Syllabus

Cybersecurity: Prevention and Regulation of Cybersecurity - 48429

Last update 08-04-2018

HU Credits: 3

Degree/Cycle: 1st degree (Bachelor) and 2nd degree (Master)

Responsible Department: program for undergraduate students & Master

Academic year: 0

Semester: 2nd Semester

Teaching Languages: English

Campus: Mt. Scopus

Course/Module Coordinator: Tamar Berenblum

Coordinator Email: tamar.berenblum@mail.huji.ac.il

Coordinator Office Hours: Mondays by appointment

Teaching Staff:
Tamar Berenblum
**Course/Module description:**

As cyberspace — the online world of computer networks and the internet — evolves, it also facilitate the spread of disruptive cyber activities, which have the potential to cause significant damages for individuals, organizations and states. Today’s transition to cyberspace and internet of things (IOT) has created new challenges for the prevention and regulation of cyber threats including cybercrimes, cyber-warfare, internet terrorism, human rights violations and more.

But what exactly is cybersecurity? What are cybersecurity threats? What kind of policy challenges, in this regard, is the world facing today? Who are the social actors taking part in solving cybersecurity problems? How efficient are the international legal instruments and the regional and the national policies in addressing problems of cybersecurity? Could multilateral diplomacy solve cybersecurity problems?

These questions will be explored in depth throughout this course from national (Israeli) as well as international perspectives. We will discuss cyber threats and their prevention and regulation from legal, criminological and public policy perspectives.

**Course/Module aims:**

**Learning outcomes - On successful completion of this module, students should be able to:**

Demonstrate knowledge about cyber security and cyber crimes and their regulation.

Create research designs in a critically meaningful way to address specific cyber security related questions

**Attendance requirements(%):**

100

**Teaching arrangement and method of instruction: Lectures**

**Course/Module Content:**

The development of cyberspace

the architecture of the internet

Cybersecurity definition
Cybersecurity policy
Cybercrimes
Cyber victimization
Cyber-warfare
Cyber terrorism

*Human rights violations* [surveillance and privacy]

Social control and the Cyber sphere

Cyber laws, regulation and enforcement

Researching cyber security

**Required Reading:**


Executive Orders, DHS, CII, FTC section 5, HIPPA, SOX

EU Network Security Directive, 6 July 2016, Articles 1,2,4,6,16

EU General Data Protection Regulation, April 27, 2016, Articles 1-4 and 12-23

Schrems v. Data Protection Commissioner, Judgement (Summary), Case C-362/14, European Court of Human Rights, 6 October 2015


Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to State Activity in Cyberspace, Cambridge, 2017, Rules 1-4 (pp. 11-27), Rule 6 (pp. 30-42) Rule 8 (pp. 51-54) and Rule 14 (pp. 84-87)

Joseph Nye, A Normative Approach to Preventing Cyberwarfare, Project Syndicate, March 13, 2017


Additional Reading Material:

Course/Module evaluation:
End of year written/oral examination 0 %
Presentation 30 %
Participation in Tutorials 0 %
Project work 55 %
Assignments 15 %
Reports 0 %
Research project 0 %
Quizzes 0 %
Other 0 %

Additional information: