



The Hebrew University of Jerusalem

Syllabus

Israeli and International Cybersecurity Law - 62324

Last update 23-08-2019

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 interesting, substantive, and rapid changes in the normative international and Israeli regimes that apply to states, organizations and individuals in cyberspace. About half of the world's population currently enjoys the benefit of access to cyberspace and operates in it on a daily basis. This is a new human phenomenon that has brought about significant positive results (for example, in the spheres of health, education and law). Nevertheless, the misuse and abuse of cyberspace by hostile elements has become routine: cyberattacks, hacking, data breaches, and other abuses are steadily increasing in number and impact. These phenomena raise many questions concerning the governance of cyberspace, the legal norms that apply, and the implementation and enforcement of them.

In the course participants will analyze the legal and regulatory arrangements in respect of cyber-space, 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 into four units: (1) legal and regulatory regulations that apply in cyberspace both in the international and national arenas, (2) cyber law and policy in Israel, (3) 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 (4) 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 the end of the course a moot court will be held in which the main issues we have studied will be examined (10% of the final grade).

Course/Module aims:

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

- To impart to the participants an understanding of the basic concepts of state and

non-state activity in cyber-space

- 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.

Attendance requirements(%):

For students' attention: The moot court exercise at the end of the course allows a grade of up to 10% in the final course grade.

Teaching arrangement and method of instruction:

Course/Module Content:

62324 - דיני סייבר ישראלים ובינלאומיים

עו"ד דב האוסן-כוריאל (com.cyberregstrategies@deborah)

סמסטר א', יום ב', בין השעות 14:00-15:30 חדר -משפטים 310

(1) תיאור כללי של הקורס

התחום המתפתח של דיני סייבר מתאפיין ע"י שינויים מרתקים, מהותיים, ומהירים - הן בישראל והן במישור הבינלאומי. החל משנת 2018, יותר ממחצית מאוכלוסיית העולם מחוברת למרחב הסייבר ופועלת בו באופן שוטף. מדובר בתופעה אנושית חדשה, המניבה תוצאות חיוביות (למשל, בתחומי הבריאות, החינוך, והמשפט). יחד עם זאת, מתקיימות תופעות של ניצול לרעה של המרחב על ידי גורמים עויינים: מדינות, חברות, קבוצות ויחידים.

הקורס יעסוק בהסדרה המשפטית והרגולטורית של המרחב במציאות מורכבת זו. הקורס בוחן את תהליכי ההתפתחות של דיני הסייבר והסדרי המשילות (governance) השונים הקיימים בו: אמנות, מנגנוני התנהגות מוסכמת (conduct of codes), והסדרים אחרים. בנוסף, נבחן את מערכת המשפט הישראלית שחלה על הפעילות במרחב והמתפתחת כעת. כמו כן, הקורס בוחן את יחסי הגומלין בין דיני הסייבר של ישראל והמערכת הנורמטיבית הבינלאומית שחלה במרחב.

תוכנית הקורס בנויה מארבעה פרקים: (1) הסדרים משפטיים ורגולטוריים החלים במרחב במישור הבינלאומי והלאומי, (2) דיני סייבר בישראל, (3) המאזן בין שיקולי בטחון לבין זכויות הפרט במרחב, ו-(4) מגמות משפטיות במרחב במישור הבינלאומי והישראלי. במסגרת פרקים אלה, ננתח סוגיות משפטיות מרכזיות והשלכותיהן, כגון מתקפות סייבר על תשתיות קריטיות; פריצת אתרים ומאגרי מידע, פשע וטרור מקוון; שימוש ביכולות האינטרנט על ידי גורמי טרור; ומנגנוני שיתוף פעולה בינלאומי לאכיפת דיני הסייבר. לקראת סיום הקורס ייערך משפט מבויים בו יבחנו הסוגיות העיקריות שנלמדו.

(2) מטרות הקורס

- להציג בפני המשתתפים הבנה של מושגי היסוד של הפעילות המדינתית והלא-מדינתית במרחב הסייבר;
- להציג בפניהם את המערכות הנורמטיביות העיקריות שחלות על הפעילות האמורה במישור הבינלאומי והישראלי;
- להקנות למשתתפים מגוון כלים מקצועיים בהם יוכלו לעשות שימוש בפרקטיקה, לרבות יכולת ניתוח של התפתחויות שוטפות במרחב הסייבר בעלי השלכות משפטיות ורגולטוריות;
- להטמיע בקרב המשתתפים את היכולת לזהות ולנתח את התפיסות האידיאולוגיות והמתודולוגיות השונות שחלות על הסדרת מרחב הסייבר; ובתוך כך, התפיסה הישראלית להסדרתו;
- לנתח את החולשות שביישומם של דיני הסייבר הבינלאומיים והישראליים; ולעודד חשיבה ביקורתית על דיני הסייבר ויישומם.

(3) סילבוס וחומרי קריאה

שיעור 1 (28.10.2019) - מרחב הסייבר כמרחב פעילות מדינתית ולא-מדינתית חדשה: היבטים משפטיים ראשוניים ומושגי יסוד
נק' עיקריות - הגדרת מרחב הסייבר, היכרות עם אתגרים נורמטיביים במרחב הסייבר, היקף וסוג השימוש באינטרנט, היכרות עם פעולות לוחמה במרחב הסייבר והתגובות להן

(א) *and Technology Cyber, Innovation Governance International for Centre (video)*, *International Security*, April 2019.

(ב) *May) CCDCOE, cyberspace for law international in Trends, Branch Law CCDCOE* (2019).

(ג) אסטרטגיית צה"ל, אוגוסט 2015 (איזכורי "סייבר", במיוחד עמ' 27, 28, 30)

(ד) כתבה של מבט על הפריצה (לכאורה) של צפון קוריאה לשרתי חברת סוני

(ה) אתר *Tracker Operations Cyber* של ה-*Relations Foreign on Council*

(ו) (רשות) *Collateral Cyber Understanding, Goldman Zachary and Romanosky Sasha* (2017) *Damage, 9 J. Nat'l Sec. L. & Pol'y* 233

(ז) (רשות) רון שמיר ואלי בכר, "התקפות סייבר על מערכת הבחירות - איך מתמודדים?" מחקר

מדיניות 136, המכון הישראלי לדמוקרטיה ומרכז פדרמן לחקר הסייבר (פברואר 2019), עמ' 18-37

(ח) (רשות) בחירות 2019: בחירות בצל מתקפת סייבר, פודקאסט של המכון הישראלי לדמוקרטיה (מרץ 2019).

יחידה א': הסדרים משפטיים ורגולטוריים החלים במרחב במישור הבינלאומי והלאומי

שיעור 2 (4.11.2019) - פיתוח הסדרים נורמטיביים במרחב במישור הבינלאומי והלאומי: מבט על

נק' עיקריות - ריבוי שחקנים בתהליכים הנורמטיביים, גישות שונות להסדרה נורמטיבית של מרחב

הסייבר, יוזמות נורמטיביות רב-צדדיות להסדרה.

Cyber International to Introduction", Roigas Henry and Osula Maria-Anna (א) Norms", in Osula and Roigas (eds.), International Cyber Norms, CCDCOE, 2016, pp. 11-22

7.8.2011 (ב) החלטת ממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי", (ג) ד. האוסן-כוריאל, "דיני הטלקומוניקציה הבינלאומית ודיני סייבר בינלאומיים", מתוך רובי סייבל ויעל רונן (עורכים), משפט בינלאומי (מהדורה שלישית), נבו, 2016, עמ' 615-630.

Global for Norms Constructing", Hollis Duncan and Finnemore Martha (ד) Cybersecurity", The American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479

on Progress Enabling :Implementation to Articulation From ,Microsoft (ה) (רשות) Cybersecurity Norms, June 2016, The Need for a Digital Geneva Convention, February 2017, and Establishing an International Cyberattack Attribution Organization to Strengthen Trust Online

French ,Cyberspace in Security & Trust for Call Paris The :Brief In (Video) (ו) (רשות) Ministry for Europe and Foreign Affairs (November 2018),

Kubo .Dr by Juris Opinio on Silence and Norms Cyber -CyCon (ז) (רשות) סרטון מכנס Macak

שיעור 3 (11.11.2019) - משילות באינטרנט

נק' עיקריות - האינטרנט כחלק ממרחב הסייבר, הגורמים המעורבים במשילות, התפתחויות בנושא, המודל הנכון למשילות.

(א) מהי משילות האינטרנט? איגוד האינטרנט הישראלי.

California A ,Numbers and Names Assigned for Corporation Internet for Bylaws (ב) Nonprofit Public-Benefit Corporation (as amended 18 June 2018).

Dutton William in , "Governance Internet of Field Emerging The" ,DeNardis Laura (ג) (ed.), The Oxford Handbook of Internet Studies, Oxford University Press, 2013, pp. 555-575

2014 ,24 April ,Statement Multistakeholder NETmundial (ד)

Fletcher 41 ,Governance Internet in Leadership of Role The ,Sepulveda .A Daniel (ה) F. World Aff. 129 (2017)

Free a Promote Can Europe How ,Hohmann Mirko and Benner Thorsten (ו) (רשות) and Open Internet, Net Politics, June 27, 2018.

,E-28 .Doc ,1.Rev ,Conference the of Work the for Proposal ,Israel of State (ז) (רשות) World Conference on International Telecommunications (WCIT-12) Dubai, 3-14 December 2012

שיעור 4 (18.11.2019) - הסדרים בין-מדינתיים נבחרים במרחב

נק' עיקריות - הסדרים בין-מדינתיים נבחרים במרחב הסייבר

:Cooperation Regional via Cyberspace Secure a Towards” ,Radunovic Vladimir (א) Overview of the Main Diplomatic Instruments”, Diplo Foundation, 2017
of Field the in Developments on Experts Governmental of Group the of Report (ב) Information and Telecommunications in the Context of International Security, A/70/174, 22.7.2015, pp. 6-14.
working two creates UN :events of turn surprising A ,Colatin Tomas De Samuele (ג) groups on cyberspace, NATO CCD COE Law Branch (2018); UN General Assembly resolution ref. A/C.1/73/L.37; UN General Assembly resolution ref. A/C.1/73/L.27/Rev.1.
for Conduct of Code International ,Organization Cooperation Shanghai (ד) Information Security, 9 January 2015
22,35 ,1-6 Articles ,2001 ,185 ETS ,Cybercrime on Convention ,Europe of Council (ה)

rapid cyber PESCO on declaration sign states EU Six ,Varfolomeeva Anna (ו) (רשות) response, The Defense Post (June 2018).
Increasing ,Lukyanov Fyodor and Demidov Oleg ,Chernrnko Elena (ז) (רשות) International Cooperation in Cybersecurity and Adapting Cyber Norms, Council on Foreign Relations, February 23, 2018.

שיעור 5 (25.11.2019) - 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

(א) רע"א 5860/16 Inc Facebook נ' אוהד בן חמו (31.5.2018).
Applicable Law International the on 2.0 Manual Tallinn ,(ed) Schmitt .N Michael (ב) 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)

Tallinn the of Launch - Operations Cyber and Law International (video) (ג) (רשות) Manual 2.0 , Atlantic Council, February 8, 2017
-Law as States engaging-Re :Rules Cyber to Norms Cyber From” ,Macak Kubo(ד) makers”, 30 Leiden Journal of International Law 2017

שיעור 6 (2.12.2019) - השימוש בכוח, הגנה עצמית ודיני המלחמה במרחב הסייבר: מדריך טאלין 0.2 (חלק ב')
נק' עיקריות - החלת דיני מלחמה במרחב הסייבר

Applicable Law International the on 2.0 Manual Tallinn ,(ed) Schmitt .N Michael (א) to State Activity in Cyberspace, Cambridge, 2017, Rules 68-75 (pp. 328-356)
Law International the on Manual Tallinn The of Review” ,Eichensehr Kristen (ב) Applicable to Cyber Warfare”(Michael N. Schmitt ed., 2013)”, 108 American Journal

of International Law 585 (2014)

on 2.0 Manual Tallinn ?Shelf the on Book Rule A ,Efroni Dani and Shany Yuval (ג)
Cyberoperations and Subsequent State Practice, AJIL Vol. 112, pp. 583-657 (2018)

.2018 ,Summary ,Strategy Cyber ,Defense of Department US (ד)(רשות)
AJIL ,Cyber of Age the in Sovereignty ,Taylor Robert and Corn .P Gary (ה) (רשות)
Unbound, Volume 111) 2017 , pp. 207-212.

יחידה ב': דיני סייבר בישראל

שיעור 7 (9.11.2019) - דיני סייבר ישראלים: התפתחות הדין הישראלי במרחב הסייבר
נק' עיקריות - בחינה ראשונית של ההסדרה של מרחב הסייבר בישראל; תזכיר חוק הגנת הסייבר
ומערך הסייבר הלאומי

(א) גבי סיבוני ועידו סיון-סביליה, "רגולציה במרחב הסייבר", מזכר INSS 180 (אוגוסט 2018), עמ'
79-91.

(ב) החלטת ממשלה 3611, "קידום היכולת הלאומית במרחב הקיברנטי", 7.8.2011,
(ג) החלטת ממשלה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת סייבר" והחלטת ממשלה
2444 "קידום ההיערכות הלאומית להגנת הסייבר", 15.2.2015

(ד) היערכות גופים חיוניים להגנת הסייבר, דו"ח 69 של מבקר המדינה (מאי 2019).
(ה) תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018

(ו) (רשות) Chief Cyber National Outgoing :Companies Israeli on Attacks Monthly 150
Jerusalem Post, June 28, 2018.

(ז) (רשות) כיצד ישראל הפכה למעצמת הגנת סייבר? סרטון דוקומנטרי קצר של HBO
(ח) בזק, דו"ח החיים הדיגיטליים, 2018

שיעור 8 (16.12.2019) - דיני סייבר ישראלים: הסדרת מקצועות הסייבר ותפיסת הרגולציה המגזרית
(מרצה אורח - יובל שגב, מערך הסייבר הלאומי)

נק' עיקריות - התפיסה הרגולטורית המגזרית לצד הגדרת תשתיות חיוניות וההגנה עליהן בישראל

(א) מדיניות אסדרת מקצועות הסייבר, מטה הסייבר הלאומי, 31.12.2015

(ב) בנק ישראל, חוזר 361, "ניהול הגנת סייבר", מרץ 2015

(ג) המפקח על שוק ההון, החזון הדיגיטלי וחוזר "ניהול סיכוני סייבר בגופים מוסדיים", אוגוסט 2016

(ד) מטה הסייבר הלאומי, "מדיניות לאומית בנושא הפיקוח על ייצוא בתחום הסייבר", אפריל 2016
עדכון בדצמבר 2016

(ה) משרד האוצר, מעבדת סייבר חדשה תוקם בבאר שבע בתחום הפינטק-סייבר בהשקעה של 15
מיליון ₪ (אפריל 2018)

(ו) (רשות) הרשות הלאומית להגנת הסייבר, "עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות
עם איומי סייבר", 2015

(ז) (רשות) אלדד הבר וטל ז'רסקי, "דרכי ההגנה על תשתיות חיוניות במרחב הסייבר בישראל" משפט
וממשל, כרך י"ח, תשע"ז (2017).

שיעור 9 (23.12.2019) - דיני סייבר ישראליים: פשע מקוון וטרור מקוון
נק' עיקריות -חקיקה שנוגעת לפשע המקוון בישראל והיבטי אכיפתה; ישראל ואמנת בודפשט, הסדרת
טרור מקוון בעולם ובהקשר של חוק המאבק בטרור - התשע"ו-2016

(א) אסף הרדוף, הפשע המקוון, נבו, 2010, "מבוא" (עמ' 21-30).
(ב) חוק המחשבים, תשנ"ה-1995.
(ג) חוק להסדרת ביטחון בגופים ציבוריים, תשנ"ח-1998.
(ד) חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז-2017.
(ה) חוק המאבק בטרור, התשע"ו - 2016 (סעיף 2, הגדרת "מעשה טרור").
(ו) חיים ויסמונסקי חקירה פלילית במרחב הסייבר, נספח - רקע על ארכיטקטורת האינטרנט, בעמ'
337-339 (2015).

(ו) (רשות) עמיר פוקס, "טרור ופרטיות: הצעה לחשיבה מחודשת על הכלים להתמודדות עם פעילות
טרור באינטרנט", פרטיות בעידן של שינוי (תהילה שוורץ אלטשולר עורכת, 2012), עמ' 247-254.
(ז) (רשות) עפג (י-ם) 35557-03-17 מדינת ישראל נ' סאלח זגארי.
(ח) (רשות) Fidler David, "in Terrorism and Law Terrorism-Counter New s'Israel", NetPolitics, Aug 22, 2016
Cyberspace".

יחידה ג': המאזן בין שיקולי בטחון לבין זכויות הפרט במרחב

שיעור 10 (30.12.2019) -בטחון סייבר במישור הגלובלי והלאומי בעידן הפוסט-סנודן; הסדרת זכויות
הפרט והמדיה החברתית במרחב הישראלי
נק' עיקריות - הצורך באיזון בין סמכויות המדינה לצרכי בטחון ובין זכויות הפרט במרחב; היבטים
משפטיים של ניטור אזרחים ע"י הממשלה; מהי "המדינה האלגוריתמית"?

(א) Snowden Edward, "Internet the Back Take We How s'Here", TEDTalks (video), March 2014
(ב) Policy Data -Facebook
(ג) al et Abelson Harold, "Requiring by Insecurity Mandating :Doormats Under Keys", Journal of Cybersecurity,
Government Access to All Data and Communications", 2015, pp. 1-4 (until "Findings...")
(ד) דו"ח בסימוכין 34/60/HRC/A של דווח האו"ם על הזכות לפרטיות בנושא מעקב ממשלתי למול
הזכות לפרטיות, ספטמבר 2017.

(ה) (רשות) Kang Cecilia, "Altered of Handling for Facebook Criticizes Pelosi Nancy", The New York Times (May 2019).
(ו) (רשות) "Protocol Ghost" regarding GCHQ s'UK to Letter Open (2019 May).
(ז) (רשות) יניב קובוביץ, עתירה: תוכנת הריגול הישראלית פגסוס שימשה למעקב אחר פעילי אמנסטי,
מאי 2019.
(ח) (רשות) ראיון של ג'ון אוליבר עם אדוארד סנואדן, החל מדקה 14:08 בסרטון. תחילתו של הסרטון
גם היא מעניינת ונוגעת במעקב ממשלתי אחר אזרחים.

effects chilling and ,regulation ,surveillance Internet” ,Penney Jonathon (רשות) (ט) online: a comparative case study”, *Internet Policy Review*, 26 May 2017.

שיעור 11 (6.1.2020) - הגנת מידע אישי כמרכיב בהגנת סייבר
נק' עיקריות - הסדרי הגנת מידע פרטי באיחוד האירופי וישראל

(א) *12-23 and 1-4 Articles ,2016 ,27 April ,Regulation Protection Data General EU Case ,(Summary) Judgement ,Commissioner Protection Data .v Schrems (ב) C-362/14, European*

(ג) תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017, סעיפים 1-3, 13, 14, תוספת ראשונה.
(ד) היבטים בהגנה על פרטיות במאגרי המידע, דו"ח שנתי 69 של מבקר המדינה (מאי 2019), עמ' 17-27.

(ה) (רשות) *Relationship the On :Frontiers without Protection Data ,Ukrow Jorg between EU GDPR and Amended CoE Convention 108, 4 Eur. Data Prot. L. Rev. 239 (2018)*

(ו) (רשות) *,court in you against testify can Fitbit and Alexa Your ,Reardon Marguerite CNET (April 5, 2018).*

יחידה ד': השפעתן של התפתחויות טכנולוגיות על מגמות משפטיות במרחב

שיעור 12 (13.1.2020) - משפט מבויים כיתתי (10% מהציון הסופי)
חומר נוסף יחולק לקראת המשפט המבויים

(א) *Cybersecurity” in Compromised Data Account MyHeritage ,Offord Catherine Incident”, The Scientist (June 6, 2018).*

(ב) *.Discuss s’Let .Security Cyber & Blockchain ,Deloitte (2017)*

שיעור 13 (20.1.2020) - מגמות בפיתוח דיני הסייבר במישור הבינלאומי והישראלי (חלק א')
נק' עיקריות - טכנולוגיות חדשות והשפעתן על מגמות רגולטוריות; שימוש ברגולציה לפגיעה בשרשרת האספקה

(א) *Warfare Influence/Information Enabled-Cyber On ,Kerr Jackie and Lin Herbert and Manipulation (August 2017 version).*

(ב) *Be Elections Should :Hack to Harder Democracy Making” ,al et Shackelford Scott Classified as ‘Critical Infrastructure?’”, 50 University of Michigan Journal of Law Reform, Vol. 3, 2017.*

(ג) *PaxAmericana ,Space Without Day A*

(ד) (רשות) *“Cybersecurity Strengthening” ,Law International of Society American (video), July 17, 2017.*

שיעור 14 (27.1.2020) - מגמות בפיתוח דיני הסייבר במישור הבינלאומי והישראלי (חלק ב')
נק' עיקריות - טכנולוגיות חדשות והשפעתן על מגמות רגולטוריות; שימוש ברגולציה לפגיעה בשרשרת
האספקה

(א) יוסי הרטוב, "מערך הסייבר הקים מערכת להגנה על שרשרת האספקה במשק", אנשים ומחשבים,
8.1.2019.

(ב) מערך הסייבר הישראלי, גרסה 1.1 של שאלון הספקים לחיזוק שרשרת האספקה, 28.6.2018.
(ג) Giles Martin, *Five emerging cyber threats to worry about*, MIT Technology Review (January 2019).

(ד) Newman Hay Lily, *Can AI Cybersecurity Help Fight Through Hype*, WIRED, April 29, 2018.

(ה) *Securing the Order Executive Communications and Information Technology and Services Supply Chain* (May 2019),

Required Reading:

PLEASE REFER TO SYLLABUS ABOVE AND/OR 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
- 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
- Cybersecurity Capacity Portal

Course/Module evaluation:

End of year written/oral examination 90 %

Presentation 0 %

Participation in Tutorials 0 %

Project work 0 %

Assignments 0 %

Reports 0 %

Research project 0 %

Quizzes 0 %

Other 10 %

Moot court

Additional information: