The Hebrew University of Jerusalem

Syllabus

Cybersecurity: Prevention and Regulation of Cybe - 48429

Last update 08-04-2018

HU Credits: *3*

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

Responsible Department: *program for undergraduate students &#41y/s&#40*

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:

DeNardis, L. (2014). Controlling internet resources. In L. DeNardis (Ed.), The global war for internet governance (pp. 33-62). CT: Yale university press.

Mueller, M.L. (2010). Critical internet resources. In M.L. Mueller (Ed.), Network and states: The global politics of internet governance (pp. 215-252). MA: MIT press.

Take, I. (2012). Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS. Regulation & Governance, 6, 499–523 doi:10.1111/j.1748-5991.2012.01151.x

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

Tabansky, L. & Ben Israel, I. (2015). Cybersecurity in Israel. NY: Springer

Cohen M.S., Freilich C.D. and Siboni G. (2015). Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, Volume 17, Issue 3, Pages 307–321, https://doi.org/10.1093/isp/ekv023

Grabosky P. (2001). Virtual criminality: old wine in new bottles? Social and Legal Studies,10(2): 243-249.

Grabosky P. (2014). The Evolution of Cybercrime, 2004- 2014. RegNet Working Paper, No. 58, Regulatory Institutions Network.

Yar M. (2005). The Novelty of "Cybercrime": an assessment in light of routine activity theory. European Journal of Criminology, 2: 407-427.

Bossler, A., & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. Journal of criminal Justice, 38: 227-236.

Shalhoub-Kevorkian, N., & Berenblum, T. (2010). Panoptical web: internet and victimization of women, International Review of Victimology 17: 69–95.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. Journal of Contemporary Criminal Justice, 29(4), 475-497.

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

Turns D. (2012). Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict & Security Law. Oxford University Press 2012. https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Turns.pdf

Droege C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross. Volume 94 Number 886. https://www.icrc.org/eng/assets/files/review/2012/irrc-886-droege.pdf

D. Housen-Couriel, "The Evolving Law on Cyber Terrorism: Dilemmas in International Law and Israeli Law" ICT Working Paper, 25 March 2013.

Goodman S.E., Seymour E., Kirk J.C. and Kirk M. H. (2007). Cyberspace as a medium for terrorists. Technological Forecasting and Social Change. 74(2): 193-210

Khan, J., Huey, L., & Broll, R. (2017). Digitalism: an Analysis of crowdsourcing and the Boston marathon bombing. British Journal of Criminology, 57: 341-361.

Don’t Panic Making Progress on the “Going Dark” Debate. February 1, 2016, Berkman Center for Internet & Society at Harvard University Https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

The Global Surveillance Industry, A report by Privacy International July 2016. https://privacyinternational.org/sites/default/files/global_surveillance_f.pdf

*Powers, S. M. &
Jablonski, M. (2015). Google, information and Power. In S. M. Powers & M. Jablonski (Eds.), The real cyber war: the political economy of Internet Freedom (pp.74-98). IL: University of Illinois Press*

Birnhack M.D., and Elkin-Koren N. (2009). "Does Law Matter Online? Empirical Evidence on Privacy Law Compliance". Available at SSRN: http://ssrn.com/abstract&eq;1456968

Mulligan D.K. and King J. (2012). Brifging the gap between privacy and design. Journal of Constitutional Law 14:4

Egelman S., Felt A. P., and Wagner D. (2012). Choice Architecture and Smartphone Privacy: There’s A Price for That. Springer.

Brignal T. (2002). The new Panopticon: the internet viewed as a structure of social control". Theory and Science, 3(1): 1-13.

Barzilai-Nahon K. (2008). "toward a Theory of Network gatekeeping: A Framework for Exploring Information Control", Journal of the American Information Science and Technology, 59(9): 1-20.

Goldsmith, J., & Wu, T. (2008). Who controls the internet? Illusions of a borderless world. New York: Oxford University Press.

Huey, L., Nhan, J. and Broll, R. (2012), ‘Uppity Civilians’ and ‘Cyber-Vigilantes’: The Role of the General Public in Policing Cyber-Crime, Criminology & Criminal Justice, 13: 81–97

Lessig, L. (2006). Code: Version 2, Ney-York: Basic Books.

McQuade III, Samuel C. 2006. Understanding and Managing Cybercrime chapter 8.

Michael N. Schmitt and Liis Vihul, “The Nature of International Law Cyber Norms”, in Anna-Maria Osula and Henry Roigas (eds.), International Cyber Norms, CCDCOE, 2016

Walker D., Brock D., and Stuart T.R. (2006). Faceless-Oriented Policing: Traditional

Policing Theories Are Not Adequate in a Cyber World. The Police Journal, 79: 169-176.

Wall S.D. (2007). Policing cybercrimes: situating the public police in networks of security within cyberspace. Police Practice and Research: An International Journal, 8(2): 183-205.

Schneider, C., & Trottier, D. (2011). The 2011 Vancouver riot and the role of Facebook in crows-sourced policing. CB Studies, 175: 57-72.

Maimon D., M. Alper, B.Sobesto and M.Cukier. (2014). Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System. Criminology 52(1): 33-59

Maybaum M. Technical methods, techniques, tools and effects of cyber operations.In
Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013.
https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf

Çalışkan E. & Peterson R. Technical Defence methods, tools, techniques and effects.

In: Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013.
https://www.ilsa.org/jessup/jessup16/Batch%202/Peacetime-Regime.pdf

Maimon, D., Wilson, T., Ren, W., & Berenblum, T., (2015). On The Relevance of Spatial and Temporal Dimensions in Assessing Computer Susceptibility to System Trespassing Incidents, British Journal of Criminology.

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: