European Security and Defence College **Doc: ESDC**/2020/031 **Date:** 14/02/2020 **Origin:** ESDC Secretariat

Curriculum

To be reviewed by	Activity number*	Course (*and module*)	ECTS
February 2022	***203***	**Cybersecurity Basics for Non-Technical Experts**	**1**

Target audience*	Aim**
Participants should be non-technical end users (civilians or military personnel) that need to use IT equipment on a daily base and want to understand the cybersecurity basics from both the regulatory and technical perspective.	This course aims to enable participants to: • Explain the current cybersecurity strategy and legislation from the European Union's perspective. • Document and in-depth understanding of current cyberattacks, threats, vulnerabilities and risks on an understandable and technical way for non-technical persons. • Move beyond the classic cybersecurity awareness training and let the participants to use their own IT defence in a real environment.

Learning outcomes* **		
	Knowledge	K1 – Outline the principles of European cybersecurity strategies and norms, K2 – Explain the complexity of cybersecurity, K3 – Define the basics of cyber-threats, K4 – List the basic technical controls. K5 – Explain the necessity of the recommended measures related to the cybersecurity protection
	Skills	S1 – Implement Cybersecurity Best Practices, aligned with EU legislation, S2 – Develop cyber-security plans, select the appropriate security measures to establish the information security management S3 – Classify the cyber threats, and identify the domain-specific vulnerabilities, S4 – Analyse the cyberattacks (i.e fundamentals of malwares, information-based attacks) and attacking methods,
	Competences	C1 – Propose measures for integration of the European cybersecurity legislation within the organization, C2 - Promote cybersecurity awareness activities in the organization, C3 – coordinate implementation a range of recommended counter-measures, C4 - Decide on the proposed security counter-measures.

Prerequisite	1. English: **Level B2 (**Common European Framework of Reference for Languages) 2. Basic knowledge of IT: ECDL or similar knowledge, 3. General Cybersecurity awareness.

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participant's satisfaction with the course*).
In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on the active contribution in the residential Module, including their syndicate session and practical activities as well as on their completion of the eLearning phases: course participants finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. Active observation by the course director/lead instructor and feedback questionnaire filled by course participants at the end of each of the three modules is used. An overall evaluation report will be drafted at the end of the course (3 modules). For the High Level Conference, a level 1 evaluation will take place.
However, no formal verification of learning outcome is foreseen; proposed ECTS is based on participants' workload only

Course structure		
Main Topic	**Recommended Working Hours (of that eLearning)**	**Contents**
Cybersecurity from the European perspective	8(4)	- European cybersecurity strategy - The interaction of the CFSP/CSDP with the EU CYBER Ecosystem (Institutions, Policies, Directives)
Cyber-attacks in practice	8	- Cyberattacks (i.e Social engineering, Malware attacks, DoS and DDoS attacks etc.), - Study cases of known cyber incidents - Mitigation measures related with the cyber-attacks.
Selection & Implementation of Technical Security Controls	10 (4)	- Information security management in the cyber field, - The usage of cybersecurity tools at the individual level (i.e firewalls, antivirus, secure procedures etc.), - Cybersecurity on networks (i.e IDS/IPS, firewalls, filters, network tools), - Cyber hygiene
TOTAL	**26 (8)**	

Materials	Additional information
E-learning material Presentations Case studies	Pre-course questionnaire on learning expectations and possible briefing topic from the 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. In order to facilitate discussion between course participants and trainers/experts/guest speakers, the **Chatham House Rule** is used during the residential Module: "participants to the CSDP HLC 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 participants are invited to agree on being photographed or filmed during the training sessions; the pictures or films can be used by the ESDC or concerned ESDC network partners in relation with CSDP related training delivered within the Network

* Description of the number, level and background of the participants. Selection criteria are also described in case there is need to limit the participation. This is copied to the invitation to advice the nominators.

** The aim describes the reason why this training is organised.

*** Learning outcomes should contain action verbs and be performance-based, describing what the participant will be able to do at the end of the course. When writing learning objectives, it is better to avoid vague and generic words such as “know, understand, internalize and appreciate”.

**** Learning outcomes are closely linked to learning evaluation questions before, during and after the course. Evaluation criteria can be developed by making use of speed, accuracy and quality. Sometimes the parameters or conditions might need to be detailed.