The Hebrew University of Jerusalem

Syllabus

Israeli and International Cybersecurity Law - 62324

Last update 18-09-2023

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@cyberregstrategies.com

Coordinator Office Hours: By appointment

Teaching Staff:

Deborah Housen-Couriel

Course/Module description:

The developing field of cyber law is characterized by rapid and substantive changes in the normative international and Israeli regimes that apply to states, organizations and individuals in cyberspace. Currently, more than 60% of the world's population has access to cyberspace. This is a new human phenomenon that has brought about significant positive results (for example, in the spheres of health, education, science and law). Nevertheless, the misuse and abuse of cyberspace by hostile elements has become routine: cyberattacks, hacking, data breaches, terrorist use of the internet and other abuses are steadily increasing in number and impact. These phenomena raise many questions concerning the governance of cyberspace, the normative legal regime that applies, and the implementation and enforcement of norms.

In the course participants will analyze legal and regulatory aspects of cyber activity that take place within this complex reality. The course examines the processes of development of cyber law and the various existing arrangements for its governance, treaties, agreed codes of conduct and other arrangements. Additionally, we shall examine the developments in the Israeli legal system currently applicable to activity in cyberspace. We shall also examine the reciprocal relationship between Israeli law and the normative international system that applies to cyberspace. Several aspects of application of developing norms and their enforcement both in the international and in the Israeli arenas, will be accompanied by an ongoing analysis of these issues.

The course syllabus is structured on the basis of six units: (1) an introduction to state and non-state activity in cyberspace (2) cyber law and policy in Israel, (3) international law and regulation of cyberspace (4) the protection of data privacy in Israel, the EU and other countries (5) the balance struck in various regimes between rights of the individual in cyberspace and security considerations (for example, in the monitoring of personal information by governmental authorities) and (6)current trends and the influence of technological developments on cyber law. In the context of these units, we shall analyze the main issues and their ramifications, such as the vulnerability of critical infrastructure; the hacking of websites and databases, online crime and terrorism; use of internet capabilities by terrorist elements; and mechanisms of international collaboration for the enforcement of cyber law.

Towards to the end of the course a tabletop exercise / moot court will be held in which the main issues we have studied will be examined (5% of the final grade). 95% of the final grade is on the basis of a written paper (8 pages max.). Students may benefit from up to 5 bonus points for legal analysis of a cyber event and presentation of the analysis to the class.

Course/Module aims:

•To impart to the participants an understanding of the basic concepts of state and non-state activity in cyberspace;

•To familiarize them with the principal norms applicable to the activity in the international and Israeli arenas;
•To provide the participants with professional tools which they will be able to use in practice, including an ability to analyze current developments in cyberspace;
•To enable the participants to assimilate the ability of identifying and analyzing the various ideological and methodological concepts that apply to the regulation of cyberspace;
•To analyze the weaknesses inherent in the normative systems applicable to cyberspace; and
•To encourage critical thinking about cyber law and its implementation, on the global and on the Israeli levels.

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

Attendance requirements(%):
There is no formal grade for attendance, but it is expected that participants will contribute to the class discussion. For students' attention: thie class will be conducted via Zoom. The tabletop exercise at the end of the course allows a grade of up to 5% in the final course grade. Students may benefit from up to 5 bonus points for legal analysis of a cyber event and presentation of the analysis to the class.

Teaching arrangement and method of instruction: The method of instruction will be online, using the Hebrew University ZOOM platform (via Moodle).

Course/Module Content:
יחידה א': מבוא
שיעור 1 - מרחב הסייבר כתחום פעילות חדשה של מדינות וגורמים לא-מדינתיים: מושגי יסוד והיבטים משפטיים ראשוניים (חלק א')
נק' עיקריות - הגדרת מרחב הסייבר, היכרות עם אתגרים נורמטיביים במרחב הסייבר, היקף וסוג השימוש באינטרנט, היכרות עם פעולות לוחמה במרחב הסייבר והתגובות להן

שיעור 2 - מרחב הסייבר כתחום פעילות חדשה של מדינות וגורמים לא-מדינתיים: מושגי יסוד והיבטים משפטיים ראשוניים (חלק ב')
נק' עיקריות - הגדרת מרחב הסייבר, היכרות עם אתגרים נורמטיביים במרחב הסייבר, היקף וסוג השימוש באינטרנט, היכרות עם פעולות לוחמה במרחב הסייבר והתגובות להן

יחידה ב': דיני סייבר בישראל
שיעור 3 – דיני סייבר ישראליים: התפתחות הדין הישראלי במרחב הסייבר
נק' עיקריות - בחינה ראשונית של ההסדרה של מרחב הסייבר בישראל; "חוק הגנת הסייבר הישראלי"

ומערך הסייבר הלאומי

שיעור 4– דיני סייבר ישראליים: תפיסת הרגולציה המגזרית
נק' עיקריות - התפיסה הרגולטורית המגזרית בישראל, לצד הגדרת תשתיות חיוניות וההגנה עליהן

שיעור 5– דיני סייבר ישראליים: פשע מקוון וטרור מקוון (מרצה אורח: רם לוי, מייסד ומנכ"ל חברת קונפידס דיגיטל בע"מ)
נק' עיקריות -מבט על פריצות במרחב הסייבר הישראלי בשנים חקיקה פשע המקוון בישראל והיבטי אכיפתה; ישראל ואמנת בודפשט, הסדרת טרור מקוון בעולם ובהקשר של חוק המאבק בטרור - התשע"ו-2016

יחידה ג': הסדרים משפטיים ורגולטוריים החלים במרחב במישור הבינלאומי
שיעור 6 – פיתוח הסדרים נורמטיביים במרחב במישור הבינלאומי: מבט על
נק' עיקריות - ריבוי שחקנים בתהליכים הנורמטיביים, גישות שונות להסדרה נורמטיבית של מרחב הסייבר, יוזמות נורמטיביות רב-צדדיות להסדרה.

שיעור 7 – ריבונות, סמכות שיפוט, עקרון בדיקת הנאותות (diligence due) ואחריות המדינה במרחב הסייבר: מדריך טאלין 2.0 (חלק א')
נק' עיקריות - החלת המשפט הבינלאומי הקיים על פעילות מדינתית במרחב הסייבר - עקרונות היסוד

שיעור 8– ריבונות, סמכות שיפוט, עקרון בדיקת הנאותות (diligence due) ואחריות המדינה במרחב הסייבר: מדריך טאלין 2.0 (חלק ב')
נק' עיקריות - החלת המשפט הבינלאומי הקיים על פעילות מדינתית במרחב הסייבר - עקרונות היסוד

שיעור 9 -הסדרים בין-מדינתיים נבחרים במרחב הסייבר
נק' עיקריות – ניתוח של הסדרים בין-מדינתיים נבחרים שחלים במרחב הסייבר ומגמות בהתפתחותם

יחידה ה': השפעתן של התפתחויות טכנולוגיות על מגמות משפטיות במרחב
שיעור 11 – איזונים בין זכויות האדם וצרכים ציבוריים במרחב הסייבר (מרצה אורח: Wein Matthew, US House of Representatives Committee on Homeland Security))
נק' עיקריות - הצורך באיזון בין סמכויות המדינה לצרכי בטחון ובין זכויות הפרט במרחב; היבטים משפטיים של ניטור אזרחים ע"י הממשלה; מהי "המדינה האלגוריתמית"?

יחידה ו': תרגיל כיתתי
שיעור 12 – תרגיל סייבר כיתתי
נק' עיקריות - 5% מהציון הסופי, חומר יחולק לקראת השיעור

יחידה ז': השפעתן של התפתחויות טכנולוגיות על מגמות משפטיות במרחב
שיעור 13 - מגמות בפיתוח דיני הסייבר במישור הבינלאומי והישראלי - מרצה אורחת: עו״ד לימור שמרלינג מגזניק מנהלת המכון הישראלי למדיניות טכנולוגיה

***

Required Reading:
FOR DETAILED READING MATERIALS, PLEASE REFER TO THE COURSE WEBPAGE IN MOODLE.

Additional Reading Material:
Recommended websites:

■ *The Federman Cyber Security Center - Cyber Law Program*
■ *International Cyber Law in Practice: Interactive Toolkit*
■ *International Cyber Terrorism Regulation Project (ICTRP)*
■ *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*
■ *מערך הסייבר הלאומי*
■ *NATO Cooperative Cyber Defence Center of Excellence*
■ *US Department of Homeland Security – Cybersecurity Division*
■ *GFCE Cybersecurity Capacity Portal*

Grading Scheme:
Essay / Project / Final Assignment / Home Exam / Referat 95 %
Presentation / Poster Presentation / Lecture/ Seminar / Pro-seminar / Research proposal 5 %

Additional information:
Students are eligible for an additional (maximum) 5 bonus points for presenting their legal analysis of a cyber event to the class.

The final paper is a maximum of 6 pages.