European Security and Defence College
Doc: ESDC/2025/027
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2027**	Activity number **216**	**Cybersecurity and international law**	ECTS **1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Non-specialised cyber course, at awareness level* • *Linked with the strategic objectives of Pillar 3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]* • *Supports the European Cybersecurity Skills Framework (ECSF) of ENISA 'Cyber Legal, Policy and Compliance Officer' profile*

Target audience	Aim
Participants should be mid-ranking to senior officials dealing with aspects of cyber security. Course participants must be available during the entire course and should be ready to contribute knowledge from their specific field of expertise and experience.	This course offers a practical approach to the application of international law in cyberspace. It is focused around current geopolitical challenges and pragmatic solutions. It covers a review of international law instruments addressing contemporary policies, including but not limited to state responsibility, cybersecurity due diligence, peaceful settlement of cyber disputes, proportional countermeasures, trans-boundary data flows including personal data, Big Data and the General Data Protection Regulation (GDPR), intermediary liability and platform regulation, as well as the human rights implications of algorithmic design and AI. Furthermore, this course will allow participants to exchange their views and share best practices on cyber-related topics while improving their knowledge, skills and competencies in this area. By the end of this course participants will possess the practical knowledge and skills needed to address contemporary international law issues in cyberspace.
Open to: ▪ EU Member States and EU institutions ▪ Candidate countries ▪ Third countries and international and regional organisations	

Learning outcomes

Knowledge	LO01 - Understand international law norms and sources and their application in cyberspace LO02 - Identify state obligations in applying international law in cyberspace, including their role in multi-stakeholder internet governance with due reference to relevant terms and definitions LO03 - Define the basic notions and concepts related to cybersecurity within international law: attribution, state responsibility, international liability, proportionate countermeasures and due diligence. LO04 - Identify the nature of the different cyber threats affecting the implementation of international law in cyberspace LO05 - Identify global cyberspace-related challenges and address them with relevant normative measures related to state responsibility and international liability

	LO06 - Define the basic notions and concepts related to hybrid threats affecting the implementation of international law LO07 - Define the basic notions and concepts related to AI in the context of international law and human rights protection online LO08 - Have a good understanding of ongoing international processes involving implementing international law online
Skills	LO09 - Classify cyber incidents in the context of 'due diligence' and 'due care' LO10 - Classify cyber threats in a risk assessment using relevant international law methodology LO11 - Categorise cyber incidents in a risk assessment as per the GDPR normative framework LO12 - Attribute cyber threats to specific actors
Responsibility and autonomy	LO13 - Evaluate the potential impacts of cyber threats in international law LO14 - Evaluate the potential impacts of cyber threats in the peaceful settlement of cyber disputes LO15 - Create opportunities for synergies with the EU cyber ecosystem and the global cyber environment for a better, safer cyberspace LO16 - Select the appropriate trust-building measures to broaden cooperation in cyber domains in the context of international law

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly level 1 evaluation (based on participants' satisfaction with the course) and level 3 evaluation (assessment of participants' long-term change in behaviour after the end of the course). Evaluation feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to fulfil all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award certificates to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the final evaluation report, which is presented to the Executive Academic Board.

Course structure

The residential course is held over 3 days

Main topic	**Suggested Residential Working Hours + (Hours required for individual learning, E-Learning etc)**	**Suggested contents**
1. Public international law – scope, sources and understanding	6 + (3)	1.1 International law principles and sources and their application to cyberspace 1.2 Responsible state behaviour in cyberspace 1.3 Attribution and state responsibility 1.4 Armed attack in cyberspace and the right to self defence 1.5 Cyber diplomacy 1.6 Cyber sanctions 1.7. Cybersecurity and cybercrime: Budapest Convention, UN Convention on countering cybercrime.
2. The EU approach to building resilience in cyberspace	12 + (4)	2.1 EU institutions, bodies and agencies working on the application of international law in cyberspace 2.2 EU policies and their impact on cyberspace and international security, including but not limited to:

		2.2.1 EU Cybersecurity Strategy 2.2.2 Digital Single Market Strategy for Europe 2.2.3 Network and Information Security (NIS) Directive 2 2.2.4 Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' 2.2.5 Cybersecurity Act 2.2.6 EU Cyber Diplomacy Toolbox 2.2.7 EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises 2.3 General Data Protection Regulation and risk-based approach to resilience building 2.3.1 Data protection risk assessment 2.3.2 Due diligence and risk mitigation – good practices 2.3.3 Data protection principles in practice 2.4 The AI Act 2.4.1 Definitions and risk assessment 2.4.2 AI and cybersecurity 2.4.3 Transnational impact of EU Regulation
3. The EU approach to hybrid threats	2	3.1 International law responses to hybrid and cyber threats 3.2 EU position on the application of international law in cyberspace 3.3 National positions on the application of international law in cyberspace 3.4 EU cyber sanctions regime 3.5 Countering disinformation and Digital Services Act Package
4. Cyber responsibility of states and stability in the global environment	7	4.1 Analysis of the impact of cybersecurity on global stability 4.2 Responsibility of states for cyber incidents, cybersecurity due diligence, cybersecurity and peaceful settlement 4.3. Confidence building measures
TOTAL	**27 + (7)**	

Materials

Required:

- AKU 1 History and Context of the CSDP
- AKU 2 on European Global Strategy

Recommended:

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union and repealing Directive (EU) 2016/1148.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Council conclusions on strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry (November 2016)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form specific area of expertise may be used.

All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all residential modules of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".

• The EU Cyber Diplomacy Toolbox (June 2017) • The EU Cybersecurity Act (June 2019) • The EU's Cybersecurity Strategy for the Digital Decade (December 2020) • United Nations Convention against Cybercrime, UN Res. 79/243. • UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report, UN Doc. A/70/174 (2015).	