Professional development is vital for the Defence's ability to solve problems – now and in the future.

COURSE DESCRIPTION

Cyberspace Operations and Cyber War

(FLEX-module in the Master in Military Studies)

Course description

Organizational impact
This course contributes to developing and sustaining the ability of the Danish armed forces to fight in, through and by cyberspace.

Purpose
This course provides officers who will serve in higher command staffs with an understanding of cyberspace as a domain for military operations. The purpose is to enable them to give relevant and timely guidance on the use of cyberspace and development of the Danish armed forces' ability to fight in, through and by cyberspace.

Entry Requirements
The target audience for this module is officers from the armed forces at the level of NATO OF-2 (captain) and OF-3 (major).

Students enrolled in the Master of Military Studies (MMS) program have priority (tier 1 audience). Other employees within the Danish armed forces or other Danish governmental institutions will be accepted for participation as tier 2.

Civilian and military personnel from NATO and partner nations will be accepted for participation as tier 3.

Applicants must at least have completed an education at level 6 (e.g. bachelor degree) and be familiar with academic methodology prior to course start.

The course is taught in English. Participants must have good English skills (NATO 3-3-3-3 iaw. ATrainP-5).

The course is taught at the unclassified level. No security

Practical information

Date of publication
01 November 2018

Target group
Military officers at NATO OF-2 (DNK M321) and NATO OF-3 (DNK M331) level, or an equivalent civilian level

Participants
Minimum 12
Maximum 24

Level of education
Level 7 (Master) cf. qualification framework for lifelong learning

ECTS
5 ECTS

Duration
11 weeks part-time

Dates
18 March 2019 -
31 May 2019

Registration
For MMS-students: Via the Event Management

clearance is required for attendance.

Learning outcomes
Officers graduating from this course can critically discuss the relevance of cyberspace for military operations and advice on needed changes to existing technologies, doctrines and organisational setups.
After graduation, the officer has the knowledge, skills and competences stated below.

Knowledge
On a theoretical basis, the officer can:
- Refer to the psychological basis for cyber security.
- Seek guidance in influence theory and the psychology behind social engineering.

- Discuss definitions and concepts related to military cyberspace operations.
- Account for how Denmark ensures nation-wide cyber security and resilience and the role of the Danish armed forces therein.
- Discuss the relevance of moral and legal norms for CO.
- Discuss the laws governing the use of force in cyberspace. Account for the characteristics of cyberspace as an operational environment.
- Discuss the nexus between mission assurance and armed forces' reliance on computers and networks.

- Explain the relevance of cyberspace operations for attaining strategic and operational ends.
- Compare and critique how different cyber forces are organised and fight.

Skills
- Differentiate between various types of actions and actors in cyberspace.
- Use correct terminology related to CO.
- Argue from relevant foundations such as deterrence theory, the security dilemma or the attribution problem.

- Extract lessons to be learned from recent cyber incidents.
- Advice on cyberspace related issues to a non-technical and non-cyber savvy audience verbally and in writing.

Competencies
Officers graduating from this course can independently and in collaboration with others:

System.
Others: Send your application through the advertisement on www.fak.dk.

Registration deadline
14 December 2018

Price
Employees under the Ministry of Defence: Free.
Others: 7.000 DKK.

Course provider
Royal Danish Defence College, Svanemoellen Barracks, Ryvangs Allé 1, DK-2100 Copenhagen OE

Course Organiser
Lt. Cdr. Henrik Palbo
Institute for Military Technology
Royal Danish Defence College
E-mail: hepa@fak.dk
FIIN: fak-imt-07
Tel.: +45 7281 7379

Study Supervisor
Cdr. Claus Smith Rasmussen
Royal Danish Defence College
E-mail: clra@fak.dk
FIIN: fak-mms01
Tel.: +45 7281 7062

Programme Office
Sr. Ass. Sascha Hedberg
E-mail: studiekontor@fak.dk
FIIN: fak-pd-stu02
Tel.: +45 7281 7082

SAP ID
D-object 03569466

Course abbreviation

- See the differences between various types of actions in cyberspace.
- See the relevance of cyberspace operations for attaining strategic and operational ends.
- Develop guidance on how to best fight in, through and by cyberspace.

Content
- Definitions and terminology.
- Cyberspace as an operational environment.
- Actors in cyberspace.
- Cyber security in the state.
- CO and strategy.
- CO and military theory.
- Laws and norms relevant to CO.
- Cyberspace and military operations.
- The psychology of cyberspace attack and defense.

Learning activities
The course is organised as a blend of distance-learning and on-campus learning activities.

Internet access is required. Wifi is provided by the Royal Danish Defence College on-campus.

On average, participants shall expect to use:
- 6 hours weekly throughout the course on reading mandatory material and
- 7 hours weekly on online learning activities (etivities) (only in distance learning periods).

It is advisable to schedule this workload to deconflict with other activities.

Time
The course spans a period of 11 weeks.

Date of access to the course e-learning platform, ICECore: 11 March 2019.
Note that access to the course site will expire after six years.

Course start: 18 March 2019
Course end: exam hand-in 31 May 2019

On-campus periods: 01-04 April (week 14), 13-15 May (week 20) 2019

Exam
Take-home assignment with approximately 14 days to write a paper.

The paper is graded using the Danish 7-point scale (ECTS-scale).
An external examiner is appointed.

Comments
Dress code during on-campus activities: Battle dress uniform (DNK "MTS"). Civilians wear casual attire.

Related courses
Cyberspace Operations Officer and Liaison (COOL).
SAP ID: D-object not yet created. Contact Lt. Cdr. Henrik Palbo, fak-imt-07, for information.

International Cyber Education (ICE).
SAP ID: D-object not yet created. Contact Cpt. Lasse Kronborg, fak-imt-08, for information.

TGR 900 – IT Sikkerhedsbrugerkursus.
SAP ID: D-objekt 03195703.