COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cyber Warfare

Course

Field of study
Computing

Year/semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes

Other (e.g. online)

Tutorials

Projects/seminars

Number of credit points

1

Lecturers

Responsible for the course/lecturer:
dr hab. inż. Sławomir Hanczewski

email: slawomir.hanczewski@put.poznan.pl

tel:61 665 3946

Faculty of Computing and Telecommunications
Polanka 3, 60-965 Poznań

Responsible for the course/lecturer:
mgr inż. Michał Weissenberg

email: michal.weissenberg@put.poznan.pl

tel: 61 665 3946

Faculty of Computing and Telecommunications
ul. Polanka 3, 60-965 Poznań

Prerequisites

The student starting this course should have basic knowledge of cybersecurity, ICT networks, and have basic programming skills. He should also have the ability to obtain information from the indicated sources.

The student should demonstrate such qualities as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

1. Provide students with a theoretical foundation about the concept of cyberwar.

2. Familiarize students with the theoretical foundations of the concept of cyber warriors as well as examples of types of weapons and the latest trends in cyber warfare.

3. Provide a theoretical basis for attacks on a computer network and their defense.

4. Show students the social, ethical, legal, and political aspects of cyberwar.

Course-related learning outcomes

Knowledge

A student has structured and theoretically founded general knowledge related to key issues in the field of computer science, including analysis of operating systems. [K2st_W2]

A student has advanced detailed knowledge regarding selected IT issues and their applications in cyber warfare risk analysis. [K2st_W3]

A student knows development trends and the most important cutting-edge achievements in computer science, particularly in the area of cyber warfare risk analysis. [K2st_W4]

A student knows the basic programs and applications used to collect data and analyze them in the process of cyber warfare risk analysis. [K2st_W6]

Skills

A student is able to assess the usefulness and the possibility of using the information obtained in the literature analysis and available on the Internet in the area of cyber warfare. [K2st_U1]

A student is able to assess the suitability and the possibility of using new achievements (methods and tools) and new IT products in the field of cybersecurity. [K2st_U6]

A student is able to assess the usefulness and the possibility of using and developing the basic tools used in the area of analysis of the risks associated with cyber warfare. [K2st_U8]

A student knows the basic concepts of cyber warfare and is able to use them to describe the process of analysis of the risks associated with cyber warfare. [K2_U12]

A student can define the stages of further acquisition of knowledge in the field of cyber warfare, as well as obtain information on this subject and implement the process of self-education, including other people in this area. [K2_U16]

Social competences

A student understands that in the field of IT, cybersecurity, and cyber warfare the knowledge and skills quickly become obsolete. [K2st_K1]

A student understands the importance of using the latest knowledge in the field of computer science, cybersecurity, and digital forensics in solving research and practical problems. [K2st_K2]

A student understands the importance of popularization activities concerning the latest achievements in the field of cyber warfare. [K2st_K3]

A student is aware of the need to develop professional achievements and comply with the rules of professional ethics. [K2st_K4]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: knowledge is verified by a written and/or oral test. The pass mark is 51% of the points, and it is not allowed to use any auxiliary materials during the test.

Programme content

1. Introduction - concepts, definitions, history, and acts related to cyber warfare.

2. Cyber Threatscape - attack methodology, tools, techniques with described attack types and defense types.

3. Cyberspace battlefield.

4. Cyber doctrine, legal system impacts, and ethics in different countries.

5. Cyber warriors.

6. Types of weapons in cyber warfare - logical weapons, physical weapons, psychological weapons.

7. Computer network security.

Teaching methods

1. Lecture: multimedia presentation illustrated with examples.

Bibliography

Basic

J. Andress and S. Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", 2nd Edition, Syngress, 2013

J. Carr, "Inside Cyber Warfare. Mapping the Cyber Underworld", 2nd Edition, O'Reilly Media,

C. Whyte, B. Mazanec, "Understanding Cyber Warfare. Politics, Policy and Strategy", Routledge 2018

Additional

H. H. Dinniss, "Cyber Warfare and the Laws of War", Cambridge University Press, 2014

Breakdown of average student's workload

	Hours	ECTS
Total workload	25	1,0
Classes requiring direct contact with the teacher	15	0,5
Student's own work (literature studies, preparation for exam)[1]	10	0,5

[1] delete or add other activities as appropriate