TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Full Syllabus

Course Title

Introduction to Cyber Events Readiness and Response

Lecturer

Niv David nivd@tauex.tau.ac.il

Semester

Summer 2023

Course requirements

Is the world ready for digital information disruption? A disruption that can grow to become a full-scale cyber warfare? Can countries face a digital attack on national, public, security, and business information systems and critical infrastructure? Are countries prepared to prevent and contain a variety of cyber threats in a way that will allow for the continuation of proper conduct of life systems in the country? Can our new 'digital global village' survive a cyber warfare attack?

Over the past two decades, the cyber threat has taken on an entirely new dimension and is now attributed as one of the most critical threats in the world. It includes all types of information infrastructures, social networks, national information assets, financial industries and commerce, business and commercial entities, security information assets and any entity that holds various types of information, including the private individual who currently holds significant digital information for his personal needs.
Today, our world experiences daily cyber-attacks on many information infrastructures for various purposes which can and do significantly harm countries in every sector. In our growing digital world, the cyber threat will increase and its power presents a particularly significant challenge for understanding and addressing.

Course Objectives:
This course aims to emphasize the cyber-security issues, technological and international dilemmas, policy initiatives and emerging doctrines. The course offers special focus on assessment, preparations and readiness for cyber events before they happen, and mitigation procedures once they do.
The goals of this course are to provide students with the understanding of definitions and meanings of the cyber strategy, threat and risk perception and crisis management of a local or widespread cyber event. The course will include a table-top exercise for a cyber incident drill and encourage students to experience decision making and cyber leadership.

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Full Syllabus

Students are required to attend all classes (minimum of 75%), read/view/listen to selected bibliography, actively participate in class and simulation and complete a (short) final home exam.

Final grade components

Participation in class – 10%; Final home exam – 90% (to be completed within 48 hours)

Course schedule

Class no. / Date 09:00 – 14:30	Subject and Requirements (assignments, reading materials, tasks, etc.)
20/8/2023 (1)	**The Cyber Phenomenon – Analog Humanity in a Digital World** Is the world ready for digital information disruption? A disruption that can grow to become a full-scale cyber warfare? Can countries face a digital attack on national, public, security, and business information systems and critical infrastructure? Are countries prepared to prevent and contain a variety of cyber threats in a way that will allow for the continuation of proper conduct of life systems in the country? Can our new 'digital global village' survive a cyber warfare attack?
20/8/2023 (2)	**National Critical Infrastructure and Tech Dependency** Protecting critical information infrastructure has become a major goal for governments due to the realization this infrastructure is the basis for running a country and keeping the civilian order. We will review critical infrastructure types, the potential harm of cyber-attacks and governments actions to improve resilience. A special focus will be provided on the healthcare system, disaster management teams and first-responder services as key components of the critical infrastructure.
21/8/2023 (3)	**Fundamentals of Digital Technology** Cyber is not only about technology, but technology is the foundation to modern world infrastructure, operations and administration. We will review the fundamental building blocks of contemporary advanced technologies such as: IT, OT, IOT, Cloud, AI and networking (wired, wireless, cellular, 5G etc.).

	Special focus will be provided on healthcare and first responders related technologies and connectivity.
21/8/2023 (4)	**Cyber weapons, Technological Vulnerabilities, Hacking and Perceptual Manipulation** The "dark side" of technology is its vulnerabilities and the potential dual-use for malicious actions. We will review the threat from key cyber weapons and offensive techniques such as: a. Software development and probability of "bad" code. b. Digital warheads, weaponized code, malware and Ransomware. c. Online attacks vs. Offline attacks. d. Adversarial AI. e. Sophisticated cyber-attacks of the recent decade. f. The Human factor: Misconfigurations, Social Engineering, Phishing and APT (Advanced Persistent Threat).
22/8/2023 (5)	**Cyber Emergencies and Cyber Disasters** Cyber-attacks have become a realistic threat due to the total dependency of organizations and people in technology and data networks. In some scenarios, Cyber-attacks can be devastating in itself and cause a local or national emergency. In addition, it can be part of an ongoing kinetic attack and intensify an existing emergency situation. We will review different scenarios and use cases of cyber emergencies and their impact in various modes of operations.
22/8/2023 (6)	**Information Security and Cyber Risks Management: Public, Commercial, Industrial and National** Information systems have become a critical and integral part of all business, industrial & public processes of any size. Damage or disabling of IT systems may result in the immediate collapse of digital services. We will review key methodologies and technologies that have been developed to evaluate and mitigate cyber risks, quantify cost-effectiveness and criticality, in order to prepare for the worst scenarios via cyber risk management plans.
23/8/2023 (7)	**Cyber readiness – Business Continuity, Resilience and Recovery** The impact of cyber-attacks in recent years has shown that even when all reasonable measures are taken to prepare for cyber events, it is nearly impossible to apply total protection and targeted cyber-attacks can hit any organization, individual or infrastructure. We will review some of the cyber

	defenses, disaster readiness and business continuity practices and methodologies applicable for cyber readiness and how to properly use them for quick recovery.
23/8/2023 (8)	**Cyber Risks and Events Management: A Tabletop Simulation** An active "Wargame" to practice firsthand the potential impact of a cyber-attack and response by different stakeholders. The wargame scenario and full details will be provided the day before and will be finetuned together with the students.

Required course reading

Due the four days intensive nature of the course, there will be minimal mandatory reading only. Specific bibliographic items will be highlighted prior to each lesson.

Optional course reading

General Cyber Background

- Cyberwar Documentary – PBS NOV 2003 and 2016 (links to be provided on Moodle)
- Tabansky, Lior. 2011. "Basic Concepts in Cyber Warfare." Military and Strategic Affairs 3 (1):75-92
- Tabansky, Lior. 2011. "Critical Infrastructure Protection from Cyber Threats." Military and Strategic Affairs 3 (2):61-78

Cyber Attacks, History and Cybercrime

- Economist. New technology has enabled cyber-crime on an industrial scale May 8th ,2021
- Economist. Ransomware highlights the challenges and subtleties of cybersecurity June 19th, 2021
- Goldsmith, M., Creese, S., Agrafiotis, I., Nurse, J. R. C., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4 (1).
- Malicious Life – a podcast about the unknown stories of the history of cybersecurity, with comments and reflections by real hackers, security experts, journalists, and politicians https://malicious.life/
- Long Johnny, No Tech Hacking (Video link to be provided on Moodle)
- The Worst Hacks of 2020, a Surreal Pandemic Year, Wired 2020

Cybersecurity @ Health and Emergency Management Systems

- Cybersecurity for EMS: Combatting The Cyber Kill Chain, https://ambulance.org/2021/02/26/cybersecurity-for-ems-on-demand/
- Hospital under cyber attack - Hillel Yaffe Medical Center, 13.10.2021 https://www.youtube.com/watch?v=50rcfztns1o
- Loukas, George & Gan, Diane & Vuong, Tuan. (2013). A review of cyber threats and defence approaches in emergency management. Future Internet. 5. 205-236. 10.3390/?5020205.
- Madanian, S., Johnson, K., St.Martin, M., Sinha, R., Cámara, J., & Parry, D. (2022). Adaptable socio-cyber physical systems for supporting disaster response. Australasian Journal of Disaster and Trauma Studies, 26, 221-234. https://trauma. massey.ac.nz/issues/2022-IS/AJDTS_26_IS_Madanian. pdf

Cyber Risk Management

- Geer, Dan, Eric Jardine, and Eireann Leverett. "On Market Concentration and Cybersecurity Risk." *Journal of Cyber Policy* 5, no. 1 (2020): 9-29.
- Israel Cyber Defense Doctrine 2.0 https://www.gov.il/en/Departments/General/cyber_security_methodology_2
- Matania, E. & Yoffe, L. & Goldstein, T. (2017) Structuring the national cyber defense: in evolution towards a Central Cyber Authority, Journal of Cyber Policy, 2:1, 16-25
- NIST guide to Cyber events recovery, 2016: NISTIR 8286a, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," 2021

Comments