



Course Syllabus
Cyber Operations in an Antagonistic Environment

Cyberoperationer i antagonistisk miljö

Course Code	2FS029	Main Field of Study	Systems Science for Defence and Security
Valid from Semester	Spring 2022	Department	Department of Systems Science for Defence and Security
Education Cycle	Advanced level	Subject	Systems Science for Defence and Security
Scope	7.5	Language of Instruction	The teaching is conducted in English.
Progression	A1N	Decided by	The Research and Education Board's Course Syllabus Committee at the Swedish Defence University
Grading Scale	Fail, Pass, Pass with Distinction	Decision date	2022-01-01
Revision	1.0		

Entry Requirements

For elective course: Admitted to a Master's Programme at the Swedish Defence University.

For freestanding courses: A bachelor's degree with a minimum of 180 credits, including a minimum of 90 credits in the field of defence, crisis management and security. Alternatively, a bachelor's degree in Engineering or equivalent.

Course Content and Structure

Based on students' previous knowledge and experience, the cyber environment is problematized with the purpose of enabling them to describe, discuss, and analyse threats, risks, and events. The course starts with an introduction to computers and networks with the aim of providing a common frame of reference for the rest of the course. The second part of the course deals with the Internet, automated systems, and the actors in the cyber environment. The distinctive features of the cyber area are particularly emphasized.

The course consists of two modules. Introduction to computers and networks (1.5 hec) and cyber operations (6 hec).

Modules

Introduction to Computers and Network

Introduktion till datorer och nätverk

Scope: 1.5

- Basic concepts and methods for computers and networks

After completed course, the student should be able to:

Knowledge and understanding

- Explain basic concepts and methods for computers and networks as well as the functional principles of the Internet.

Cyber Operations

Cyberoperationer

Scope: 6.0

- Function and governance of the Internet.
- Threats, risks, and opportunities with regard to automated systems.



- Principal actors and their general approaches to cyber operation

After completed course, the student should be able to:

Knowledge and understanding

- Explain the processes and organisations that govern the Internet.

Competence and skills

- Describe and discuss automated technical systems from a vulnerability and user perspective.
- Describe and discuss different actors' actions within the cyber environment.

Judgement and approach

- Independently discuss and analyse the content in research articles relevant to the area.

Intended Learning Outcomes

After completed course the student should be able to:

Reference to the respective module.

Type of Instruction

The course is taught through lectures, self-study, laboratory work and seminars.

Assessment

Introduction to Computers and Networks

Scope: 1.5

Grading Scale: Fail, Pass

Assessment is through a written lab report.

Late exams are not graded unless approved by the examiner on the basis of special reasons.

The examiner can decide regarding supplementary tasks for attaining passing grade.

Supplementary task must be turned in no later than five working days after results and supplementary task have been conveyed for the exam in question.

Cyber Operations

Scope: 6.0

Grading Scale: Fail, Pass, Pass with Distinction

Assessment is through a written home examination.

Late exams are not graded unless approved by the examiner on the basis of special reasons.

The examiner can decide regarding supplementary tasks for attaining passing grade.

Supplementary task must be turned in no later than five working days after results and supplementary task have been conveyed for the exam in question.

Grading

Module 1 Introduction to computers and networks

Grading is made on a two-step scale: pass (G) and failed (U).

Module 2 Cyber operations

Grading is made on a three-step scale: pass with distinction (VG), pass (G), and failed (U).

The overall grade of pass (G) requires passing grade on both the written lab report and the home examination.



The overall grade of pass with distinction (VG) requires passing grade on the written lab report and pass with distinction on the home examination.

Restrictions in Number of Examinations

The number of examination opportunities is not limited.

Restrictions Concerning Degree

The course can not be included in a degree with another course whose content fully or partially corresponds to the content of this course.

Transitional Provisions

When the course is no longer given or when the course content has changed significantly, the student has the right to be examined once per semester during a three-semester period according to this syllabus

Miscellaneous

If a student has a decision from the Swedish Defence University on special educational support due to a disability, the examiner may decide on alternative forms of examination for the student.

Course evaluation is carried out after completion of the course through the course coordinator and is the basis for any changes to the course.

The course is given as an elective course within the Master's program in the development of systems for defense and security.

The course can also be given as a stand-alone course.

The course is given in English. If there are no international students, parts or the entire course can be given in Swedish.



Reading List

Cyber Operations in an Antagonistic Environment

Cyberoperationer i antagonistisk miljö

Course Code	2FS029
Revision	1.0
Reading List Valid from Date	2020-05-28
Reading List Decided Date	2020-05-28

2MF016 course textbooks

The course is based on research articles which will be made available during the course.