

Program	Leaders at Work
Course title	Cyber Threats and the modern organization
Number of ECTS	4
Language of Teaching	English
Year and semester	Spring 2023
Lecturer name	Dr. Tal Pavel
Lecturer telephone	052-525-8985
Lecturer email	Talpv@mta.ac.il
Office hours	After session, by appointment

Course Details:

Course description	<p>The course deals with cyberspace and focuses on challenges for the country, the organization, and the individual while emphasizing the existing threats in the modern era and the ways to confront them.</p> <p>The course will first examine basic concepts related to cyberspace, followed by an examination of the various actors and the threats they pose, at the levels of the state, the organization, and the individual. We will discuss the challenges facing the participants in cyberspace and the ways to confront them. Finally, we will summarize and try to draw the future concerning threats and challenges in cyberspace.</p>
Learning Outcomes	<p>The students will be able to understand basic features of the Internet and cyberspace,</p> <p>To explain the major actors in cyberspace, the differences and uniqueness of each actor,</p> <p>To analyze nation-states actors' motivations and activities,</p> <p>To understand what Hacktivism is and who are its main represents.</p>

	To analyze the usage of the Internet and Cyberspace by terrorists' activists and organizations.			
Teaching Methods	On-site lectures			
Assignments and Requirements	Final exam			
Grade composition	Final exam – 100%			
Work Parameters (Per week-13 weeks)	Contact hours in lecture form	Assignments (hours)	Reading (hours)	Self-Study (hours)
	2	2	2	2
Attendance	<p>Students must attend 80% of the sessions.</p> <p>Unexcused absences exceeding 20% (more than 3 during the semester) will result in an “incomplete” grade in the course.</p>			

Course Plan - Weekly Topics

Session No.	Date	Topic	Reading / Assignments
1	6 March 2023	Introduction to the Internet and Cyberspace	Baezner, M., & Robin, P. (2018). Cyber sovereignty and data sovereignty (No. 2). ETH Zurich.
2	13 March 2023	Social engineering	Francois Mouton, Louise Leenena, H.S. Venterb, " Social engineering attack examples, templates and scenarios ", Computers & Security Volume 59, June 2016, Pages 186–209.
3	20 March 2023	APTs – Definitions	Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks . California, Estados Unidos: FireEye.
4	27 March 2023	APTs – Iran, Russia, China, North Korea	Baezner, M. (2019). Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions . ETH Zurich.
5	17 April 2023	Cyber crime	Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime .
6	24 April 2023	Hactivism and Anonymous	Romagna, M., & van den Hout, N. J. (2017, October). Hactivism and website defacement: motivations, capabilities and potential threats . In 27th Virus Bulletin International Conference (Vol. 1).

7	1 May 2023	Wikileaks	Di Salvo, P. (2020). WikiLeaks: An Inspiration, a Reference, a Model? . In Digital Whistleblowing Platforms in Journalism (pp. 137-153). Palgrave Macmillan, Cham.
8	8 May 2023	The Dark web	Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study . Security Journal, 32(2), 102-118.
9	15 May 2023	Introduction to terrorism	Stohl, M. (2020). Introduction: demystifying terrorism: the myths and realities of contemporary political terrorism . In The politics of terrorism (pp. 1-28). CRC Press.
10	22 May 2023	Terrorism and the Internet	Ramsay, Gilbert. " Terrorist' Use of the Internet: An Overblown Issue ." <i>Middle East-Topics & Arguments</i> 6 (2016): 88-96.
11	29 May 2023	Right-wing lone wolves	J.M Berger, " The Dangerous Spread of Extremist Manifestos ," <i>The Atlantic</i> , 26 February 2019.
12	5 June 2023	Fake news	Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda . <i>Annals of the International Communication Association</i> , 43(2), 97-116.
13	12 June 2023	Cyber and international relations	Demir, İ. (2018). CYBER CHALLENGE: DIMINISHING POWER OF THE STATE IN INTERNATIONAL RELATIONS . <i>Cyberpolitik Journal</i> , 3(5 & 6), 35-46.

Required Reading List and Additional Sources:

Baezner, M., & Robin, P. (2018). Cyber sovereignty and data sovereignty (No. 2). ETH Zurich.
Pfaffenberger, B. (2000). The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing . <i>Knowledge, Technology & Policy</i> , 13(3), 78-92.
Francois Mouton, Louise Leenena, H.S. Venterb, " Social engineering attack examples, templates and scenarios ", Computers & Security Volume 59, June 2016, Pages 186–209.
Geenens, P. (2020). How worried should you be about nation-state attacks? . <i>Network Security</i> , 2020(3), 17-19.
Baezner, M. (2019). Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions . ETH Zurich.
Lutz, J. M., & Lutz, B. J. (2019). Global terrorism. Routledge. Chapter 8 - Terrorism and Ideologies of the Right
Ramsay, Gilbert. " 'Terrorist' Use of the Internet: An Overblown Issue ." <i>Middle East-Topics & Arguments</i> 6 (2016): 88-96.
Ingram, Haroro J. " The Strategic Logic of Islamic State Information Operations ." <i>Australian Journal of International Affairs</i> 69.6 (2015): 729-52.
Klausen, Jytte. " Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq ." <i>Studies in Conflict & Terrorism</i> 38.1 (2015): 1-22.
Mazi, H., Arsene, F. N., & Dissanayaka, A. M. (2020, April). The influence of black market activities through dark web on the economy: a survey . In The Midwest Instruction and Computing Symposium.(MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin.
Mikhaylova, G. (2014). The "anonymous" movement: Hacktivism as an emerging form of political participation (Unpublished thesis). Texas State University, San Marcos, Texas.

Optional Reading List and Additional Sources:

Pym, D. (2018). The origins of cyberspace .
Romagna, M., & van den Hout, N. J. (2017, October). Hacktivism and website defacement: motivations, capabilities and potential threats . In 27th Virus Bulletin International Conference (Vol. 1).
Hayes, Adam. " Is Bitcoin Funding ISIS? " <i>Investopedia</i> . Nov. 24, 2015.
Charleston Church Shooting, " Dylann Roof Documentary Charleston Church Shooting ," YouTube, 11 November 2018.

J.M Berger, " The Dangerous Spread of Extremist Manifestos ," <i>The Atlantic</i> , 26 February 2019.
Ravndal, J. A., " The Dark Web Enabled the Christchurch Killer ," <i>Foreign Policy</i> , 16 March 2019.
Federal Bureau of Investigation, Anti-Government, Identity Based, and Fringe Political Conspiracy Theories Very Likely Motivate Some Domestic Extremists to Commit Criminal, Sometimes Violent Activity , 30 May 2019.
Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks . California, Estados Unidos: FireEye.
Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study . <i>Security Journal</i> , 32(2), 102-118.
Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime .
Di Salvo, P. (2020). WikiLeaks: An Inspiration, a Reference, a Model? . In <i>Digital Whistleblowing Platforms in Journalism</i> (pp. 137-153). Palgrave Macmillan, Cham.
Stohl, M. (2020). Introduction: demystifying terrorism: the myths and realities of contemporary political terrorism . In <i>The politics of terrorism</i> (pp. 1-28). CRC Press.
Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: A framework and research agenda . <i>Annals of the International Communication Association</i> , 43(2), 97-116.
Demir, İ. (2018). CYBER CHALLENGE: DIMINISHING POWER OF THE STATE IN INTERNATIONAL RELATIONS . <i>Cyberpolitik Journal</i> , 3(5 & 6), 35-46.