ESDC Executive Academic Board

Doc.: EAB/2015/007
Date : 12 February 2015
Origin: ESDC Secretariat

EUROPEAN SECURITY AND DEFENCE COLLEGE

Activity number 20

Cyber Security/Cyber Defence Course (CSC)

Curriculum

February 2015

Aim

1. The overall aim of the Cyber Security/Cyber Defence Course (CSC) is to enable participants:
   - To understand the extensive nature of the information society we are living in and to recognise its complexity and the different threats we are experiencing;
   - To understand the basic notions and concepts related to cyber security and cyber defence;
   - To identify the EU institutions involved in cyber security, cyber defence and their respective roles;
   - To understand cyber threats, and get an overview on technological tools;
   - To be aware of the different trends in Cyber Threats;
   - To become familiar with international cyberspace issues and cyber diplomacy; ;
   - To identify the challenges of cyber security at a European level and the way ahead;
   - To evaluate the potential impacts of cyber security on public policies; To identify the challenges of industrial and public planning needed to face cyber threats.

2. Provide opportunity to create a network of people working in the field

General description and Organisation

3. **Initial situation**

   Required level of course participants:

   Participants should be mid-ranking to senior officials dealing with strategic aspects in the field of Cyber Security and cyber defence. They should be either working in key positions or have a clear potential to achieve leadership positions, in particular in the field of Cyber Security or Defence.

   The CSC audience should be a well balanced mix of diplomats, civilians working in the field of rule of law (including police) or civil administration, and military personnel. Academics and members of the business community may also be invited to participate in this course.

   Course participants must be available for the whole course and must be ready to bring in their specific expertise and experience throughout the course.

4. **Methodologies**

   In general, interactive learning methods should be used throughout the residential module. That should include seminar work and working groups followed by discussions in the plenary. The focus should be on deepening knowledge of the various issues and giving the course participants the chance to discuss issues in a wider context and with key players working within the EU.

   Case studies should be conducted to allow course participants to see and learn how theory works in the context of actual EU activities.

5. **Evaluation**

This CSC will be evaluated according to the Kirkpatrick model[1]. An evaluation feed back should be given to participants at the beginning of the module. Module leaders will provide an evaluation report (according to the pattern established by the secretariat) . The Course Director will be responsible for presenting the final evaluation report to the Steering Committee, including recommendations on how to further develop and improve the course.

Overall structure and duration of the course

The course will be composed of a preparatory Internet-based Distance Learning module (IDL) and the residential course of 3 days.

6. **The Internet-based Distance Learning (IDL) module will**
include as mandatory the study of the following Autonomous Knowledge Units
AKU 1 'History and Context of CSDP Development',
AKU 2 'European Security Strategy',
AKU 3 'Role of EU institutions in the field of CFSP/CSDP and
AKU 7 ' The impact of the Lisbon Treaty on the CSDP'.

Based on the need, other available AKU's for study on a mandatory or voluntary basis could be made available.

This residential module lasts 3 days:

7. **Residential Module Program**.

Day 1	Day 2	Day 3
Introduction to the ESDC Defining Information Society Trends in Cyber Threats	Legal framework for cyber security and cybercrime Concepts for cyberspace governance, including national strategies and international policies	Capacity challenges in cyber security Public-Private Partnerships in the Cyber security framework
European cyber security strategy EU's implementation of cyber security EU Cyber Defence Policy Framework	Critical infrastructure protection against cyber attacks EU Military cyberspace protection (EU Cyber defence policy framework)	Internet and democracy Exercise of power in the Information Society => related to CSDP missions/operations

[1] In 1959, Dr Donald L Kirkpatrick developed a four-level evaluation model. The four levels address the following aspects: student reaction, learning, (long term) influence on behaviour and organisational results. Since then, this model has arguably become most used evaluation model in the world. For more information, you can i.a. consult: http://www.businessballs.com/kirkpatricklearningevaluationmodel.htm.

The Course Programme can be adapted according to recent needs and to national education systems.

8. Reading material

- European Commission: Communication on Critical Information Infrastructure Protection. 'Achievements and next steps: towards global cyber-security' (2011)
- Enhanced cyber defence policy since September 2014,
- Wales summit conclusions
- The UK Cyber Security Strategy. Protecting and Promoting the UK in a digital world (2011)
- Défense et sécurité des systèmes d'information. Stratégie de la France (2011)
- Council of Europe: Convention on Cybercrime (2004)
- EU Cyber Security Strategy – An open, safe and secure cyberspace
- EU Cyber Defence Policy Framework
- EU Council Conclusions on Cyber Diplomacy
- Military concept for EU led operations (EUMS)

9. The presentations and discussions will focus on the general following topics:

Defining the information society:
- Economic Drivers
- Fragility of our information society
- Our digital footprints

Trends in Cyber Threats:
- Modus operandi
- Most widespread attack tools and malware
- Actors

European cyber strategy:
- Concepts for European cyber security
- Cyber defence concepts

EU's implementation of cyber security:
- Institutions in charge
- European documents of reference

Cyber diplomacy, international cyber policy and legal frameworks for cyber security:
- Cyber diplomacy and international cyber issues
-
- Applying the UN Charter and International Humanitarian Law in cyberspace
- Addressing cybercrime and promoting the Budapest Convention
- State of the art of cyber regulation in the EU and national best practices

Concepts for cyberdefence:
- EU-NATO cooperation
- International cooperation
- Benchmark of national practices

Critical infrastructure protection against cyber attacks:

- Description of the EU initiatives
- National approaches and best practices
- Achievements and way ahead

EU Military cyberspace protection:

- Specificity of military cyberspace
- Incidence of digitization and robotization of the battle field
- Cyber security and cross-domain warfare

Capacity challenges in cyber security:

- State of the art of EU capacities in cyber security
- Actions of EDA
- Human resource capacity building
- Building a European cyber industry

Public-Private Partnerships in the Cyber security framework:

- Needs of public security on a private infrastructure
- Program coordination

Internet and democracy:

- The e-infrastructure for e-democracy
- Open society and access to information over Internet
- Use of Internet and human rights

Exercise of power in the Information Society

- Social network HUMINT
- Profiling online user