



The Hebrew University of Jerusalem

Syllabus

Israeli and International Cybersecurity Law - 62324

Last update 13-08-2017

HU Credits: 2

Degree/Cycle: 1st degree (Bachelor)

Responsible Department: law

Academic year: 0

Semester: 1st Semester

Teaching Languages: Hebrew

Campus: Mt. Scopus

Course/Module Coordinator: Deborah Housen-Couriel

Coordinator Email: Deborah.HousenCouriel@huji.ac.il

Coordinator Office Hours: By prior arrangement with the instructor

Teaching Staff:

Course/Module description:

The emerging field of cyber law is characterized by rapid and substantive changes in the activities to which it applies both in the international arena and in Israel. Nearly half of the world's population currently has access to cyberspace, a new human phenomenon that has had much positive impact (such as in the fields of health, education and law). However, there are also phenomena of abuse by hostile elements: states, societies, groups and individuals.

This course reviews and analyzes the legal and regulatory regimes applicable to activities in cyberspace, given this complex reality. It examines the development of cyber law and the various governance arrangements currently in place, including international agreements, codes of conduct, and other developments; as well as the developing body of Israeli laws and regulations and its relationship to international cyber law.

The course program consists of four units: Legal and Regulatory Frameworks for Cyberspace at the International and Domestic Levels; Israeli Cyber Law and Regulation; The Balance between Security and Individual Rights in Cyberspace; and International and Israeli Legal and Regulatory Developments in Cyberspace. Within these four units we will analyze events in cyberspace and the key legal issues they raise, such as cyberattacks on critical infrastructures, data breaches, cybercrime and terrorist use of the internet, and international cooperation mechanisms for the enforcement of cyber law and regulation. Towards the end of the course, an in-class moot court will be held on the main issues studied.

Course/Module aims:

- ☐ *To present course participants with an understanding of the basic concepts of state and non-state activities in cyberspace*
- ☐ *To present them with the main normative systems applicable to such activities on the international and Israeli levels*
- ☐ *To provide participants with a range of professional tools for their use in practice, including the ability to analyze ongoing developments in cyberspace and their legal and regulatory implications*
- ☐ *To instill in the participants the ability to identify and analyze the various ideological and methodological approaches to cyber law and regulation; in particular, Israel's approach to cyber law and regulation*
- ☐ *To analyze the weaknesses in the application of international and Israeli cyber law, and to encourage critical thinking about cyber law and its application*

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

- Understand basic concepts relevant to global and Israeli cyberspace activity, including concepts relevant to internet governance
- Identify the main norms and institutions applicable to state activity in cyberspace
- Identify the main norms and institutions applicable to the activities of non-state actors in cyberspace (companies, groups, individuals)
- Describe the main theoretical approaches to the study of cyber law
- Identify the main trends in the development of cyber law on the global and Israeli levels, including the main dilemmas
- Evaluate the achievements and failures of cyber law, the various approaches to its continued development and the main critique of cyber law and its implementation

Attendance requirements(%):

academic to According דרישות נוכחות לפי כללי הפקולטה; חובה למשפט המבוים הכיתתי requirements; obligatory for in-class moot court exercise
Attendance requirements (%)

Teaching arrangement and method of instruction: Lectures and in-class moot court exercise

Course/Module Content:

►Cyberspace as a New Arena of State and Non-State Activity: Initial Legal Aspects and Concepts

Unit A: Legal and Regulatory Frameworks for Cyberspace at the International and Domestic Levels

►Development of Normative Frameworks Internationally and Domestically: An Overview

►Internet Governance

►Selected International Agreements and Arrangements Applicable to Cyberspace

►Sovereignty, Jurisdiction, Due Diligence and State Responsibility in Cyberspace: Tallinn Manual 2.0 (I)

►Use of Force, Self-Defense, and International Humanitarian Law in Cyberspace: Tallinn Manual 2.0 (II)

Unit B: Israeli Cyber Law and Regulation

Israeli Law in Cyberspace: Development of Israeli Law Applicable to Cyberspace

► *Israeli Law in Cyberspace: Regulation of the Cyber Professions and the Sectoral Regulatory Approach*

► *Israeli Law in Cyberspace: Cyber Crime and Cyber-Enabled Terrorism*

Unit C: The Balance between Security and Individual Rights in Cyberspace

► *International and National Security in Cyberspace in the Post-Snowden Era; Protection of Individual Rights and Regulation of Social Media in Israel*

► *EU Law and Regulation: Network Security and Data Protection*

Unit D: International and Israeli Legal and Regulatory Developments in Cyberspace

► *In-class Moot Court Exercise (15%)*

► *Current Global and Israeli Developments in Cyber Law*

Required Reading:

Class 1 (22.10) – Cyberspace as a New Arena of State and Non-State Activity: Initial Legal Aspects and Concepts

Unit A: Legal and Regulatory Frameworks for Cyberspace at the International and Domestic Levels

Class 2 (29.10) –Development of Normative Frameworks Internationally and Domestically: An Overview

Class 3 (5.11)- Internet Governance

Class 4 (12.11) –Selected International Agreements and Arrangements Applicable to Cyberspace

Class 5 (19.11) – Sovereignty, Jurisdiction, Due Diligence and State Responsibility in Cyberspace: Tallinn Manual 2.0 (Part I)

Class 6 (26.11) – Use of Force, Self-Defense, and International Humanitarian Law in Cyberspace: Tallinn Manual 2.0 (Part II)

Unit B: Israeli Cyber Law and Regulation

Class 7 (3.12) – Israeli Law in Cyberspace: Development of Israeli Law Applicable to Cyberspace

Class 8 (10.12)- Israeli Law in Cyberspace: Regulation of the Cyber Professions and the Sectoral Regulatory Approach

Class 9 (24.12)- Israeli Law in Cyberspace: Cyber Crime and Cyber-Enabled Terrorism

Unit C: The Balance between Security and Individual Rights in Cyberspace

Class 10 (31.12) – Global and National Security in Cyberspace in the Post-Snowden Era; Protection of Individual Rights and Regulation of Social Media in Israel

Class 11 (7.1) – EU Law and Regulation: Network Security and Data Protection

Unit D: International and Israeli Legal and Regulatory Developments in Cyberspace

Class 12 (14.1) – In-class Moot Court Exercise (15%)

Class 13 (21.1) – Current Global and Israeli Developments in Cyber Law

Additional Reading Material:

אתרי אינטרנט נבחרים :

- ☐ *Electronic Frontier Foundation*
- ☐ *European Union Agency for Network and Information Security (ENISA)*
- ☐ *FBI Cybercrime*
- ☐ *International Telecommunication Union – Cybersecurity*
- ☐ *Israel National Cyber Event Readiness Team – CERT-IL*
- ☐ *מטה הסייבר הלאומי*
- ☐ *הרשות הלאומית להגנת הסייבר*
- ☐ *NATO Cooperative Cyber Defence Center of Excellence*
- ☐ *NETmundial*
- ☐ *OECD – Information security and privacy*
- ☐ *US Department of Homeland Security – Cybersecurity Division*

Course/Module evaluation:

End of year written/oral examination 85 %
Presentation 0 %
Participation in Tutorials 0 %
Project work 0 %
Assignments 0 %
Reports 0 %
Research project 0 %
Quizzes 0 %
Other 15 %
other

Additional information:

Should students require special arrangements for learning and testing, please consult university authorities for the appropriate documentation. Please refer to the Dean of Students site for more information.