity No 220) 89
Practical Strategies for Mitigating AI-Driven Cyber Attacks (Activity No 225) 90
Advanced Cyber Range Training for Maritime Cyber Resilience (Activity No 226) 91
Advanced EU Security and Intelligence Awareness (Activity No 227) 92
Advanced FIMI Analysis (Activity No 228) 93
Military Aviation CEMA Resilience (Activity No 230) 94
AI in Cybersecurity: The new Frontier in Defence Strategies (Activity No 258) 96
Cyber awareness for Trainers (Activity No 259) 97
Cyber ETEE (Education, Training, Exercise and Evaluation) Summer School (Activity No 260) 98
Open-Source Intelligence (OSINT) (Activity No 261) 99
Cyber Defence Policy on National and International Levels (Activity No 262) 100
Cyber Threat Management (Activity No 264) 101
Intelligence Analysis (Activity No 268) 102
Image Intelligence Analysis (IMINT) (Activity No 269) 103
Maritime Cybersecurity (Activity No 270) 104
Cyber awareness Raising-in-a-Box (Activity No 271) 105
Implementation of Cybersecurity Technical Controls (Activity No 272) 106
The Contribution of Cyber in Hybrid Conflict (Activity No 274) 107
Cybersecurity Educator (Activity No 278) 108
Hybrid Threats and Intercultural Strategic Communication (Activity No 280) 109
ESDC Pilot Courses 110
The Climate-Environment-Security and Defence Nexus (advanced) 110
Drones and Unmanned Systems in European Security 110
Hydro Diplomacy: A tool for Climate and Environmental Resilience, Peace and Security 110
Info-Ops for Peace, Security and Defence 110
AI in Intelligence 110
Environmental Management for CSDP 110
Intelligence Standardisation, Reporting and Briefings 110

Military Diplomacy 110

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 during 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 an official invitation letter has been disseminated.

Publication of a course usually takes place three months before the start of the course. Applications are not submitted directly, they 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) 2024/3116 of 09 December 2024 on the European Security and Defence College, and repealing Decision (CFSP) 2020/1515 https://eur-lex.europa.eu/eli/dec/2024/3116/oj/eng

What the ESDC offers

Course list

The ESDC will offer the following courses in the academic year 2026-2027. 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://www.esdc.europa.eu/training-and-education/course-catalogue-and-curricula_en. In each curriculum, you will find a more detailed description of the course objectives and a detailed list of learning outcomes.

- CSDP High-Level Course
- Training of Trainers
- CSDP Orientation Course
- Capability Planning and Development Course
- Basic Course on Security Sector Reform
- Core Course on Security Sector Reform
- Course on Recovery and Stabilisation Strategies
- EU-NATO Cooperation
- Civilian Aspects of EU Crisis Management
- Training of eTrainers
- A Comprehensive Approach to Gender in Operations
- Course on European Armament Cooperation
- Challenges of space for CSDP
- Mediation, Negotiation and Dialogue Skills for CSDP
- Cognitive Warfare in the new international competition
- Comprehensive Protection of Civilians
- Cross-Cultural Competence in CSDP
- Pre-deployment Training for CSDP Missions and Operations
- Scenario-Based Civil Defence Course
- 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
- HEAT - Hostile Environment Awareness Training
- Vehicle Safety and 4x4 Driving
- Advanced Modular Training (AMT) for CSDP Strategic Crisis Management
- The Climate-Environment-Security and Defence Nexus
- Strategic Communication for Peace, Security and Defence

- Investigating & Preventing Sexual and Gender-Based Violence in Conflict Environments
- Project Management in support of CSDP M/O – PM2
- Energy Security
- Reflective Leadership in Complex Environments
- Senior Strategic Course
- Diplomatic Skills for Peace, Security and Defence
- Cultural Heritage Protection Course
- Advanced Diplomacy for Peace, Security and Defence
- Integrated Border Management (IBM) in CSDP
- European gendarmerie forces in crisis management operations
- Foreign Information Manipulation and Interference
- Advanced Research into Hybrid Threats
- Modern Leadership in the Context of Law of Armed Conflicts and Open-Source Intelligence
- Security in the Black Sea region
- Artificial Intelligence, Security and Cooperation in the EU
- Team and Conflict Management in Peace Operations
- PsyOps for Peace, Security and Defence
- Mission Medical Security course
- Women, Peace and Security
- Strategic Leadership in Security and Intelligence Culture
- Medical Advisor
- Crisis Management in Multilateral Frameworks
- Challenges of European Cybersecurity
- Critical Infrastructure in the Context of Digitization
- CSIRT Fundamentals
- Cybersecurity Risk Management
- Cyber Diplomacy Advanced
- Critical Entities Resilience Advanced
- The EU's Cybersecurity Strategy for the Digital Decade
- Cyber Range - Pentester Tools
- Data Governance
- Cyber Range - Cybersecurity in Practice
- Course on Cybersecurity and International Laws
- Countering Disinformation with Applied OSINT Techniques
- Chief Information Security Officer (CISO)
- Practical Strategies for Mitigating AI-Driven Cyber Attacks
- Advanced Cyber Range Training for Maritime Cyber Resilience
- Advanced EU Security and Intelligence Awareness

- Advanced FIMI Analysis
- Military Aviation CEMA Resilience
- AI in Cybersecurity: The new Frontier in Defence Strategies
- Cyber awareness for Trainers
- Cyber ETEE (Education, Training, Exercise and Evaluation) Summer School
- Open-Source Intelligence (OSINT)
- Cyber Defence Policy on National and International Levels
- Cyber Threat Management
- Intelligence Analysis
- Image Intelligence Analysis (IMINT)
- Maritime Cybersecurity
- Cyber awareness Raising-in-a-Box
- Implementation of Cybersecurity Technical Controls
- The Contribution of Cyber in Hybrid Conflict
- Cybersecurity Educator
- Hybrid Threats and Intercultural Strategic Communication
- The Climate-Environment-Security and Defence Nexus
- Drones and Unmanned Systems in European Security
- Hydro Diplomacy: A tool for Climate and Environmental Resilience, Peace and Security
- Info-Ops for Peace, Security and Defence
- AI in Intelligence
- Environmental Management for CSDP
- Intelligence Standardisation, Reporting and Briefings

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	Dates
Brussels, Belgium	5 – 10 October 2026
Madrid, Spain	23 – 27 November 2026
Tartu, Estonia	5 – 9 April 2027
Vienna, Austria	21 – 25 June 2027

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
- NGOs of EU Member States

Training of Trainers (Activity No 2)

Location: Boblingen, Germany
Dates: Winter 2026

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	14 - 18 September 2026
Budapest, Hungary	7 - 11 October 2026
Lisbon, Portugal	26 - 30 October 2026
Sofia, Bulgaria	02 - 06 November 2026
Brussels, Belgium	9 - 13 November 2026
Paris, France	Winter/Spring 2027
Thessaloniki, Greece	8 - 12 February 2027
Brussels, Belgium	15 - 19 March 2027
Zagreb, Croatia	5 - 9 April 2027
Brussels, Belgium	19 - 23 April 2027
Larnaca, Cyprus	10 - 14 May 2027
Madrid, Spain	31 - 04 June 2027
Bucharest, Romania	21 – 25 June 2027

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

Capability Planning and Development Course (Activity No 8)

Location: Brussels, Belgium
Dates: 28 September - 2 October 2026

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	29 September – 2 October 2026
Chisinau, Moldova	28 - 30 October 2026

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
Vienna, Austria	05 - 09 October 2026
Vienna, Austria	05 – 09 April 2027

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: 19 - 23 October 2026

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 organisations like the EU, NATO, UN, and OSCE. They will also be able to compare the crisis management approaches of these institutions. The course will emphasise 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 analyse conflicts, identify lessons learned, and develop recovery and stabilisation 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 stabilisation 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)

Location: Larnaca, Cyprus
Dates: Winter/Spring 2027

Course aim

The aim of the Course on International Law for Military Legal Advisers is to enhance the knowledge and understanding in the fields of international operational law and international humanitarian law (IHL). Through an extended practical exercise simulating an EU-led military CMO participants get to know the working method of a Legal Adviser in a multilateral setting. It is intended to increase information sharing, collaboration and cooperation among the participants, namely military and civilian personnel from the different states. This effect will be strengthened by rotating the composition of the syndicates. This course contributes to creating a legal adviser's network which enhances professional cooperation between Armed Forces and Ministries of Defence.

Learning outcomes

By the end of this course, participants will be able to identify and interpret legal issues arising in military operations, determine the applicable legal frameworks, and assess the legal consequences of operational decisions. They will develop practical skills to analyse situations, propose and prioritise legal solutions, and communicate legal advice effectively through presentations and oral advocacy. In addition, participants will strengthen their ability to work collaboratively within legal teams, evaluate problem-solving processes, and provide concise legal guidance to support commanders' decision-making.

Target audience

Participants should be military lawyers of civilian legal advisers in the Armed Forces or Ministries of Defence, particularly those who have been or are to be assigned to military crisis management operations as legal advisers. Participants must be available for the whole course, which includes eLearning and residential modules, and must be ready to actively contribute throughout the course.

Course open to

- Third Countries

EU-NATO Cooperation (Activity No 16)

Location: Garmisch, Germany
Dates: April 2027

Course aim

The course aims to enhance participants' understanding of the evolving EU–NATO strategic partnership, its institutional frameworks, areas of cooperation, and operational challenges in light of current global security dynamics. It will provide a platform for exchange among practitioners from EU, NATO, and partner countries, fostering a network of experts across the Euro-Atlantic space.

Learning outcomes

By the end of this course, participants will understand the strategic framework and evolution of EU-NATO cooperation, including key policy areas from the Warsaw Declaration, such as hybrid threats, cybersecurity, and defence capacity building. They will analyse the complementarities between CSDP and NATO's collective defence, identify cooperation opportunities, and assess Member States' policy priorities and geopolitical regional challenges.

Participants will gain skills to evaluate EU and NATO roles in crises, enhance burden-sharing and transatlantic relations, and develop recommendations for improving cooperation in resilience, military mobility, and countering hybrid threats, while integrating gender and human security perspectives.

Finally, learners will promote stronger EU-NATO-partner cooperation, interpret the functioning of both organisations, and critically analyse strategic documents like NATO's Strategic Concept and the EU's Strategic Compass. This course prepares participants to strengthen collaboration between the EU and NATO.

Target audience

Participants should be entry-/mid and senior level police, military personnel, diplomats, and civilian staff from EU Member States, EU institutions/agencies, NATO structures, CSDP missions/operations, with responsibilities in security policy.

Course open to

- EU Member States/Institutions
- Candidate Countries
- Third Counties, incl. NATO Allies
- International organisations

Civilian Aspects of EU Crisis Management (Activity No 17)

Location: Brussels, Belgium
Dates: 15 – 17 June 2027

Course aim

The course aims to enhance a shared understanding of the civilian aspects of EU crisis management among personnel from Member States, EU institutions, and relevant EU agencies. It seeks to improve comprehension of EU crisis management decision-making processes and provide insights into relevant CSDP instruments, such as the Civilian Compact, the Strategic Compass, and Lessons Learned. The course also examines current and future trends, challenges, and opportunities within civilian crisis management, focusing on fostering long-term partnerships with international, regional, and local actors. Additionally, it supports the creation of a professional network of experts in crisis management.

Learning outcomes

By the end of this course, participants will understand the EU crisis management process, assess the impact of EUGS principles (ownership, resilience, sustainability), and describe the EU's integrated approach and key actors' roles. They will analyse trends, challenges, and legal/financial aspects of CSDP missions, evaluate instruments like the Civilian Compact and Strategic Compass, and explore the links between internal/external security, gender, and human rights.
Learners will develop skills to analyse crisis management challenges, design prevention and response strategies, and create effective communication plans, including audience analysis and counter-misinformation tactics. They will critically review communication case studies and interpret mission documents (PFCA, SOMA, OPLAN).
Finally, participants will form independent opinions on CSDP missions, coordinate stakeholders, and apply intercultural and ethical communication principles. This course equips professionals to enhance EU crisis management effectiveness.

Target audience

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

Course open to

- EU Member States – institutions
- Non-EU participants
- NATO Staff

Training of eTrainers (Activity No 19)

Location: Online
Dates: Winter/Spring 2027

Course aim

This digital eTrainer course aims to empower educators to deliver engaging online training by focusing on core principles that enhance learning experiences. It highlights that even small adjustments in teaching methods can significantly boost student engagement and outcomes. While covering various evolving digital tools, the course underscores the importance of enduring pedagogical principles. Participants will build a solid foundation in digital pedagogy, adapting to any platform and learner needs, and they will receive feedback to ensure effective implementation and continuous improvement.

Learning outcomes

This course aims to equip participants with a comprehensive understanding of effective digital teaching and learning strategies. It begins by exploring the relationship between learning and teaching, emphasising principles like retrieval practice and outcome-based learning. Participants will learn about cognitive load theory and the importance of structured feedback, self-reflection, and social presence in enhancing student engagement. The course also addresses the integration of visual elements in both face-to-face and virtual settings, the impact of limited social interactions, and techniques for fostering social interaction online. Additionally, it highlights the significance of screen breaks, experimental learning, sound and video quality, and the challenges posed by the lack of non-verbal communication in online environments.

Further, the course delves into strategies for managing technical issues and environmental challenges in digital learning. It covers participatory learning and cognitively activating teaching methods, supported by AI tools to enhance educational outcomes. Participants will be guided on developing learning objectives using Bloom's Taxonomy, planning and implementing digital sessions with the BOPPPS model, and applying adult learning and feedback principles. The course also emphasises designing interactive, participatory activities and employing digital tools for a visually engaging learning experience. By the end, participants will be equipped to implement focus-enhancing techniques, utilise collaborative tools, and demonstrate delivery competencies in online teaching sessions.

Target audience

Participants can be experienced and unexperienced trainers from the civilian, police and military component, involved in learning related events in a national as well as international context. 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

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

Location	Dates
The Hague, The Netherlands	30 November – 04 December 2026
Menges, Slovenia	Spring 2027

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

Course on European Armament Cooperation (Activity No 25a + 25b)

Location	Dates
Brussels, Belgium	06 – 08 October 2026
Larnaca, Cyprus	09 – 13 November 2026

Course aim

The aim of the European Armament Cooperation course (EACC) is to enhance mutual understanding in the field of armament cooperation by offering participants the opportunity to engage in critical analysis of the armaments sector, identify the frameworks, stakeholders, tools and processes involved and understand the challenges at stake and benefits at EU level. The course will deliver EAC staff and managers who have received harmonised training to ensure they can efficiently undertake international armament cooperation projects with appropriate skills in the context of a developing CSDP.

Learning outcomes

By the end of this course, participants will be able to identify key stakeholders in armament cooperation and their roles, while analysing the political and economic factors influencing collaborative defence efforts. They will describe existing cooperation frameworks, apply strategic management principles, and incorporate best practices and lessons learned in the field.

Learners will explain the structures and processes of European institutions involved in armament, as well as current trends in capability development, research, and industrial cooperation. They will develop practical skills to implement armament cooperation strategies, utilise soft skills, and apply cultural awareness in multinational settings.

Additionally, participants will assess intercultural dynamics, lead discussions in multinational projects, and select the most appropriate cooperation model for procurement, in line with EU defence regulations. They will also manage procurement projects, managing requirements from research and development through to funding and acquisition. This course prepares participants to effectively navigate and lead international armament cooperation initiatives.

Target audience

The course is aimed at personnel working in the field of national and international armament cooperation who need to gain knowledge of cooperative acquisition and project management. It also supports experts looking to take on leadership positions in the wider defence area.

Course open to

- EU Member States,
- EU institutions, bodies and agencies
- States that have an administrative arrangement with the EDA

Challenges of space for CSDP (Activity No 27)

Location	Dates
Rome, Italy	12 – 15 October 2026
Paris, France	Spring 2027

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: Sofia, Bulgaria
Dates: 14 – 16 September 2026

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

Cognitive Warfare in the new international competition (Activity No 29)

Location: Rome, Italy
Dates: 23 - 26 November 2026

Course aim

This course is designed to enhance awareness by providing participants with the knowledge and skills to effectively understand the emerging competition in the cognitive dimension and its associated risks to the resilience and cohesion of EU institutions and societies.

Learning outcomes

The learning outcomes of this course emphasise the importance of understanding the cognitive dimension in both current and future competitive scenarios. Participants will learn to identify the challenges faced by civilian and military leaders due to cognitive operations, particularly those targeting civilian populations through modern influence tools. The course outlines the interdisciplinary nature of cognitive sciences, which encompasses fields such as psychology, neuroscience, AI, and anthropology, and highlights the legal and ethical concerns associated with the democratisation and dual-use of enabling technologies. Understanding human-machine interaction, particularly neural interfaces and biochemical interference, is presented as a crucial aspect of emerging competition, posing unprecedented challenges.

The course also focuses on the security needs and the impact of cognitive operations on political and social resilience, especially during peacetime. It emphasises the importance of EU-level efforts, like the "Strategic Compass," to combat disinformation and enhance resilience against cognitive manipulation through a "whole-of-society" approach. Participants will be encouraged to develop foresight skills to anticipate and respond to technological developments, which could otherwise catch concerned actors off-guard. Moreover, fostering societal trust and cohesion, recognising the role of research, and promoting responsible awareness in democracies are crucial for mitigating vulnerabilities to cognitive manipulation operations in today's digital landscape.

Target audience

The target audience should include civilian and military decision-makers, policymakers, and leadership involved in national security and defence. Additionally, individuals working in fields related to cognitive sciences, technology development, legal and ethical governance, and information strategy would benefit.

Course open to

- EU Member States – institutions

Comprehensive Protection of Civilians (Activity No 30)

Location: Stadtschlaining, Austria
Dates: 09 - 13 November 2026

Course aim

The course aims to give participants a comprehensive and critical understanding of the multiple dimensions and meanings of the protection of civilians (PoC) in armed conflict and crisis areas. This course enhances participants' knowledge and understanding of the EU integrated approach to conflict and crisis: It also aims to increase information sharing, collaboration and cooperation amongst the different actors, namely military, civilian crisis management, humanitarian and development aid actors in the wider context of CFSP/CSDP in the area of Protection of Civilians in Armed Conflict (PoC). The course is an excellent opportunity to network and exchange views with other professionals from various institutional, geographical and cultural backgrounds, all working towards improving the PoC in complex environments. The course will also provide an understanding of the challenges and problems facing civilians, police and military decision-makers in the field, as well as best practices aimed at preventing or responding to violence against civilians.

Learning outcomes

By the end of this course, participants will understand Protection of Civilians (PoC) principles, terminology, and legal frameworks, including approaches by the EU, UN, NATO, and ICRC. They will clarify roles and responsibilities of military, police, civilian, and humanitarian actors in conflict zones and identify key challenges and dilemmas in PoC operations, including gender and environmental considerations.

Participants will gain skills to plan and execute protection measures, conduct threat and risk assessments, and contribute to crisis management while addressing climate-related security risks. They will analyse conflict contexts, develop sustainable protection strategies, and apply PoC principles in their work.

Finally, learners will leverage lessons from past operations, foster multi-actor cooperation, and design effective, context-sensitive responses to protect civilians in armed conflict.

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 the area of peacekeeping, peacebuilding or international crisis management.

Course open to

- EU member States / Institutions

- Third countries
- Candidate countries

Cross-Cultural Competence in CSDP (Activity No 32)

Location	Dates
Kilkis, Greece	02 - 06 November 2026
Kilkis, Greece	14 - 18 June 2027

Course aim

The aim of the course is to provide participants with a comprehensive set of cross-cultural knowledge and skills. An additional aim is to establish a network of personnel with cross-cultural competence participating in CSDP missions and operations.

Learning outcomes

By the end of this course, participants will understand the internal diversity of cultural groups and recognise their own assumptions, stereotypes, and biases, as well as how these influence perceptions of others. They will explore the impact of language and cultural background on worldviews, develop communicative awareness of unique cultural expressions, and gain intercultural competence through training. Learners will also acknowledge differences in verbal and non-verbal communication across cultures and understand the dynamics of cultural, societal, and individual interactions. Participants will acquire skills to adopt multiple perspectives, research and interpret other cultural practices, and respond with empathy to diverse beliefs and values. They will adapt their thinking and behaviour to different cultural contexts, make informed judgments about cultural norms, and avoid behaviours that may cause offence. Learners will also manage communication breakdowns, use language skills for inter-comprehension, and act as mediators in intercultural exchanges. Finally, participants will embrace openness to learning from diverse cultural perspectives, demonstrate empathy towards those with different backgrounds, and challenge their own cultural assumptions. They will tolerate ambiguity, seek opportunities for cross-cultural engagement, and foster cooperation with individuals from varied cultural orientations. This course equips participants with the skills and mindset to navigate and bridge cultural differences effectively.

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
- Third countries
- Candidate countries

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

Location	Dates
Brussels, Belgium	05 - 09 October 2026
Brussels, Belgium	09 - 13 November 2026
Brussels, Belgium	07 - 11 December 2026
Brussels, Belgium	01 – 05 February 2027
Brussels, Belgium	01 - 05 March 2027
Brussels, Belgium	05 – 09 April 2027
Brussels, Belgium	May 2027
Brussels, Belgium	10 - 14 May 2027
Brussels, Belgium	05 - 09 July 2027

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

Scenario-Based Civil Defence Course (Activity No 34)

Location	Dates
Ahrweiler, Germany	01 - 05 March 2027
Ahrweiler, Germany	11 - 15 October 2027

Course aim

This course aims at unfolding how the experiences and lessons from Russia's aggression against Ukraine can be used to further develop national operations and structures in civil defence. Although national structures in civil defence vary significantly across EU Member States, many of the lessons drawn from Ukraine are applicable to the different countries. The course provides officials at the strategic level responsible for civil defence with the necessary insights from Ukraine in order to draw robust, actionable conclusions that can be put to use in developing their own operations and structures that contribute to total defence.

Learning outcomes

Participants will understand how to integrate military and civil defence into total defence structures, the legal framework and core humanitarian principles which underpin any operation, and threats to and posed by new technologies, in particular AI, robotics and drones, in the context of civil defence. They will also understand the interconnected nature of security threats and the EU's multi-hazard approach, especially in regard to hybrid attacks and climate-related risks.

Participants will be able to assess complex interconnected risks, utilising foresight, cross-sectoral planning and multi-hazard frameworks to improve the readiness and resilience of civil defence-related national structures, and to critically assess, review and develop concrete proposals to improve their own national operations and structures in civil defence based on lessons learned from Ukraine. Applying knowledge of the Climate and Defence Nexus will further enhance the readiness and resilience of their own national operations and structures.

Participants will critically evaluate their own national operations and structures in civil defence, recommend adaptations based on lessons learned from Ukraine, and contribute to cooperation among civil defence stakeholders in the EU and towards Ukraine.

Target audience

Senior and mid-level officials from the European Union (EU) entities and EU Member States' ministries and agencies responsible for civil crisis management in a defence environment (Civil Defence, Emergency Services, Military). Priority will be given to decision makers in Civil Defence.

Course open to

- EU Member States / EU Institutions, Bodies and Agencies
- NATO countries

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

Location: Paris, France
Dates: March 2027

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: 21 - 25 September 2026

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: Brussels, Belgium
Dates: December 2026

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: Brussels, Belgium
Dates: Spring 2027

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: Bucharest, Romania
Dates: 13 – 16 July 2027

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
- Participants from Academia and the international humanitarian community
- Third countries and international organisations

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

Location	Dates
Nicosia, Cyprus	21 – 25 September 2026
Soave, Italy	12 – 16 October 2026
Lisbon, Portugal	12 – 16 October 2026
Lubeck, Germany	14 – 18 December 2026
Lubeck, Germany	25 – 29 January 2027
Paris, France	08 – 12 February 2027
Gotenica, Slovenia	07 – 12 March 2027
Lubeck, Germany	19 – 23 April 2027
Lisbon, Portugal	May 2027
Lubeck, Germany	21 – 25 June 2027
Soave, Italy	28 June – 02 July 2027

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	10 - 11 December 2026
Lubeck, Germany	15 - 16 April 2027
Lubeck, Germany	17 - 18 June 2027

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	Dates
Brussels, Belgium	22 – 26 March 2027
Thessaloniki, Greece	24 – 28 May 2027
Stockholm, Sweden	05 – 09 July 2027

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

The Climate-Environment-Security and Defence Nexus (Activity No 52)

Location: Sofia, Bulgaria
Dates: 19 – 22 April 2027

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, emphasising 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	Dates
Bucharest, Romania	21 – 23 September 2026
Madrid, Spain	21 – 23 September 2026
Rome, Italy	16 – 18 March 2027

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

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

Location	Dates
Boeblingen, Germany	12 – 23 October 2026
Larnaca, Cyprus	Spring 2027

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: Thessaloniki, Greece
Dates: 12 - 16 April 2027

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
- Candidate Countries
- Personnel seconded from third countries to CSDP missions

Energy Security (Activity No 59)

Location: Brussels, Belgium
Dates: 10 - 12 November 2026

Course aim

The course provides a thorough understanding of Energy Security as a concept, its overarching principles and objectives predominantly within the EU Integrated approach. It aims at enhancing participants' understanding of relevant frameworks, current energy developments and vulnerabilities related to the EU's energy security agenda and the EU's approach to the climate-energy-defence nexus.

Learning outcomes

By the end of the course, participants will gain insights into EU strategies, such as the European Green Deal and REPowerEU, and learn to identify vulnerabilities in energy systems, including cyber and geopolitical risks. The course emphasises analysing the integration of renewable energy and sustainable fuels into crisis management, while highlighting the link between climate and energy security. Participants will develop strategic approaches to prevent and respond to disruptions, utilising risk assessment tools and scenario planning. By examining past energy crises and fostering international cooperation, attendees will improve their ability to coordinate crisis responses and design resilient energy strategies. The course also aims to critically evaluate EU mechanisms in addressing these challenges, ultimately equipping participants with the skills to secure energy infrastructure against hybrid and environmental threats.

Target audience

Participants should be involved in the planning, implementation, or management of CSDP missions and operations, or EU Commission projects. Priority is given to personnel from EU Member States engaged in energy security, climate resilience, and sustainability policy development and implementation at national or EU levels, including agencies like EEAS/EUMS and various DGs (e.g., ECHO, CLIMA, ENV, NEAR, INTPA), and EU Delegations. Additionally, it prioritises individuals involved in climate and environmental mainstreaming, as well as education and training experts, faculty advisers, professors, consultants, and analysts.

Course open to

- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations
- Members of Non-Governmental Organisations

Reflective Leadership in Complex Environments (Activity No 62)

Location	Dates
Lubeck, Germany	19 – 23 October 2026
Brussels, Belgium	11 – 15 January 2027
Lubeck, Germany	01 – 05 May 2027

Course aim

The course is designed to give experienced leadership staff room to reflect on their own leadership experiences and develop their leadership skills further from this stage.

Learning outcomes

By the end of this course, participants will be able to discuss various leadership concepts and styles, explore the role of perceptions in leadership, and analyse motivation theories to understand their impact on team performance. They will explain the value of diversity within teams and examine how personal and cultural values influence leadership in multicultural settings, while also identifying the benefits of coaching in mission environments. Participants will develop practical skills to reflect critically on leadership within a CSDP (Common Security and Defence Policy) context, apply dialogue tools effectively, and assess the origins of their own leadership behaviours. They will learn to use motivation techniques, build, work in, and lead diverse and multicultural teams, and employ cross-cultural and gender-responsive communication methods. Additionally, they will foster team resilience, empower and motivate team members, and manage relationships appropriately in diverse environments. Learners will also demonstrate the importance of cooperation and implement self-care routines to maintain personal energy and well-being.

Finally, participants will perform with integrity, upholding EU values and interests while respecting host nations, develop a personal leadership vision, and create and implement a shared team vision. They will also cultivate a positive feedback culture to enhance team cohesion and performance.

Target audience

Participants should have own leadership experiences in an international, multicultural context, e.g. EU CSDP mission/operation or an international organisation. The course addresses mid to senior management with civilian, police or military background.

Course open to

- EU member States / Institutions
- Candidate countries
- Third countries and international organisations

Senior Strategic Course (Activity No 64) – Modular course

Location	Dates
Brussels, Belgium	08 – 10 February 2027
Berlin, Germany	Spring 2027
Brussels, Belgium	March 2027

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 horisontal 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

Diplomatic Skills for Peace, Security and Defence (Activity No 67)

Location: Timisoara, Romania
Dates: 10 _ 13 May 2027

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
- Third countries and international organisations

Cultural Heritage Protection Course (Activity No 68)

Location: Rome, Italy
Dates: 22 - 26 February 2027

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	Dates
Lisbon, Portugal	28 September – 02 October 2026
Brussels, Belgium	23 – 25 November 2026

Course aim

The Advanced Diplomacy Course for Peace, 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

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

Location: Kilkis, Greece
Dates: 26-30 October 2026

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
- Members of Non-Governmental Organisations

European gendarmerie forces in crisis management operations (Activity No 75)

Location: Vicenza, Italy
Dates: 28 September - 02 October 2026

Course aim

The course aims to provide participants with an in-depth understanding of the European Gendarmerie Force (EUROGENDFOR), an international organisation established by the Treaty of Velsen in 2007, consisting of Gendarmerie-type forces from EU Member States. It will highlight the added value and role of these forces in crisis management operations. The course covers EUROGENDFOR's police functions under both civilian and military command, across all crisis management phases. It will explore EUROGENDFOR doctrine, decision-making, leadership, and capabilities, focusing on collaboration and interoperability with agencies and international partners such as the EU, UN, NATO, and OSCE.

Learning outcomes

The learning outcomes of the course focus on providing participants with a comprehensive understanding of the European Gendarmerie Force (EUROGENDFOR) and its operations. Participants will analyse the organisational structure, decision-making processes, and the unique value of Gendarmerie-type forces globally. They will examine EUROGENDFOR's role in crisis management, focusing on interoperability with international partners. The course covers conflict analysis, prevention, management, and post-conflict stabilisation, preparing participants for future roles within EUROGENDFOR. It emphasises applying crisis management doctrine, coordinating peacekeeping efforts, and fostering scalability in operations. Attention is given to integrating gender policies, understanding contemporary conflict challenges, and countering hybrid and cyber threats, illustrating EUROGENDFOR's adaptability in dynamic scenarios.

Target audience

Mid and senior-level experts (civilian and military staff) from EUROGENDFOR Member States, EU countries and Institutions intended to work or working in areas related to crisis management operations. Eventually, representatives from non-EU Member States, especially from EU candidate countries, could be invited.

Course open to

- EU Member States - institutions
- EUROGENDFOR member states
- EU Candidate Countries

Foreign Information Manipulation and Interference (Activity No 76)

Location: Brussels, Belgium
Dates: 21 - 22 October 2026

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
- International Organisations

Advanced Research into Hybrid Threats (Activity No 77)

Location: Brussels, Belgium
Dates: 20 - 23 October 2026

Course aim

Advanced Research into Hybrid Threats is an interactive course that examines the intersection of information manipulation tactics and cyber-attacks. It enhances experts' and practitioners' understanding of the tools and strategies used by hostile actors to spread disinformation and conduct covert operations at the EU level. The course also explores coercive and subversive strategies shaping geopolitical dynamics, particularly in the context of ongoing conflicts. Through lectures, debates, problem-solving exercises, and scenario-based activities, participants will analyse the impact of hybrid threats and anticipate future trends.

Learning outcomes

By the end of this course, participants will understand the key challenges to EU security posed by the evolving landscape of hybrid threats. They will identify the core elements of the EU's integrated approach and analyse how information manipulation and cyberattacks intersect, developing the ability to conduct shared threat assessments. Learners will also comprehend the principles of the EU Hybrid Toolbox, including preventive, cooperative, stability-building, restrictive, and support measures. Participants will acquire practical skills to extract lessons learned in response strategies and design resilience mechanisms. They will mitigate risks using available resources while applying critical thinking skills through scenario-based exercises. Finally, learners will utilise tools to assess hybrid threat patterns, disinformation, and cyberattacks, deploy cyber-diplomacy instruments and interference countermeasures, and translate knowledge into solutions for implementation. This course equips participants to effectively counter hybrid threats within an EU framework.

Target audience

Participants should be mid-ranking to senior officials, doctoral researchers, academics, and practitioners whose work is related to hybrid threats (ministries of foreign affairs, defence, intelligence, internal affairs). Priority is given to personnel from EU Member States and institutions involved in policy development, governance, and strategic security initiatives.

Course open to

- ESDC Doctoral School on CSDP fellows
- EU member States / Institutions
- Candidate Countries

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

Location: Thessaloniki, Greece
Dates: 05 - 09 October 2026

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
- Candidate Countries
- Third Countries/ Organisations

Security in the Black Sea region (Activity No 79)

Location: Bucharest, Romania
Dates: 21 - 23 April 2027

Course aim

The security in the Black Sea Region. Shared Challenges, Sustainable Future program is an interactive and practical training program, ideal for promising young leaders and junior managers in security, diplomacy and intelligence. This advanced professional course examines the evolving security dynamics in the Black Sea Region against the backdrop of the war in Ukraine and shifting geopolitical alignments. The course provides a comprehensive analysis of emerging security challenges, regional power dynamics, and strategies for building sustainable security frameworks in this critical area. The course is also designed to enhance analytic and forward thinking skills, as well as joint leadership capacities focusing on the challenges specific to security and intelligence organisations transformation in the 21st century.

Learning outcomes

The learning outcomes focus on equipping participants with a comprehensive understanding of the EU's strategic environment, particularly concerning European security in relation to the Eastern Neighbourhood. Participants will enhance their analytical and strategic planning capabilities to identify transformation processes in regional security and economic resilience. They will gain insights into the interplay between security, intelligence, and diplomatic skills, improving their understanding of regional security dynamics. Participants will learn to employ practical tools for addressing security challenges and developing strategic responses, optimising crisis management skills, and translating academic knowledge into actionable solutions within security, intelligence, and foreign affairs organisations.

Target audience

Mid-level professionals from EU Member States and States from Eastern Neighbourhood involved in Common Security and Defence Policy (CSDP) implementation and international organisations. Officials from ministries of foreign affairs, defence, intelligence, and internal affairs. Practitioners with management and leadership experience in security and intelligence from MS authorities Representatives from relevant EU Institutions and Agencies.

Course open to

- EU Member States - institutions
- EU candidate countries
- States from Eastern Partnership (EAP countries)

Artificial Intelligence, Security and Cooperation in the EU (Activity No 80)

Location	Dates
Larnaca, Cyprus	23 - 27 November 2026
Thessaloniki, Greece	14 – 18 June 2027

Course aim

This course aims to provide a comprehensive overview of the role of Artificial Intelligence (AI) in European security and cooperation, focusing on its strategic implications, the most prominent threats, ethical considerations, and operational applications. Participants will explore AI's impact on national security, cybersecurity, hybrid threats, disinformation, diplomacy, and gender-related security issues.

Learning outcomes

Participants will learn how Artificial Intelligence (AI) is shaping the EU's strategic environment, security policies, and defence strategies. They will explore AI's role in addressing hybrid threats, cybersecurity, predictive analytics, and disinformation, including its impact on democratic processes. The course will also cover AI's implications in diplomacy, international cooperation, and gender-based security issues. Participants will examine the ethical and governance dimensions of AI in security, learn to apply scenario-based assessments, and develop strategies to counter AI-enabled disinformation. They will also gain skills in contributing to AI-driven policy frameworks, fostering interdisciplinary collaboration, and integrating AI into EU security and defence research and policymaking.

Target audience

Participants should be mid-ranking to senior officials, doctoral researchers, academics, and practitioners whose work intersects with or is expected to be impacted by the integration of AI in security, defence, and cooperation within the EU. Priority is given to personnel from EU Member States and institutions involved in policy development, governance, and strategic security initiatives, who would benefit from acquiring the necessary knowledge to effectively manage and adapt to these emerging developments.

Course open to

- ESDC Doctoral School on CSDP Fellows
- EU Member States - institutions
- EU candidate countries
- Third countries and international organisations

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

Location	Dates
Brussels, Belgium	Spring 2027
In-mission training	

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

PsyOps for Peace, Security and Defence (Activity No 82)

Location: Pordenone, Italy
Dates: 28 September – 02 October 2026

Course aim

The course aims to provide an enhanced learning environment that promotes understanding and the importance of PSYOPS for Peace, Security and Defence in protecting EU interests and in enhancing CSDP mission capabilities. It provides the most updated illustration of the different levels and applications of PSYOPS, also outlining the links between PSYOPS and CSDP missions. By focusing on human Neuro-Physio-Psycho-Social elements and vulnerabilities, along with the Cognitive Domain, the course provides concrete elements to identify and map foreign PSYOPS actions targeting EU interests and CSDP missions, also using case studies, distinguishing PSYOPS specific features, peculiarities, technical elements and PSYOPS operations, using social media and in the digital environment.

Learning outcomes

This course equips learners with the knowledge and skills to understand and counter psychological operations (PSYOPS) targeting the European Union and its Common Security and Defence Policy (CSDP) missions. It covers the classification, applications, and distinctive features of PSYOPS, including their technical elements and use in digital and social media environments. Learners will explore the cognitive vulnerabilities of individuals and societies, assess emerging security threats, and analyse real-world PSYOPS campaigns. The course also focuses on developing analytical frameworks, operational strategies, and tailored countermeasures to enhance EU policy, defence capabilities, and societal resilience against PSYOPS threats.

Target audience

The Course is open to mid-ranking/senior officers and experts (civilian, military, diplomats and police) from EU Member States and EU Institutions/agencies working in the area of strategic affairs, the information environment, intelligence and decision-making processes, as well as personnel deployed on CSDP missions in an operational or leadership position. It is also open to practitioners with expertise employed in EU Member State authorities and from related EU institutions and agencies.

Course open to

- EU Member States - Institutions and agencies and EU missions
- EU CSDP mission personnel

Mission Medical Security course (Activity No 83)

Location: Stockholm/Rosersberg, Sweden
Dates: Spring 2027

Course aim

This course targets security personnel with minimal medical training, focusing on essential objectives: it aims in equipping participants with skills to deliver basic lifesaving care to prevent fatalities and minimise further complications, enabling them to independently manage care until professional medical services are available, and preparing them to effectively contribute to a Mass Casualty Incident (MCI) response team.

Learning outcomes

This course equips security personnel with essential first responder skills, focusing on medical emergency management. Participants will learn the role and responsibilities associated with first response, including handling trauma with an understanding of gender-specific outcomes and ensuring the proper use of body armor. The course covers protocols for exposure to bodily fluids, recognising and managing massive bleeding, and utilising airway adjuncts and tourniquets. It addresses the principles of wound management, the significance of hypothermia prevention, vital sign monitoring, casualty documentation and handover, and strategies for rapid evacuation and triage in mass casualty incidents.

The course also emphasises practical skills, offering hands-on training in scene safety, bleeding control, airway management, and casualty assessment. Participants will practice using CPR techniques, Automated External Defibrillators (AEDs), and casualty movement strategies. The course will also prepare participants to stabilise fractures, manage severe injuries such as amputations, and operate within a Casualty Collection Point (CCP). These components are designed to enhance the effectiveness of security personnel in medical emergencies, ensuring they are prepared to act swiftly and competently.

Target audience

The Course is open to Seconded and international contracted Security staff who have been selected to be deployed to a CSDP Mission/Operation.

Course open to

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

Women, Peace and Security (Activity No 84)

Location: Thessaloniki, Greece
Dates: 05 – 09 July 2027

Course aim

The overall aim of the course is to provide specific knowledge about the way in which wars and crises affect women, both as agents of peace and post-conflict reconstruction and as victims of war-related gender violence. At a time of growing conflict and violent extremism such a course is all the most important for the EU's internal and external policies. Another key objective of the course is to render participants familiar with EU policies that support the four pillars of the Women, Peace and Security (WPS) agenda: the protection of women and girls, men and boys; conflict prevention policies; equal participation of women in the peace and security policies of the EU and other organisations; and the provision of relief and recovery to victims of gender violence, especially in the context of war and crises caused by violent extremism. The course is geared towards military and police officials, civilians and other decision makers in the field. For the above reasons, the course also aims to provide participants with the appropriate skills not only to optimise EU policies and common security and defence policy (CSDP) mechanisms serving the policy framework related to the implementation of UNSCR 1325 and its supporting documents, but also to be able to harness other EU policies promoting WPS at European and global level.

Learning outcomes

By the end of this course, participants will understand the geopolitical context of EU CSDP/CFSP operations, key strategic documents (EUGS, Strategic Compass), and institutional roles in peace and security. They will explore the WPS agenda, capability development, and CSDP decision-making processes, including prevention, response, and links to EU security policies.
Learners will assess EU interests in the Western Balkans and MENA, apply gender analysis in crisis management, and evaluate cooperation with international partners (UN, NATO, OSCE). They will develop skills to engage EU institutions in WPS-aligned capability development, implement UNSCR 1325, and design gender-sensitive crisis responses.
Finally, participants will critically evaluate the EU's role in promoting WPS globally, assess the impact of EU diplomacy and CSDP mechanisms, and analyse strategic documents and partnerships (e.g., NATO) to advance women's empowerment in conflict and post-conflict settings. This course empowers professionals to integrate WPS principles into EU external actions.

Target audience

Participants should be selected from EU, UN and other international experts and decision makers of the armed forces (at all levels), policy officers from civil society organisations (academics and heads of thematic sections and above), political institutions, and civilian administrations (at all levels), with

relevant experience in crisis management, gender governance, peacebuilding, and security sector reform.

Course open to

- EU Member States/institutions
- Candidate countries
- Third countries
- International organisations

Strategic Leadership in Security and Intelligence Culture (Activity No 85)

Location: Bucharest, Romania
Dates: 21 – 25 September 2026

Course aim

The course is a hands-on, interactive training program designed for young leaders and junior managers in security, diplomacy, and intelligence. It aims to strengthen leadership and management skills by addressing the unique challenges of transforming intelligence organisations in the 21st century. Participants will learn practical techniques to lead teams and support institutional change, guided by expert academics, industry professionals, and senior intelligence leaders. The course uses a mix of formal and non-formal education, experiential learning, coaching, and mentoring. It culminates in a practical exercise where participants apply their learning to tackle real-world transformation challenges using future scenarios and predictive approaches.

Learning outcomes

Participants will learn to navigate the EU's strategic security environment by understanding key threats, challenges, and drivers of change that impact managerial roles in security and intelligence organisations. They will explore transformation processes, leadership strategies, and the integration of security, intelligence, and diplomatic competencies to support human-centric, adaptive organisations. The course emphasises practical application of leadership, coaching, mentoring, and critical thinking skills, while analysing their impact on organisational dynamics. Participants will use tools to assess managerial challenges, develop strategic responses, and foster autonomy, collaboration, and mutual respect. Ultimately, they will learn to translate academic insights into practical solutions for real-world application in security, intelligence, and foreign affairs contexts.

Target audience

Participants should be mid-level professionals in MSs involved in the implementation of CSDP (ministries of foreign affairs, defence, intelligence, internal affairs). Practitioners with management and leadership knowledge in security and intelligence from the authorities of the MSs and from related EU Institutions and Agencies could be as well invited to join the course. Depending on the design of the course, senior decision makers, Political Advisors to the Head of Mission/Commander could join the training, especially when the experts with field experience are invited to contribute with their expertise.

Course open to

- EU Member States – Institutions

Medical Advisor (Activity No 86)

Location: Stockholm, Sweden
Dates: 08 - 13 November 2026

Course aim

The course -Introduction to Medical Advisory and Duty of Care for Healthcare Providers in Civilian CSDP Missions aims at introducing course participants to the role of a medical advisor in Civilian CSDP Mission, giving participants a comprehensive understanding of the tasks and responsibilities. The course will enable participants to learn and develop the specialised skills and knowledge necessary to perform and/or support the role of a medical adviser efficiently and effectively in Civilian CSDP missions.

Learning outcomes

By the end of this course, participants will demonstrate a comprehensive understanding of the roles and responsibilities linked to the Medical Adviser position in CSDP missions, including key interactions with related posts. They will anticipate challenges in the role and apply effective problem-solving skills to uphold duty of care while supporting mission mandate delivery. Learners will also assess and address medical needs in diverse, resource-constrained, and high-pressure environments. Participants will develop practical skills to execute common mission medical procedures, such as MEDEVAC and sickness/absence management, and communicate and collaborate effectively within multidisciplinary teams and with external stakeholders. They will also promote health and disease prevention initiatives across mission areas while ensuring compliance with legal and professional duty-of-care obligations. Finally, learners will develop and implement medical contingency plans for CSDP missions and provide strategic medical advice to leadership teams, balancing medical risks, operational constraints, and mission objectives with confidence and competence. This course prepares Medical Advisers to deliver effective, mission-aligned healthcare support in complex operational settings.

Target audience

Medical professionals, including physicians and registered nurses, who are either already deployed or interested in deploying on medical teams on Civilian CSDP missions.

Course open to

- EU Member States / Institutions
- Candidate countries
- Third countries and International Organisations

Crisis Management in Multilateral Frameworks (Activity No 87)

Location: Sofia, Bulgaria
Dates: 18 - 21 May 2027

Course aim

The course aims to develop knowledge and understanding about the concepts and practice of crisis management in multilateral crisis diplomacy contexts, to reiterate the indispensable role of major IGOs in this process (from political/civilian and military perspectives). It also aims to analyse the crisis management in the context of the EU integrated approach to crisis management.

Learning outcomes

In this course, participants will gain a comprehensive understanding of the integrated approach to crisis management and multilateral crisis diplomacy, exploring key conceptual frameworks, practices, and the roles of major international actors such as the EU, NATO, UN, and OSCE across the conflict cycle. They will examine the impact of gender issues, hybrid and cyber threats, and the role of strategic communication (Stratcom) in crisis contexts. The course emphasises analysis of both inter- and intra-state crises, highlighting the tools, principles, and cooperation between military and civilian/political-diplomatic actors, including IGOs and NGOs. Participants will learn to plan and conduct peace operations, assess stakeholder roles, develop integrated crisis strategies, and evaluate how the evolving global security environment shapes crisis management and diplomacy.

Target audience

Participants should be preferably 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 European Commission.
Priority is given to the personnel from EU Member States. However, the course is also open to participants from third countries, in particular those working in major IGOs, with focus on crisis management and multilateral crisis diplomacy contexts.

Course open to

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

Challenges of European Cybersecurity (Activity No 200)

Location	Dates
Online	21 – 25 September 2026

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

Critical Infrastructure in the Context of Digitization (Activity No 202)

Location: Vienna, Austria
Dates: 21 – 22 October 2026

Course aim

The aim of this course is to enable participants to understand the current context of Critical Infrastructure Protection (CIP) strategies within the EU cyber ecosystem. It will equip them to analyse the regional impact of CIP and apply these strategies in the face of continuous digitisation. Participants will learn to identify, evaluate, and mitigate cyber risks, threats, and attack vectors targeting critical infrastructures (CI). Additionally, the course will empower learners to move beyond traditional CIP approaches by leveraging new technologies within the evolving cyber ecosystem.

Learning outcomes

By the end of this course, participants will be able to identify the EU institutions and agencies involved in cybersecurity and cyber defence, understanding their respective roles, while recognising the key challenges of cybersecurity at the European level. They will define core concepts related to Critical Infrastructures (CI) and associated Operational Technologies (OT), summarise strategies for protecting CIs, and identify best practices, standards, and emerging threats targeting these infrastructures. Learners will also analyse attack vectors affecting CI protection and explore mitigation, response, and recovery measures to counter cyber threats effectively. Participants will have developed the skills to assess risk management frameworks at national and regional levels, classify technical and organisational tools for CI protection, and evaluate the potential impacts of cyber threats on CI security and policies. They will categorise critical risks in information security management and apply risk management techniques to enhance CI resilience. Additionally, learners will be able to assess the potential impact of cyber threats and incidents on CIs, policies, and systems, and determine appropriate countermeasures to strengthen protection. This course will provide participants with the analytical and practical capabilities needed to safeguard critical infrastructures in a dynamic cyber threat environment.

Target audience

Participants should be mid-ranking to senior officials, dealing with technical and operational aspects in the field of cyber security related to Critical Infrastructures, from EU MSs, EU Institutions and Agencies. Course participants must be available during the entire residential course and should be ready participate with their specific field of expertise and experience.

Course open to

- EU member States, Institutions and Agencies
- Candidate Countries

CSIRT Fundamentals (Activity No 204)

Location: Nicosia, Cyprus

Dates: 22 – 25 September 2026

Course aim

This course will prepare participants to understand how to organise and which capabilities and procedures need to be developed, implemented and provided by a Computer Security Incident Response Team. The educational material combines the theoretical framework and innovative interactive e-learning methods and provides the materials to cover the fundamental knowledge required for cybersecurity incident monitoring and response, forensics analysis, an introduction to risk management and cyber threat intelligence. Furthermore, this course will allow cyber security experts to exchange views and share best practices on cyber-related topics by improving their knowledge, skills and competencies.

Learning outcomes

By the end of this course, participants will understand the roles of EU institutions and agencies in cybersecurity and cyber defence, recognise the challenges posed by the modern information society, and identify emerging cyber threats, including hybrid operations. They will learn incident handling standards and CSIRT structures, while developing practical skills to analyse threat intelligence, assess security incidents, and classify cybersecurity tools. Participants will also apply malware analysis, forensic techniques, and risk management, and report findings effectively. Finally, they will evaluate the impact of cyber threats on policies and systems and select appropriate countermeasures, gaining both theoretical and practical expertise to address cybersecurity challenges in Europe.

Target audience

The course is aimed at personnel working in the field of national and international armament cooperation who need to gain knowledge of cooperative acquisition and project management. It also supports experts looking to take on leadership positions in the wider defence area.

Course open to

- EU Member States - institutions

Cybersecurity Risk Management (Activity No 205)

Location: Brussels, Belgium
Dates: 15 - 17 February 2027

Course aim

The aim of this course it that participants will understand cybersecurity risk management principles and frameworks, conduct comprehensive risk assessments to identify threats and vulnerabilities, and implement mitigation strategies to bolster organisational resilience. They will ensure compliance with cybersecurity standards and regulations, enhance decision-making for policies and investments, and bridge communication between technical teams and leadership to promote a proactive risk-aware culture.

Learning outcomes

By the end of this course, participants will be able to define cybersecurity risk management principles, including risk identification, assessment, mitigation, and monitoring, and analyse threats and vulnerabilities affecting organisational assets. They will explain the role of risk management in achieving business resilience and describe key framework components, such as risk assessment, treatment, and monitoring, while applying standards like ISO 27001, NIST, and GDPR. Learners will gain skills to conduct risk assessments, develop and implement risk management plans, and monitor risks to ensure ongoing effectiveness. They will communicate risk insights to stakeholders and design frameworks aligned with organisational goals.
Finally, participants will take ownership of risk management processes, make informed mitigation decisions, and collaborate with internal and external partners to integrate cybersecurity into broader risk strategies. This course prepares professionals to build and maintain a resilient cybersecurity risk management programme.

Target audience

Participants should be IT and cybersecurity professionals who specialise in risk assessment and mitigation strategies, managers and team leaders overseeing cybersecurity initiatives or projects, decision-makers involved in policy development and implementation for cybersecurity, professionals involved in compliance and regulatory roles within the realm of cybersecurity.

Course open to

- EU Member States / EU institutions, bodies and agencies
- Candidate countries

Cyber Diplomacy Advanced (Activity No 207b)

Location: Brussels, Belgium
Dates: 19 - 21 January 2027

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 Advanced (Activity No 208b)

Location: Nicosia, Cyprus
Dates: 05 - 09 October 2026

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: May 2027

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, Poland
Dates: Spring 2027

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

Data Governance (Activity No 214)

Location: Brussels, Belgium
Dates: 20 – 23 September 2026

Course aim

This course presents the mechanism for effective data governance and outlines the seven critical factors for effective strategy execution: strategy, shared values, structure, systems, style, staff and skills. Furthermore, this course will allow mid-ranking to senior officials to exchange their views and share best practices on data governance in connection with cyber-related topics, thus improving their knowledge, skills and competencies. By the end of this course, participants will be able to create and implement a data governance strategy, drawing on their enhanced knowledge and understanding of the relevant principles.

Learning outcomes

By the end of the course, participants will be able to define the basic principles of data governance and list the seven critical factors for effective strategy execution, including strategy, shared values, structure, systems, style, staff, and skills. They will identify the key organisational roles involved in the planning, development, implementation, monitoring, and evaluation of data governance—particularly in relation to cybersecurity under international law—while also recognising the nature of internal and external cyber threats that impact data governance. Learners will further identify technical, organisational, and operational controls to mitigate associated risks. In terms of practical skills, participants will classify cyber incidents affecting data governance, assess the impact of cyber threats on governance frameworks, and categorise the consequences of such incidents on an organisation's data integrity. Finally, they will evaluate the potential impacts of cyber threats on data governance and select appropriate mitigation measures to safeguard organisational data effectively.

Target audience

Participants should be mid-ranking to senior officials employed in the field of cybersecurity from MS or EU institutions, bodies and agencies. Course participants must be available for the duration of the course. Participants are expected, based on their experience and expertise, to actively engage and participate during the course.

Course open to

- EU Member States and EU institutions

Cyber Range - Cybersecurity in Practice (Activity No 215)

Location	Dates
Warsaw, Poland	06 - 08 October 2026
Varna, Bulgaria	12 – 14 January 2027
Warsaw, Poland	Spring 2027

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, Belgium
Dates: 22 - 24 February 2027

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

Countering Disinformation with Applied OSINT Techniques (Activity No 218)

Location: Athens, Greece
Dates: 02 – 13 November 2026

Course aim

This course is intended to strengthen the establishment of the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC and widen the scope of its activities by addressing basic technical and strategic/operational-level training in countering disinformation. This course aims to provide knowledge, skills and competencies via structured methods of applying advanced OSINT techniques, lab exercises and practice in various scenarios. In addition, the course aims to provide a forum for the exchange of knowledge and best practices among personnel tasked to counter disinformation campaigns and allow the participants to exchange their views and share best practices on related topics of countering disinformation. By the end of this course the participants will be able to be more effective in large scale collection from open sources with the use of structured analytic techniques and create more accurate estimations in order to provide accurate intelligence on countering disinformation.

Learning outcomes

By the end of this course, participants will be able to define disinformation and misinformation and explain key concepts within the EU Cyber Security Strategy. They will analyse how social media platforms are exploited to spread disinformation, identify its origins, and understand how these platforms amplify its impact on audiences. Learners will also examine the intent and capabilities of disinformation actors and describe the tactics, techniques, and procedures used to manipulate information at scale. Participants will develop practical skills to conduct fact-checking and establish validation principles, analyse suspicious accounts linked to troll or bot networks, and perform in-depth social network analysis to map interactions between accounts. They will use visualisation tools to investigate troll networks on platforms like Twitter, applying techniques such as ego-centric network analysis and node isolation, and set up data collection environments for network analysis. Finally, learners will source existing datasets from troll networks and perform basic analysis, select optimal open-source intelligence (OSINT) collection methods, and develop advanced techniques for real-time monitoring of disinformation networks. This course equips participants with the analytical and technical skills needed to detect, analyse, and counter coordinated disinformation campaigns.

Target audience

Participants should be officials dealing with aspects in the field of intelligence, security and cyber security from Member States (MS), EU Institutions and Agencies.
Course participants must be available during the entire course and should be ready participate with

their specific field of expertise and experience.

Course open to

- EU Member States / EU Institutions Bodies and Agencies

Chief Information Security Officer (CISO) (Activity No 220)

Location: Nicosia, Cyprus
Dates: 07 – 12 December 2026

Course aim

The aim of the course is to prepare the participants to design, apply and manage the implementation of cybersecurity policies across the organisation. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on the implementation of cybersecurity strategies in organisations by improving their knowledge, skills and competencies.

Learning outcomes

In this course, participants will learn to understand and implement key aspects of cybersecurity, including policies, procedures, resource and risk management frameworks, and cyber-attack prevention plans. They will develop the ability to apply and supervise cybersecurity standards, certifications, and methodologies, as well as design, monitor, and improve an Information Security Management System (ISMS). The course also equips learners to review security documentation, ensure compliance with security objectives, and lead the development of cybersecurity strategies and plans. Additionally, participants will strengthen their communication and coordination skills with stakeholders and manage continuous capacity building within their organisations.

Target audience

Participants should be mid-ranking to senior military or civilian officials dealing with cybersecurity management tasks from EU Institutions, Bodies and Agencies as well as EU Member States.

Course open to

- EU Member States - institutions

Practical Strategies for Mitigating AI-Driven Cyber Attacks (Activity No 225)

Location: Constanta, Romania
Dates: 17 - 19 March 2027

Course aim

This course is an essential three-day programme that presents the key policy drivers, cutting-edge technological tools, and strategies for identifying, mitigating, and managing AI-driven cyber threats across critical industries and infrastructures. It is meticulously designed to equip participants with in-depth understanding and practical skills in addressing AI-driven cybersecurity challenges, particularly within the EU context. Through a blend of expert-led sessions, interactive workshops, and real-world case studies, the course aims to enhance participants' ability to identify, analyse, and respond to the evolving threats posed by AI in cyber operations.

Learning outcomes

By the end of this course, participants will possess essential practical knowledge and skills to effectively address AI-driven cybersecurity challenges at both policy and technical levels, enabling them to contribute to a secure and resilient digital environment in a rapidly advancing and interconnected world.

They will also gain a comprehensive understanding of the EU's regulatory, policy, and investment frameworks for mitigating AI-driven cyber threats, along with key concepts and entities involved at both national and EU levels. They will learn to identify, analyse, and manage AI-driven threats strategically, apply relevant cybersecurity policies and regulations, and use advanced technological tools and best practices to enhance security measures. The course emphasises ethical conduct, responsible decision-making, and stakeholder collaboration across critical sectors. Through practical simulations, learners will also develop crisis management and strategic response skills, balancing autonomy with accountability in complex cybersecurity environments

Target audience

Participants should be officials dealing with aspects of AI and cybersecurity from the EU Member States (MS) or EU institutions and agencies.

Course open to

- EU Member States - institutions

Advanced Cyber Range Training for Maritime Cyber Resilience (Activity No 226)

Location: Constanta, Romania
Dates: 09 - 12 February 2027

Course aim

This course is an intensive four-day programme designed to provide participants with a comprehensive understanding of the key policy frameworks, advanced technological tools, and practical strategies for enhancing maritime cybersecurity resilience. Tailored specifically to address the unique challenges of the maritime sector, the course focuses on building skills to identify, mitigate, and manage cyber threats targeting critical maritime infrastructures and systems. Through expert-led sessions, interactive workshops, and hands-on exercises in advanced cyber range environments, participants will gain practical experience in threat modelling, incident response, and resilience planning for maritime operations.

Learning outcomes

By the end of the course, participants will be equipped with the technical expertise and strategic insights necessary to strengthen maritime cybersecurity frameworks, ensuring robust defences and resilient operations in an increasingly complex and interconnected digital landscape.
They will develop a thorough understanding of the EU's regulatory, policy, and investment frameworks aimed at enhancing maritime cybersecurity and resilience. They will learn to identify key national and EU entities involved in maritime cyber defence and grasp essential concepts and terminology related to maritime cybersecurity. The course covers advanced tools and best practices for detecting and managing cyber threats in maritime IT and operational technology systems, with a focus on strategic risk assessment and long-term resilience planning. Participants will apply relevant policies to ensure compliance, collaborate with diverse stakeholders, and use cyber range environments to strengthen defences. Through practical simulations, they will build decision-making skills for crisis management while emphasising ethical conduct, accountability, and responsible autonomy in complex maritime cybersecurity scenarios.

Target audience

Participants should be officials dealing with aspects of cybersecurity from the EU Member States (MS) or EU institutions and agencies.

Course open to

- EU Member States - institutions

Advanced EU Security and Intelligence Awareness (Activity No 227)

Location: Brussels, Belgium
Dates: 21 - 23 October 2026

Course aim

This course aims to deepen policy-level understanding of security and intelligence, tailored to the needs of EU and Member State officials. It explores key security threats from adversarial states and provides practical, preventive measures to counter them. Structured in three parts, the course first examines intelligence organisations and their practices, then outlines EU security departments and their guidelines, and finally focuses on applied strategies for prevention and response at both organisational and individual levels. Topics include intelligence structures, foreign interference, espionage, and cyber threats, as well as security roles in EU delegations and intelligence support for decision-making. Developed with EU security leaders and INTCEN, the course delivers actionable insights for professionals in EU intelligence and security.

Learning outcomes

By the end of this course, participants will understand the intelligence function and its structure within Europe, including FIMI tactics and resilience-building methods at individual and organisational levels. They will recognise defensive practices against espionage, counterintelligence, and cyber threats from adversarial states, while grasping EU legal security rules, data protection, and the roles of key institutions (Commission, Council, EEAS, Parliament). Learners will also explore security roles in EU delegations and missions, as well as SIAC's role in supporting decision-makers.
Participants will develop skills to identify threat-response best practices, detect risk patterns, and mitigate vulnerabilities using existing resources. They will differentiate between threats targeting EU institutions and apply tools to assess security risks, disinformation, and cyberattacks. This course prepares learners to enhance security and resilience in EU contexts.

Target audience

Representatives and officials of EU institutions involved in security and intelligence affairs (EU Officials and European Economic Area M.S. officials).
It is also open to other potential audiences who develop their training at the ESDC, as well as to officials from member states with a vocation to work in EU institutions or with their representatives.

Course open to

- ESDC Doctoral School on CSDP fellows
- EU member States /Institutions
- International Organisations

Advanced FIMI Analysis (Activity No 228)

Location: Brussels, Belgium
Dates: 24 - 27 November 2026

Course aim

The course aims at building resilience of CSDP missions and EU Member States against the FIMI threat, focusing on reinforcing the analytical capabilities of data analysts of the Rapid Alert System (RAS) network and relevant CSDP missions' personnel deployed in the field . The Course will address the different blocks of the FIMI analytical cycle, including advanced FIMI detection, analysis of Tactics, Techniques and Procedures (TTPs), data modelling and STIX encoding of FIMI investigations.

Learning outcomes

By the end of this course, participants will be able to integrate the EU's common framework and methodology to analyse Foreign Information Manipulation and Interference (FIMI). They will understand FIMI tactics, techniques, and procedures (TTPs), recognise the added value of data modelling and long-term analysis of FIMI incidents, and learn the STIX language for structured threat intelligence. Additionally, learners will encode FIMI data using OPEN CTI.

Participants will develop practical skills to apply scenario-based assessments in analysing FIMI TTPs, identify STIX objects within FIMI incidents, and practise OPEN CTI encoding for real-world applications.

Finally, learners will be able to develop a data-driven approach to FIMI analysis and collaborate effectively with analysts in the Rapid Alert System. This course equips participants with the technical and analytical expertise needed to detect, assess, and counter FIMI threats within an EU context.

Target audience

Priority participants are EU Member States Rapid Alert System (RAS) analysts and CSDP personnel addressing FIMI in their area of deployment (Mission Analytical Capability analysts, Information Analysts, Press and Public Information Officers, Political Advisers, and/or Mission Security Officers) with extensive knowledge of FIMI. Other participants should have completed an intermediate ESDC FIMI course and have preliminary FIMI analysis experience to be eligible for this course.

Course open to

- EU Member States /EU Institutions

Military Aviation CEMA Resilience (Activity No 230)

Location: Nicosia, Cyprus
Dates: Spring 2027

Course aim

The aim of the course is to inform participants on the risks posed to EU Military Aviation capabilities by the malign use of Cyberspace and the Electromagnetic Spectrum (EMS), and by non-intentional events affecting Cyberspace and the EMS as well as the mitigation actions that might enhance the resilience of Military Aviation capabilities to these types of Cyber and Electromagnetic Activities (CEMA) and events

The course will also, via involvement in Table-Top Exercises (TTXs), enable participants to assess key implications which they can then address in their future work related to Military Aviation capabilities.

Learning outcomes

By the end of this course, participants will understand the nature of digital technologies (including AI), their rapid evolution, and inherent cybersecurity vulnerabilities, as well as the electromagnetic spectrum (EMS) and techniques for electronic protection and countermeasures in military contexts. They will grasp cyberspace dependencies of military aviation capabilities, potential impacts of cyber and electronic attacks, and EU responses to cybersecurity and cyber defence challenges in CSDP missions. Learners will also examine malign cyber and electronic threats to military aviation, vulnerabilities they exploit, and current and future mitigation measures, while considering environmental risks and unintentional human actions that may disrupt operations. Additionally, they will explore how to identify and manage CEMA-triggered risks affecting military aviation.

Participants will develop skills to apply this knowledge in their work, recognising contested cyberspace and EMS environments, CEMA threats, and potential impacts on aviation capabilities. They will derive insights on malign CEMA, environmental risks, and human factors to inform procurement, employment, and logistical support of military aviation assets. Learners will also advise or lead teams in addressing these challenges and effectively communicate CEMA concepts to colleagues at all levels.

Finally, participants will reflect on the implications of technological change and CEMA vulnerabilities, evaluate evolving threats from state and non-state actors, and extract key insights from EU publications to inform mission planning, operational procedures, and decision-making. This course equips professionals to integrate cyber and electronic warfare awareness into military aviation operations and strategic planning.

Target audience

For military audiences, participants should be mid-rank military officers (of NATO grades OF-2 to OF-4), currently working (or will work in the future) in a CEMA generalist position in EU Institutions, EU Member State MOD, defence procurement agency, military HQ, or a Military Aviation unit, who:

(1) Support the planning or direction of Military Aviation operations or operational training
(2) Operate, or provides operational support services to Military Aviation capabilities
(3) Procure, or manages in-service logistical support to Military Aviation capabilities
(4) Develop policies, concepts, strategies or doctrine related to Military Aviation, or
(5) Design and/or deliver CEMA-related professional military education courses, or command post exercises.
For civilian audiences, participants should be personnel of similar seniority to the Military Audience, who are currently working (or will work in the future) in a CEMA generalist position in EU Institutions, EU Member, or in a Member State governmental body, with duties related to Military Aviation capabilities.

Course open to

- EU Member States / EU Institutions

AI in Cybersecurity: The new Frontier in Defence Strategies (Activity No 258)

Location: Rome, Italy
Dates: 27 - 29 October 2026

Course aim

This course offers a comprehensive exploration of how Artificial Intelligence is revolutionising the security and defence landscape. Participants will gain cutting-edge knowledge and skills to leverage AI in addressing emerging cyber threats, enhancing situational awareness, and automating incident response mechanisms. Beyond cybersecurity, the course delves into broader applications of AI in the governmental and public sectors. Participants will explore real-world scenarios and enterprise-level projects, such as using AI to optimise decision-making, enhance data-driven governance, and develop predictive models for crisis management and disaster relief. The programme also highlights innovative AI-driven solutions for improving citizen engagement through customer relationship models, such as chatbot implementations and smart public service delivery systems to better understand the needs of diverse communities. Additionally, the course emphasises the critical intersection of AI, cybersecurity, and 5G networks. With the rapid deployment of 5G technology enabling unprecedented connectivity and data flow, participants will learn how AI-powered applications can be utilised to safeguard critical infrastructure.

Learning outcomes

By the end of this course, participants will be able to design AI-driven cybersecurity strategies to counter emerging threats and apply AI solutions to protect critical infrastructure in key sectors. They will lead public-sector AI projects, enhancing decision-making and operational efficiency, and implement AI tools for crisis management and citizen engagement. Learners will develop integrated AI-cybersecurity frameworks for Europe's defence ecosystems, collaborate across multidisciplinary teams, and navigate the intersection of AI, cybersecurity, and 5G. They will gain technical expertise in AI and cybersecurity, lead teams in deploying AI models, and safeguard infrastructure against cyber threats. Additionally, participants will maintain cyber threat awareness, automate incident response, and deploy AI-powered defences to prevent attacks. This course prepares professionals to drive innovation in AI-enhanced cybersecurity and defence.

Target audience

The course is open to mid-level to senior officials (civilian and military) from EU Member States, EU Institutions, Bodies, Agencies, law enforcement officers, diplomats, and public sector leaders

Course open to

- EU Member States and EU institutions
- Candidate countries

Cyber awareness for Trainers (Activity No 259)

Location: Pocking, Germany
Dates: 15 - 18 June 2027

Course aim

The aim of the course is to help participating training managers, trainers, and cybersecurity educators standardise cyber awareness trainings within their respective organisations across EU Member States, EU Institutions, Bodies and Agencies. Furthermore, the course supports the development, implementation and evaluation of cybersecurity awareness programmes within EU institutions and Member States. providing participants with up-to-date knowledge on evidence-based predictors of successful cybersecurity training of staff.

Learning outcomes

By the end of this course, participants will be able to identify key cyber vulnerabilities, risks, and threats across security, defence, and crime domains. They will explain cyber awareness, its role in cybersecurity, and how to deliver effective training, while defining training goals and principles for design and implementation. Learners will also understand the importance of evaluation in cyber awareness programmes.

Participants will develop skills to compare different cyber awareness approaches and delivery methods, identify organisational barriers and enablers, and analyse the behavioural science behind successful cybersecurity training. They will evaluate different assessment methods, examining their strengths and limitations.

Finally, learners will assess training requirements, design conceptual approaches for course development, and create evaluation frameworks for cyber awareness programmes. They will also apply scientifically validated concepts to ensure sustainable training success. This course equips participants to develop, deliver, and evaluate impactful cyber awareness training.

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 / EU institutions, bodies and agencies
- Switzerland, Hybrid CoE
- NATO CCD CoE

Cyber ETEE (Education, Training, Exercise and Evaluation) Summer School (Activity No 260)

Location: Constanta, Romania
Dates: 15 - 18 June 2027

Course aim

The aim of the Cyber ETEE Summer School is to deepen participants' understanding of critical cybersecurity issues through interactive lectures and workshops. The program focuses on enhancing knowledge of EU cybersecurity policy, fostering resilience against cyber threats, and promoting international collaboration. It seeks to balance surveillance challenges with privacy concerns and integrate advanced technologies into cybersecurity strategies. By cultivating a multidisciplinary and collaborative ethos, the summer school aims to enhance participants' skills, expand their professional networks, and facilitate the exchange of best practices. This initiative aligns with Europe's strategic goal of strengthening digital autonomy and enhancing defence mechanisms against evolving cyber threats.

Learning outcomes

The learning outcomes of the Cyber ETEE Summer School focus on enhancing participants' understanding of EU cybersecurity policy and fostering resilience against advanced cyber threats. The summer school program aims to deepen insights into international cyber collaboration and the development of cyber resilience through a multi-stakeholder approach. Participants will explore the balance between surveillance and privacy protection and the use of emerging technologies in cybersecurity strategies. The summer school promotes a multidisciplinary and collaborative framework, aiming to transfer knowledge, improve skill sets, and expand professional networks. It encourages best practices in the maritime sector and broader cybersecurity strategies at national, European, and international levels, aligning with Europe's strategic goal of strengthening digital autonomy and defence mechanisms.

Target audience

Participants can be both civilian and military officials, junior to senior representatives from EU Member States' governmental institutions, academia, research, training providers and EU bodies and agencies and interested experts.

Course open to

- EU Member States - institutions

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

Location	Dates
Athens, Greece	23 November – 04 October 2026
Athens, Greece	Spring 2027

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: 15 - 19 March 2027

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

Cyber Threat Management (Activity No 264)

Location: Thessaloniki, Greece
Dates: 09 - 11 November 2026

Course aim

The aim for this course is to collect and analysing cyber threat intelligence from various sources, Identify and assess cyber threats and vulnerabilities, develop and implementing threat management strategies, collaborate with stakeholders to ensure a comprehensive approach to cyber threat management, provide actionable intelligence to support proactive decision-making and risk management.

Learning outcomes

By the end of this course, participants will be able to describe current cyber threats, attack methods, and stages of cyberattacks, as well as explain security measures and the role of cyber threat intelligence in organisational defence. They will analyse cyber threats using frameworks like MITRE ATT&CK and the Cyber Kill Chain, and integrate threat intelligence into security practices to strengthen incident response and overall cybersecurity.

Participants will develop skills to identify vulnerabilities, propose targeted security measures, and prioritise mitigations to reduce organisational risk. They will communicate threat intelligence effectively to stakeholders and ensure compliance with legal, regulatory, and ethical standards in intelligence handling.

Finally, learners will stay updated on emerging threats and technologies, manage cyber threat intelligence processes, and support strategic decision-making to maintain a proactive cyber defence posture. This course equips participants with the expertise to detect, analyse, and mitigate cyber threats in a dynamic digital landscape.

Target audience

The target audience for the course are cybersecurity professionals who are responsible for managing and mitigating cyber threats within their organisations. This includes Cyber Threat Intelligence Specialists, Cybersecurity Analysts, Incident Response Specialists, and IT Security Managers.

Course open to

- EU Member States / EU Institutions Bodies and Agencies
- Candidate countries

Intelligence Analysis (Activity No 268)

Location	Dates
Athens, Greece	12 – 23 October 2026
Athens, Greece	01 – 12 March 2027

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: 17 - 29 May 2027

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	Dates
Nicosia, Cyprus	10 – 12 November 2026
Constanta, Romania	21 – 23 April 2027

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

Cyber awareness Raising-in-a-Box (Activity No 271)

Location: Brussels, Belgium

Dates: 21 - 22 October 2026

Course aim

This training course will delve into all the necessary steps for crafting an Awareness Raising Program customised to suit organisations of varying types and sizes in a train–the trainer approach. Participants will gain the knowledge and skills necessary to implement a tailor-made Cyber Security Awareness Raising Program, ensuring relevance and effectiveness in their specific organisational context. This 2-day long course is crafted to enable the swift implementation of a robust Cyber Security Awareness Program. The distinctions between custom and ready-made programs will be highlighted, and ENISA's AR-in-a-box methodology will be thoroughly discussed, including guidance on maximising the use of the provided materials. Additionally, an introduction to designing a small tabletop exercise will be offered. To conclude, participants will engage in a real-time cyber awareness game, allowing them to apply their newly acquired skills and suggest enhancements.

Learning outcomes

By the end of this course, participants will be able to design and implement a comprehensive Cyber Security Awareness Programme, identifying key target audiences and the most effective dissemination channels to maximise engagement. They will learn to outline clear implementation steps for establishing such a programme and define essential evaluation metrics to measure its success. Participants will develop practical skills to create and execute a Cyber Awareness Programme, select optimal channels for content distribution, and develop engaging, gamified materials that enhance learning retention. They will also take ownership of planning and delivering awareness activities, ensuring alignment with organisational objectives. Additionally, learners will collaborate with internal and external stakeholders to maintain campaign coherence, deliver content in a timely, accurate, and compliant manner, and propose data-driven improvements to awareness strategies based on evaluation and feedback. This course equips participants with the expertise to build, manage, and refine impactful cybersecurity awareness initiatives.

Target audience

The participants should be mid-ranking to military or civilian officials dealing with information security and cybersecurity.

Course open to

- EU Member States / EU Institutions Bodies and Agencies

Implementation of Cybersecurity Technical Controls (Activity No 272)

Location	Dates
Brussels, Belgium	28 – 30 September 2026
Chania, Greece	16 – 18 March 2027

Course aim

This course aims to reinforce the necessity and precise scope of the most critical security controls, perform essential cybersecurity functions and basic incident response, and enhance understanding of performance differences between security devices, along with practical tips for handling common threats. It also provides hands-on training on cybersecurity issues, including lab-based exercises to build practical skills.

Learning outcomes

By the end of this course, participants will be able to identify cybersecurity best practices and standards, explain methodologies for implementing essential security functions, and describe incident detection, response techniques, and threat mitigation tools. They will understand Defense-in-Depth, Zero Trust, EDR, centralised logging, endpoint investigations, and network traffic analysis. Participants will gain practical skills to configure network segmentation, firewalls, IDS/IPS, endpoint security, access controls, and MFA, as well as apply system hardening, SIEM rules, and basic traffic analysis. Finally, learners will implement technical controls in supervised settings, support incident response, assess control effectiveness, and follow first-responder procedures for common cyberattacks. This course prepares participants to strengthen organisational cybersecurity defences.

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 to better support their organisation's mission. Prerequisites:

- good work/administration experience in the Linux and Windows environments, especially command line
- intermediate knowledge and experience in IT or networking.
- intermediate knowledge in some of these topics: Basic Information Security Controls, Cryptography concepts, Secure communications.

Course open to

- EU Member States, Institutions Bodies and Agencies
- Candidate countries

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

Location: Helsinki, Finland
Dates: 05 - 09 October 2026

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 by 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 counter cyber and hybrid threats and campaigns.

Target audience

The course is for 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
- Switzerland, Ukraine, Hybrid CoE, NATO CCD CoE and NATO Nations on the condition of reciprocity for all EU Member States

Cybersecurity Educator (Activity No 278)

Location: Nicosia, Cyprus
Dates: Spring 2027

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

Hybrid Threats and Intercultural Strategic Communication (Activity No 280)

Location	Dates
Rome, Italy	12 – 15 January 2027
Brussels, Belgium	April 2027

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
The Climate-Environment-Security and Defence Nexus (advanced)	07 – 14 September 2026	Sabaudia, Italy
Drones and Unmanned Systems in European Security	19 – 23 October 2026	Brussels, Belgium
Hydro Diplomacy: A tool for Climate and Environmental Resilience, Peace and Security	23 – 26 October 2026	Nicosia, Cyprus
Info-Ops for Peace, Security and Defence	27 – 30 October 2026	Pordenone, Italy
AI in Intelligence	02 – 13 November 2026	Athens, Greece
Environmental Management for CSDP	23 – 27 November 2026	Lisbon, Portugal
Intelligence Standardisation, Reporting and Briefings	07 – 18 December 2026	Athens, Greece
Military Diplomacy	17 - 21 March 2027	Warsaw, Poland

European Security
and Defence College