European Security and Defence College
Doc: ESDC/2022/069
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Course on Cybersecurity and International law	ECTS 1
Feb. 2024	216		EAB.CYBER N/A

Target audience	Aim
Participants should be mid-ranking to senior officials dealing with aspects in the field of cyber security including from Third Countries Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience. Open to: ▪ EU Member States / EU Institutions Bodies and Agencies ▪ Third countries ▪ International Organisations	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 GDPR, intermediary liability and platform regulation, as well as human rights implications for algorithmic design and AI. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on cyber-related topics by improving their knowledge, skills and competencies. By the end of this course the participants will dispose of practical knowledge and skills to address contemporary international law issues in cyberspace..

Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

Knowledge	L01- Understanding of international law norms, their sources and application in cyberspace L02- Identifying state obligations in applying international law in cyberspace, identifying their respective role in multi-stakeholder internet governance with due reference to relevant terms and definitions. L03- Define the basic notions and concepts related to cyber security within international law: attribution, state responsibility and international liability, proportionate countermeasures and due diligence. L04- Identify the nature of the different cyber threats affecting the implementation of international law in cyberspace L05- Identify global cyberspace related challenges and address them with relevant normative measures on state responsibility and international liability L06- Define the basic notions and concepts related to hybrid threats affecting the implementation of international law L07- Define the basic notions and concepts related to AI in the context of the international law and human rights protection online L08- Have a good understanding of ongoing international processes around implementing international law online L08- Define the basic notions and concepts related to hybrid threats

Skills	L09- Classify cyber incidents in the context of 'due diligence' and 'due care' L10- Classify cyber threats risk assessment with relevant international law methodology L11- Categorize cyber incidents risk assessment as per the GDPR normative framework L12- Attribute cyberthreats to specific actors
Responsibility and Autonomy	Evaluate the potential impacts of cyber threats in the international laws L13- Evaluate the potential impacts of cyber threats in the peaceful settlement of cyber disputes L14- Create opportunities for synergies with the EU cyber ecosystem and the global cyber environment for a better safe cyberspace L15- Select the appropriate trust building measures to broaden cooperation in cyber domains in the context of the international laws

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *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 feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *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 module is held over 3 days. It is a non- specialised course, at awareness level link with the Pillar 3 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020).
Furthermore, the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase].

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Public International Law – scope, sources and understanding	6(3)	1.1 International law principles and sources and their application to cyberspace
2. The EU Approach 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 2.2.4 Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 2.2.5 Cyber Security Act 2.2.6 General Data Protection Regulation 2.2.7 EU Cyber Diplomacy Toolbox 2.2.8 EU Coordinated Response to Large Scale Cybersecurity Incidents and Crises
3. The EU Approach in the Hybrid threats	2	3.1 International law responses to hybrid and cyber threats
4. Cyber responsibility of states and the stability in the Global Environment	7	4.1 Analysis of the impact of the cyber security in the global stability 4.2 Responsibility of states for cyber incidents, cybersecurity due diligence, cybersecurity and peaceful settlement
TOTAL	**27(7)**	

Materials	Methodology
Required: AKU 2 on European Global Strategy **Recommended:** • Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union • 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) • The EU Cyber Diplomacy Toolbox (June 2017) • The EU Cybersecurity Act (June 2019) • The EU's Cybersecurity Strategy for the Digital Decade (December 2020)	The course is based on the following methodology: lectures, panels, workshops **Additional information** The Chatham House Rule is applied during all residential modules of the HLC: "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 mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September).