Module 8 **Information, Knowledge Protection and Cybersecurity**			
Workload	ECTS-Credits	Semester	Length of module
180 hours (47 hours class contact time, 133 hours self study time)	6	2nd semester	1 semester
Responsible academic			
N.N.			

Structure of the Module		
No.	Section	Class Contact Time
1	Information and Knowledge in International Security Management	1 SWS
2	Knowledge Protection in Companies	1 SWS
3	Cyber Protection and Investigation	1,5 SWS

Module Description

Information is crucial in knowledge-based societies. Knowledge creation and technological development are the most substantial prerequisites for welfare, and worldwide information-sharing facilitates intercultural exchange and international cooperation. But information and knowledge are also vulnerable. In international politics, states might steal information to gain advantages in international power competition, or misuse (des)-information to manipulate political opponents and foreign publics. In the economic sector, companies may be deprived of valuable knowledge, trade secrets, and inventions they heavily invested in. Furthermore, corporate information and information infrastructure can be damaged or blocked for ransom or sabotage purposes. It is thus often necessary to protect valuable knowledge and critical information infrastructure for various corporate, private and political security reasons.

State agencies and private companies use mass data generated by the use of electronic devices for surveillance and marketing purposes. The protection of human rights, especially of privacy and data protection, has therefore become highly relevant in using information.

The global interconnection of information infrastructure is an important security issue. The internet facilitates international communication, but also makes it vulnerable. This has made cybersecurity another major issue.

Module Aims

This module aims to:

- develop and deepen students' understanding of the role of information for security management and in knowledge-based societies in general
- strengthen skills in assessing threats related to globalised information networks
- enhance research skills to analyse the implementation of information security

in critical infrastructures and private companies, using of a wide range of primary sources
- enhance critical understanding of public and private strategies developed for information security.

Learning Outcomes/Competences/Skills

By the end of the module, students will be able to demonstrate a theoretical understanding of information and knowledge. They will:

- have critical knowledge about the distinction between different kinds of information and be able to analyse their value and vulnerability from an interdisciplinary perspective
- make use of theoretical insights to analyse empirical cases and to develop strategies for information security in the private or public sector
- analyse the range of state and private actors who operate with different means and toward different ends in cyberspace
- identify critical vulnerabilities that need special protection, and the technological and methodological approaches that can be used to secure the information environment.

Content

Section 1: Information and Knowledge in International Security Management

- Ontological and epistemic fundaments of information and knowledge
- Knowledge as an asset
- Categorisation of information operations
- International and European copyright standards
- Privacy/data protection: European and international challenges and approaches
- Cooperation/information sharing between private and state actors/public-private partnerships
- Knowledge management/ transfer of knowledge

Section 2: Knowledge Protection in Companies

- Identification of risks and security gaps
- Scenarios of informational damage
- Strategic threat analysis
- Technical and management tools for knowledge protection
- Information security in companies, public administrations and critical infrastructures

Section 3: Cyber Protection and Investigation

- Characteristics of cyber space
- Actors and interests in cyber space
- Cyber regulation – European and international approaches
- Detecting and analysing cyber attacks
- Strategic threat analysis
- Simulation of cyber attacks
- Preventive strategies and methods for defensive information security (sensitisation, significance of cryptology, early warning, incidence response,

ISMS etc.)
Prerequisites for attending
-
Teaching Language
English
Examination
Project/case study [Projektarbeit/ Fallstudie]
Relevance of the Examination for the final Scale
10,5 %