



UNIVERSITY OF NICOSIA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΛΕΥΚΩΣΙΑΣ

University of Nicosia, Cyprus

Course Code	Course Title	ECTS Credits
COMP-527	Cyber Warfare	10
Department	Semester	Prerequisites
Computer Science	Fall/Spring	COMP-514 Cryptography and Network Security
Type of Course	Field	Language of Instruction
Required for <i>CyberSecurity</i> concentration	Computer Science	English
Level of Course	Year of Study	Lecturer(s)
2nd Cycle	1st	Dr Ioanna Dionysiou
Mode of Delivery	Work Placement	Co-requisites
face-to-face	N/A	None

Objectives of the Course:

The main objectives of the course are to:

- provide students with the appropriate theoretical foundations on the main cyber warfare concept.
- expose students to practical techniques that aim in exploiting, attacking, and defending computer networks.
- provide a comprehensive view of cyber warfare from the technical, legal, and regulatory perspectives.
- present the deployment of cyber warfare activities at national levels.
- expose students to the social, ethical, legal, and political aspects of cyber warfare.

Learning Outcomes:

After completion of the course students are expected to be able to:

1. discuss the impact of warfare in the cyberspace.
2. discuss the subjects of network security, information assurance, intelligence, cryptology, infrastructure protection in both defensive and offensive contexts.
3. identify and explain actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information in computers and computer networks.
4. identify and explain actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks.
5. explain how to enable intelligence collection capabilities conducted through computer networks to gather data from target or adversary automated information systems or networks.
6. analyze cyber related decisions as they apply to national and military strategy from social, ethical, legal, and political viewpoints.
7. investigate and evaluate national cyber warfare activities.

Course Contents:

1. Introduction to Cyber Warfare *Threatscape*: definition of cyberwar, motivation, attackers, threats, fifth domain on warfare, differences between cyber warrior and traditional warrior.
2. Analysis of Cyber Attacks: analysis of recent years' sophisticated cyber attacks such as Stuxnet.
3. Cyber Weapons: Logical (scanning, exfiltration tools, etc.), physical (physical means), psychological (social engineering).
4. Cyber Warfare Attacks and Tactics: cyber attack process and evolution, select cyber weapons and associated attack strategies, network exploitation techniques.
5. Cyber Defense Tactics: defensive strategies for securing networks and information, global intelligence and deception operations, emergence of new intelligence tools.
6. Cyber Warfare Doctrine and Strategy: materialization of cyber warfare in modern armies, evolving doctrines and changes in national doctrines for the usage of cyber force (e.g. US and Russian).
7. Cyber Warfare Capabilities by Nation.
8. Legal Status and Ethics of Cyber Warfare: legislations, targeting and precautions in attack, legitimate military objectives, protection of civilian objects, hospitals and other medical units, etc.
9. Emerging trends in Cyber Warfare such as critical infrastructure protection, models and dilemmas in the use of cyber weapons.

Learning Activities and Teaching Methods:

Lectures, case studies, lab activities, guest lectures

Assessment Methods:

Written and programming assignments, lab exercises, midterm exam, final exam

Required Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
Jeffrey Carr	Inside Cyber Warfare: Mapping the Cyber Underworld	O'Reilly Media	2011	1449310044
Jason Andress and Steve Winterfeld	Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Second edition	Syngress, Elsevier	2013	0124166725
Heather Harrison Dinniss	Cyber Warfare and the Laws of War	Cambridge University Press	2012	1107011086

Recommended Textbooks/Reading:

Authors	Title	Publisher	Year	ISBN
Steve Winterfeld and Jason Andress	The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice	Syngress, Elsevier	2012	0124047378
Christopher Paul	Information Operations - Doctrine and Practice: A Reference Handbook	Praeger Security International	2008	0275995917
Dorothy Denning	Information Warfare and Security	Addison-Wesley Professional	1998	0201433036
Pauline C. Reich and Eduardo Gelbstein	Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization	IGI Global	2012	1615208313

Richard Clarke	Cyber War: The Next Threat to National Security and What to Do About It	Ecco	2012	0061962244
----------------	-------------------------------------------------------------------------	------	------	------------

