| FLORENCE UNIVERSITY OF THE ARTS<br>THE AMERICAN UNIVERSITY OF FLORENCE | SYLLABUS | |
|---|---|---|

DIVA – DIGITAL IMAGING AND VISUAL ARTS

**SCHOOL OF SCHOOL OF DIGITAL IMAGING AND VISUAL ARTS**
**DEPARTMENT OF INTERNET TECHNOLOGY**
**COURSE TITLE: INFORMATION SECURITY & RISK ANALYSIS**
**COURSE CODE: DIITIS150**
**3 semester credits**

## 1. DESCRIPTION

This course investigates the pillars of information security and risk analysis, providing students with the technical and linguistic skills necessary to understand how cyber threats and vulnerabilities are controlled and mitigated by state and non-state actors. Students will become familiar with the political, social, and economic governance of cyberspace, while exploring notions such as security, privacy, transparency, and confidentiality. The exploration of methods employed for information security, such as encryption, will be assessed in relation to ethical considerations. The course comprises the analysis of a variety of case-studies to allow students to interlink theory and practice, and envision the dynamics and impacts of cybersecurity on real-life scenarios.

## 2. OBJECTIVES

Upon successful completion of this course, students will be able to:

- Understand the terminology and the tools related to information security and risk analysis.
- Understand the notions of security, privacy, transparency, and confidentiality.
- Identify the roles of state and non-state actors in cyber security.
- Identify the means used by key players to mitigate risks.
- Recognize the social and legal implications of information security.
- Become familiar with the pillars of cyberterrorism, crime intelligence, and information warfare.

## 3. REQUIREMENTS

There are no prerequisites for this course.

## 4. METHOD

This course consists of lectures, class discussions, projects, and site visits within the local community. Mediums for instruction used will include, but are not limited to, interactive and hands-on activities which challenge thought processes, academic texts and studies, videos, slides, guided problem solving, and experiential and/or field learning activities where applicable.

## 5. TEXTBOOK – FURTHER READINGS – RESOURCES

TEXTBOOK:

- Harkins, Malcolm W. *Managing Risk and Information Security*. Auerbach Publishers, 2nd ed. 2016.
- Van Puyvelde, Damien & Brantly, Aaron F. *Cybersecurity: Politics, Governance, and Conflict in Cyberspace*. Polity Press. 2019.

The Textbooks are pre-ordered and available at: Paperback Exchange in Via delle Oche 4r or

laFeltrinelli Via dei Cerretani 40R. Textbooks may also be available for purchase online or in e-book format.

The textbook is mandatory for successful completion of the course.

Where applicable, additional materials, handouts and/or notes will be provided by the instructor.

## FURTHER READINGS

- Kick, Jason. *Cyber Exercise Playbook*. 2014. Available here: https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf
- Nastase, Ramon. *Computer Networking, An Introductory Guide for Complete Beginners*. 2018.
- Wikileaks, https://wikileaks.org/

## LIBRARIES IN FLORENCE

The FUA-AUF library is located in Corso Tintori 21. Please consult the posted schedules for official opening times. Also note that the library is for consultation only and it is not possible to borrow materials. The library is equipped with a scanner and internet access so that you may save or email a digital copy of the pages needed.

Students may also utilize additional libraries and research centers within the local community:

### BIBLIOTECA PALAGIO DI PARTE GUELFA

Located in Piazzetta di Parte Guelfa between Piazza della Repubblica and Ponte Vecchio. Please consult the library website for hours of operation:
http://www.biblioteche.comune.fi.it/biblioteca_palagio_di_parte_guelfa/

### BIBLIOTECA DELLE OBLATE

Located in via dell'Oriuolo 26. Please consult the library website for hours of operation:
www.bibliotecadelleoblate.it

### THE HAROLD ACTON LIBRARY AT THE BRITISH INSTITUTE OF FLORENCE

Located in Lungarno Guicciardini 9. Please consult the library website for hours of operation. This library requires a fee-based student membership. For information: www.britishinstitute.it/en

## 6. FIELD LEARNING

Please consult your Official Registration for any mandatory field learning dates. Field Learning Activities cited in Official Registrations are an integral part of the course and also include an assignment that counts towards your final grade, details will be provided on the first day of class.

## 7. COURSE MATERIALS

No additional course materials are necessary.

## 8. COURSE FEES

Course fees cover course-related field learning activities, visits, and support the instructor's teaching methodologies. Book costs are not included in the course fee. The exact amount will be communicated by the instructor on the first day of class.

## 9. EVALUATION – GRADING SYSTEM

10% Attendance

20% Participation & Assignments

25% Midterm Exam

30% Final Exam

15% Final Presentation

A = 93-100 %, A- = 90-92%, B+= 87-89%, B = 83-86%, B-=80-82%, C+ = 77-79%, C=73-76%, C-=70-72%, D = 60-69%, F= 0-59%, W = Official Withdrawal, W/F = Failure to withdraw by the designated date.

## 10. ATTENDANCE – PARTICIPATION

Academic integrity and mutual respect between instructor and student are central to the FUA-AUF academic policy and reflected in the attendance regulations. Student presence is mandatory and counts toward the final grade.

Absences are based on academic hours: 1 absence equals 3 lecture hours.

Two absences: 6 lecture hours, attendance and participation grade will be impacted.
Three absences: 9 lecture hours, the final grade may be lowered by one letter grade.
Four absences: 12 lecture hours, constitutes automatic failure of the course regardless of when absences are incurred.

Please note:

- The above hours refer to lecture hours. Please note that the contact / credit hour policy in the academic catalog includes additional distribution ratios according to delivery category.

Ex: 1 absence equals 6 FL/SL/Lab hours or 9 EL hours.

- Hours may be distributed in different formats according to the academic course schedules.

LATE ARRIVAL AND EARLY DEPARTURE

Arriving late or departing early from class is not acceptable. Two late arrivals or early departures or a combination will result in an unexcused absence. Travel is not an exceptional circumstance.

TRAVEL (OR DELAYS DUE TO TRAVEL) IS NEVER AN EXCUSE FOR ABSENCE FROM CLASS.

It is always the student's responsibility to know how many absences he or she has in a course. If in doubt, speak with your instructor!

**Participation:** Satisfactory participation will be the result of contributing to class discussions by putting forth insightful and constructive questions, comments and observations. Overall effort, cooperation during group work, proper care of work space and tools, responsible behavior, and completion of assignments will be assessed. All of the above criteria also apply to Field Learning and site visits.

## 11. EXAMS – PAPERS – PROJECTS

Example of how exams, papers, and projects are detailed and graded:

The **Midterm Exam** accounts for 25% of the final course grade. For exam time and date consult the course addendum. **The time and date of the exam cannot be changed for any reason.**

Format: the exam is divided into three sections:

- Part I: Multiple choice questions for a total of 20 points.
- Part II: Short-answer questions for a total 50 points.
- Part III: Essay questions for a total of 30 points.
-

The **Final Exam** accounts for 30% of the final course grade. For exam time and date consult the course addendum. **The time and date of the exam cannot be changed for any reason.**

Format: the exam is divided into three sections:

- Part I: Multiple choice questions for a total of 20 points.
- Part II: Short-answer questions for a total 50 points.
- Part III: Essay questions for a total of 30 points.

The Final Exam is cumulative.

The **Final Presentation** is worth 15% of the final course grade. This is a group presentation focusing on a case-study of choice, to be confirmed by the instructor. The case-study should explore a security violation, a risk mitigation tactic, and/or cybersecurity policy. Each student should use 3 slides circa to support their argument.

## 12. LESSONS

| **Lesson 1** | |
|---|---|
| **Meet** | In class |
| **Lecture** | The value of information.<br>Information security and cybersecurity.<br>The spread of the Internet and the rise of cyber threats. |
| **Objectives** | Gain knowledge of the basic concept of the IT network.<br>Develop a technical dictionary related to information security.<br>Identify the major cyber threats. |
| **In-Class Activity** | Discuss major cyber incidents, find commonalities and differences. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Introduction, Ch. 1 |

| **Lesson 2** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Approaching risk in the cyberspace.<br>Deep and dark web. |
| **Objectives** | Be able to define cyberspace.<br>Gain knowledge of the physical-network layer, logical-network layer, and persona layer of the cyberspace.<br>Identify the key pillars used to manage risk.<br>Learn about the features of deep and dark web. |
| **In-Class Activity** | How to use a TOR browser to navigate the dark web. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 2<br>Read: Harkins, Ch. 1 |

| **Lesson 3** |
|---|

| | |
|---|---|
| **Meet** | In class |
| **Lecture** | The subjectivity of risk.<br>Security, privacy, transparency, confidentiality.<br>Uses and abuses of social media. |
| **Objectives** | Identify the meanings, similarities, and differences of security and privacy.<br>Be able to define notions related to information security.<br>Gain knowledge about the nature of cyber risk and its misperceptions.<br>Understand the ways of using social media platforms with particular attention to legal limits.<br>Show how the algorithms underlying social media work. |
| **In-Class Activity** | In groups, share which social media you have and assess the risks that each one presents, then define which one is more threatening for you. |
| **Readings/ Assignments** | Read: Harkins, Ch. 2 |

| **Lesson 4** | |
|---|---|
| **Meet** | In class |
| **Lecture** | The political, social, and economic governance of cyberspace.<br>History and uses of encryption and cryptography, from steganography to public key-private key cryptography. |
| **Objectives** | Explore the relationship between Internet governance and cybersecurity.<br>Identify the differences between a multilateral and a multistakeholder institution.<br>Identify the history of encryption and cryptography.<br>Recognize the current uses of cryptography. |
| **In-Class Activity** | Discuss end-to-end encryption and compare WhatsApp and Telegram. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 3 |

| **Lesson 5** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Cyber capabilities and insecurities.<br>Emerging threats and vulnerabilities. |
| **Objectives** | Identify the various malware types and features.<br>Learn how offensive, criminal, and state cyber capabilities are developed.<br>Be able to recognize threat agents.<br>Gain knowledge of the malware industry.<br>Become familiar with the Cyber Kill Chain. |
| **In-Class Activity & Visit** | In class, learn how to use a network scanner.<br>Explore an open network in the wild, and assess which vulnerabilities you are able to find. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 4<br>Read: Harkins, Ch. 6 |

| **Lesson 6** |
|---|

| | |
|---|---|
| **Meet** | In class |
| **Lecture** | National cybersecurity and strategy.<br>Case studies of different countries: rues and impacts. |
| **Objectives** | Identify the role, characteristics, and threats of national cybersecurity.<br>Become familiar with a variety of national case studies and be able to compare the systems. |
| **In-Class Activity** | Create an infographic discussing the different national cybersecurity models of China, Russia, United States, and Italy. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 5 |

| **Lesson 7** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Midterm Exam |

| **Lesson 8** | |
|---|---|
| | Academic Break |

| **Lesson 9** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Cyber war and warfare.<br>State and non-state threats. |
| **Objectives** | Gain knowledge about war in the fifth domain.<br>Gain knowledge about cyberterrorism.<br>Identify the role of hacktivism. |
| **In-Class Activity** | Discuss the Stuxnet and Olympic Games case study.<br>Confirm Final Presentation's topic. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 6-7 |

| **Lesson 10** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Corporate social responsibility.<br>Ethics of hacking: white hats, black hats, gray hats<br>The history of hacking: bright side vs dark side. |
| **Objectives** | Identify the meaning and significance of corporate social responsibility.<br>Identify the uses of backdoors, phishing, trojan, ransomware, and spyware.<br>Gain knowledge about penetration tests. |
| **In-Class Activity** | Discuss the actions of the groups Anonymous and Legion of Doom.<br>If you were a hacktivist, what or who would you target? |
| **Readings/ Assignments** | Read: Harkins, Ch. 9 |

| **Lesson 11** |
|---|

| | |
|---|---|
| **Meet** | In class |
| **Lecture** | Mass surveillance and privacy management.<br>Uses of big data. |
| **Objectives** | Understand the technologies and the legal structures on which mass surveillance is based.<br>Show how the analysis of large data structures, even publicly available, allows the development of predictive criteria. |
| **In-Class Activity** | Discuss the Wikileaks case study.<br>Discuss the Cambridge Analytica case study. |
| **Readings/ Assignments** | Watch: Mr. Robot, Episode 1<br>Browse: https://wikileaks.org/ |

| **Lesson 12** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Deterrence and defense in the cyberspace.<br>Pros and cons of implementing costs-benefit analyses. |
| **Objectives** | Identify the characteristics and differences between deterrence by denial and by punishment.<br>Recognize the difficulties to achieve justice in the cyberspace.<br>Recognize the issues with costs-benefit analyses in relation to cyberattacks. |
| **In-Class Activity** | Create an infographic analyzing the advantages and disadvantages of defense and deterrence. Discuss which option appears to be more effective. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 8 |

| **Lesson 13** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Cybersecurity and democracy.<br>The futures of information security in the cyberspace. |
| **Objectives** | Be able to discuss whether cybersecurity has become essential to democracy.<br>Identify the main interrelations between cybersecurity and democracy.<br>Identify the bearings caused of the IoT for the future. |
| **In-Class Activity** | Discuss the EuroMaidan movement and Ghostnet case studies. |
| **Readings/ Assignments** | Read: Van Puyvelde & Brantly, Ch. 9-10 |

| **Lesson 14** | |
|---|---|
| **Meet** | In class |
| **Lecture** | Final Presentations.<br>Revision. |
| **Objectives** | Be able to present a case study in relation to the notions learned during the course.<br>Be able to interlink the diverse pillars of information security and risk analysis. |
| **In-Class Activity** | Final Presentations and Q&As. |
| **Readings/ Assignments** | Submit Final Presentation's slides. |

| **Lesson 15** |
|---|

| | |
|---|---|
| **Meet** | In class |
| **Lecture** | Final Exam |