COURSE SYLLABUS

ISSUES IN CYBERSECURITY FOR STARTUPS

IFSA Tel Aviv

US semester credit hours: 3
Contact Hours: 45
Course Code: SS387-07 / EI387-07
Course Length: Semester
Delivery Method: Face to face
Language of Instruction: English
Suggested cross-listings: Intelligence/Security Studies, Entrepreneurship and Innovation
Associated Host Institution: Academic College of Tel Aviv

COURSE DESCRIPTION

The information age, with the emergence and spread of advanced communication technologies, contributes to significant changes in culture, politics and society, and – most recently—has transformed the world of warfare. This course reviews the cyber are from two perspectives: acts of cyber warfare by state-sponsored hackers and acts of resistance by ideological hackers. Students will examine issues of industrial espionage and consider how cybercrime can impact startups, evaluating methods for securing their new ideas, products and services.

Technological changes have impacted military and security systems and led to the development of new military tactics and technologies. By the end of the course, the students will understand critical differences between cyber warfare and traditional warfare and will have evaluated strategies for protecting their innovations and companies.

COURSE DELIVERY

Primary course delivery is lectures and guest speakers, combined with class discussions of real-life cases, utilizing a theory to practice approach.

Students are expected to read or view assigned resources in advance and be prepared to actively discuss them in class.

STUDENT LEARNING OBJECTIVES

Students who successfully complete this course will:

- Compare concepts of cyber warfare compared to traditional warfare and articulate the difference
- Describe and evaluate methods for protecting innovative ideas, products and services from cyber attack
- Apply security strategies to specific business scenarios
- Strengthen critical thinking skills
- Strengthen written communication skills

COURSE SYLLABUS

- Become familiar with resources available for further research on cybersecurity
- Make cognitive connections between learning in this course and other learning experiences in IFSA Tel Aviv.

COURSE OUTLINE

Session	Subject	Readings
1	Introduction: What is cyber warfare?	Arquilla, J., & Ronfeldt D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: RAND. http://www.rand.org/pubs/monograph_reports/MR1382.html
2-3	The practice of cyber warfare	Saalbach, K. (2013). Cyber war: Method and practice. Osnabruck University, Germany. http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32. Stone, J. (2013). Cyber war will take place. *Journal of Strategic Studies*, *36*(1), 101-108. http://dx.doi.org/10.1080/01402390.2012.730485
4-5	Cyber-weapons & technological & human vulnerabilities	Liff, A. P. (2012). Cyberwar: A new absolute weapon? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35(3), 401-428. Liff, A. P. (2013). The proliferation of cyberwarfare capabilities and interstate war, redux: liff responds to junio. *Journal of Strategic Studies*, 36(1), 134-138. Peterson, D. (2013). Offensive cyber weapons: Construction, development, and employment. *Journal of Strategic Studies 36*(1), 120-124.
6	Hackers: Whitehat, blackhat & in-between	Dahan, M. (2013, January). Hacking for the homeland: Patriotic hackers versus hacktivists. In *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013* (p. 51). Academic Conferences Limited. Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace.* Toronto: McClelland & Stewart.
7-8	Crime, terrorism & deterrence in the cyber era	Glenny, M. (2011). *DarkMarket: Cyberthieves, cybercops, and you*, New York: Random House. Gragido, W., Molina, D., Pirc, J., & Selby, N. (2012). Blackhatonomics: An inside look at the economics of cybercrime. Boston: Syngress.

COURSE SYLLABUS

		Schweitzer, Y., Siboni, G., & Yogev, E. (2011). Cyberspace and terrorist organizations", *Military and Strategic Affairs*, *3* (3), 39-47. Lupovici, A. (2011). Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs*, *3*(3), 49-62. Moore, T. Clayton, R. & Anderson, R. (2009) The economics of online crime. *Journal of Economic Perspectives, 23*(3), 3-20. http://people.seas.harvard.edu/~tmoore/jep09.pdf Steptoe Cyberblog. The Hackback Debate. Nov. 2, 2012. http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/
9-10	Military doctrines & strategies in the cyber era	*The Tallinn Manual on the International Law Applicable to Cyber Warfare*. March 9, 2013. http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 Committee on Deterring Cyber-Attacks (2010). *Proceedings of a workshop on deterring cyberattacks*. National Research Council. http://www.nap.edu/catalog.php?record_id=12997 Ben-Israel, I., & Tabansky, L (2011). An interdisciplinary look at security challenges in the information age. *Military and Strategic Affairs*, *3*(3), 21-37. Owens W. A., Dam, K. W, & Lin, H. S (Eds.) (2009). *Technology, policy, law, and ethics regarding U.S. acquisition, and use of cyberattack capabilities.* Washington, DC: The National Academies Press. Schneider, F., & Mulligan, D. (2011). Doctrine for cybersecurity. *Daedalus* (Fall), 70-92. http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf United States Department of Defense. Department of Defense Strategy for Operating in Cyberspace. July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
11-12	Examples: Stuxnet, the Russia-Georgia War, & the Chinese cyber units	Falliere, N., Murchu, L. O., & Chien, E. W32. Stuxnet Dossier, Version 1.4. February 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Congressional Research Service (2008). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress. http://www.fas.org/sgp/crs/terror/RL32114.pdf

13-14	Summary	PBS documentary on cyberwar

EVALUATION METHODS

Your final grade in the course will be comprised of the following course requirements:

- Final paper – 100%
- Reading the course materials

Students are required to read the course regulations on the College website.

Timely Submissions
Assignments submitted after the deadline will be accepted at the discretion of the course instructor and generally only in the event of a documented illness or emergency.

ACADEMIC INTEGRITY

Any academic endeavor must be based upon a foundation of honesty and integrity. Students are expected to abide by principles of academic integrity and must be willing to bear individual responsibility for their work while studying abroad. Any academic work (written or otherwise) submitted to fulfill an academic requirement must represent a student's original work. Any act of academic misconduct, such as cheating, fabrication, forgery, plagiarism, or facilitating academic dishonesty, will subject a student to disciplinary action.

IFSA takes academic integrity very seriously. Students must not accept outside assistance without permission from the instructor. Additionally, students must document all sources according to the instructions of the professor. Should your instructor suspect you of plagiarism, cheating, or other forms of academic dishonesty, you may receive a failing grade for the course and disciplinary action may result. The incident will be reported to the IFSA resident director as well as your home institution.