Cyber crime, cyber terrorism and cyber war

Academic Year: (2020 / 2021) **Review date: 08-09-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: ESTEVEZ TAPIADOR, JUAN MANUEL

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

None

OBJECTIVES

- Acquire the knowledge required to propose original designs or developments, often in a research process within the area of cyber security.

- Ability to apply acquired knowledge to solve problems under novel or almost novel situations, or within broader (multidisciplinar) contexts related with cyber security.

- Ability to state critical opinions and judgements having incomplete or limited information in the field of cyber security. These judgements must take into account considerations about social and ethical responsibilities.

- Ability to communicate to a public audience the conclusions of a work carried out. Students will be able to give their foundational and most convincing reasons to a specialized and non specialized audience in a clear way, without ambiguities.

- Students should have the learning skills required to continue studying in a autonomous or self-directed way.

- Understand and apply methods and techniques to investigate vulnerabilities of a given site.

- Create and refine concise and comprehensively documents, plans and projects in the scope of cyber security.

- Know the relevant technical parts of legal regulations in cyber security and their implications in the design of systems and security tools.

- Analyze and detect anomalies and attack signatures in systems and networks.

- Analyze and detect hiding techniques in attacks to systems and networks.

- Knowledge of trends in cyber attack techniques and learned experiences in real cases.

- Know and apply cryptographic and steganographic mechanisms required to protect data stored in a system or data transiting a network.

DESCRIPTION OF CONTENTS: PROGRAMME

1. Introduction, Definitions, and Basic Concepts
1.1. Origins
1.2. Cyberattacks galore
1.3. A brief history of malware
1.4. Welcome to the underground economy
1.5. The cyberthreat landscape 2011-2017
1.6. Trends

2. Cyberattacks and Cyberactivism
2.1. Types of cyber attacks
2.2. Cybercrime

2.3. Cyberespionage
2.4. Analysis of Practical Cases
2.5. Legal Aspects

3. Cyberterrorism and Cyberoperations against Critical Infrastructures
3.1. Critical Infrastructures: Interconnections and Vulnerabilities
3.2. Industrial Control Systems
3.3. Other Critical Infrastructures
3.4. Analysis of Practical Cases

4. Cyberwar
4.1. Cyberweapons: Logic, Physical, and Psychological Instruments
4.2. Cyberdoctrine
4.3. Analysis of Practical Cases

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES:

- Lectures and practicals
- Tutorship
- Group work
- Individual work

METHODOLOGIES

- Lectures to introduce and discuss the main course concepts.

- Study and analysis of references provided by the lecturer, including academic papers, reports, selected book chapters, and press articles. This will be instrumental to consolidate and complement concepts introduced in the course, and also as material to be discussed during some lectures.

- Analysis of practical cases proposed by the lecturer, either individually or in group.

- Presentation and discussion of topics and practical cases related to the course.

- Preparation of individual essays and reports.

ASSESSMENT SYSTEM

The assessment system includes:

1. Continuous assessment of the student through one or more of the following methods:
   1.1. Oral or written tests.
   1.2. Essays and reports assigned by the lecturer.
   1.3. Presentations about a course topic.
   1.4. Participation in the debates organized throughout the semester.

Continuous assessment accounts for 60% of the final mark.

2. Final exam assessing the knowledge and skills acquired during the course.

The final exam accounts for 40% of the final mark.

For the extraordinary exam there are three cases:
a) Keep the grade obtained during the term in the continuous assessment process and sit an exam for the remaining 40% of the final grade; or

b) Students who have not followed the continuous assessment process will sit an exam for 100% of the final grade. This exam may have questions related to all activities done during the course.

c) Students who have followed the continuous assessment process can request being marked using the procedure discussed in b).

% end-of-term-examination:	40
% of continuous assessment (assigments, laboratory, practicals…):	60

BASIC BIBLIOGRAPHY

- Bill Blunden, Violet Cheung Behold a Pale Farce: Cyberwar, Threat Inflation, & the Malware Industrial Complex, Trine Day, 2014
- Brian Krebs Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door, Sourcebooks, 2014
- Bruce Schneier Secrets and Lies: Digital Security in a Networked World, Wiley, 2004
- Christopher Hadnagy, Paul Wilson Social Engineering: The Art of Human Hacking, Wiley, 2010
- Christopher Paul Information Operations - Doctrine and Practice: A Reference Handbook, Praeger, 2008
- Cliff Stoll The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, 2005
- Cristopher Hadnagy, Paul F. Kelly, Paul Ekman Unmasking the Social Engineer: The Human Element of Security, Wiley, 2014
- Dennis F. Poindexter The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests, McFarland, 2013
- Derek S. Reveron Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Georgetown University Press, 2012
- Edwin L. Armistead Information Operations: Warfare and the Hard Reality of Soft Power, Potomac Books Inc., 2004
- Ian Mann Hacking the Human, Gower, 2008
- Ian Mann Hacking the Human 2, Consilience Media, 2013
- J. D. Lasica Darknet: Hollywood's War Against the Digital Generation, Wiley, 2005
- Jason Andress, Steve Winterfeld Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners, Syngress, 2013
- Jeffrey Carr Inside Cyber Warfare: Mapping the Cyber Underworld (2nd Edition), O'Reilly Media, 2011
- Jonathan Clough Principles of Cybercrime, Cambridge University Press, 2010
- Julie E. Mehan Cyberwar, Cyberterror, Cybercrime and Cyberactivism (2nd Edition), ITGP, 2014
- Kevin D. Mitnick, William L. Simon The Art of Deception: Controlling the Human Element of Security, Wiley, 2003
- Kevin D. Mitnick, William L. Simon The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Wiley, 2005
- Kevin Hogan, James Speakman Covert Persuasion: Psychological Tactics and Tricks to Win the Game, Wiley, 2006
- Kevin Mitnick, William L. Simon Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, Back Bay Books, 2012
- Kevin Poulsen Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground, Broadway Books, 2012
- Majid Yar Cybercrime and Society, 2nd Edition, SAGE Publications Ltd., 2013
- Mark Bowden Worm: The First Digital World War, Grove Press, 2012
- Martin C. Libicki Cyberdeterrence and Cyberwar, RAND Corporation, 2009
- Nicholas Capaldi The Art of Deception: An Introduction to Critical Thinking, Prometheus Books, 2007
- P.W. Singer, Allan Friedman Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014
- Parmy Olson We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, Back Bay Books, 2013
- Patrick D. Allen Information Operations Planning, Artech House Publishers, 2007
- Phil Lapsley Exploding the Phone, Grove Press, 2014
- Richard A. Clarke, Robert Knake Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2012
- Robert Moore Cybercrime, Second Edition: Investigating High-Technology Computer Crime, Anderson, 2006
- Ronald J. Deibert Black Code: Surveillance, Privacy, and the Dark Side of the Internet, Signal, 2013
- Thomad Rid Cyber War Will Not Take Place, Oxford University Press, 2013