TEL AVIV UNIVERSITY
INTERNATIONAL

From Viruses and Trojans to a War Domain – The Evolution of the Cyber Threat

Course overview:

The link between cyberspace and national security is often presented as an unquestionable and uncontested "truth." However, there is nothing natural or given about this link: It had to be forged, argued, and accepted in the political process.

The course will explore the constitutive effects of different threat representations in the broader cyber-security discourse and the evolution of cyber threat, what started as a minor activity of hackers and criminals and become a real war-domain.

It seems that only yesterday the biggest cyber threat was the theft of credit card information. And in fact, only a few years ago when that was indeed the case, and although cyber security was by no means a walk in the park, at least there was a certain simplicity given the relatively small number of aggressors, the unsophisticated attacks and the small number of devices that needed protection.

Today, with the increase in use of digital technologies and the need to become more agile and adaptable, there has been a surge in the number of endpoints and potential ways for cyber aggressors to gain access to their targets.

This potential was recognized by different actors who adopted the new tools and started using them broadly. As a result, the entire cyber world has evolved and is now far more complex: a battlefield and even a war-domain. These changes have a constant effect and thus influence wide aspects: national and international, governmental and private, civilian and military, tactical and strategic, and many more.

The course will explore the evolution of cyber threat, and the effects of different threat representations in the broader cyber-security.

In contrast to previous work on the topic, the focus will not be solely on discursive practices by "visible" elite actors, but also on how a variety of less visible actors shape and influence the evolution of the cyber threat landscape.

The course will consist of lecture and class discussion, covering five modules:

- An introduction to cyber and overview of the history of cyber-attacks, including major events of earlier use of cyber as a weapon.
- The role of cyber as a major tool for Reconnaissance and Intelligence Gathering, its effects and influence on the evolution of cyber as a weapon. Major test cases will be analyzed.

- The third module will deal with the creation of a new cyber based war domain and the different models evolving (for example, the differences between the Russian and the Western models). This module will also include understanding of new concepts, like Cyber Superiority and Cyber Dominance.
- The evolving war domain and threats included are now creating new challenges for the defending side, and national security and strategy. We will describe these changes and challenges and will try to identify and understand them.
- The last module will deal with the potential influence of new and future technologies on the cyber domain, threats and challenges.

Attendance policy: students are allowed to have only one excused absence.
Research Paper: Each student will write a 5-10 page research paper, not including citations, on a cyber as war domain issue of their choice (National, international, technological, strategical or operational focus). The paper should include recommendations for policy makers (national level).
Evaluation criteria : 80% of the grade will be based on the final paper and 20% on attendance and participation.
Recording: Recording of any class session is prohibited.
In-class Laptop Usage: Note-taking during class using personal laptops is permitted.

Required Textbooks / Readings:

1. Matania Eviatar, "Israel – The Making of a Cyber Power – Case Study", Issue brief 5 based on Symposium Fall 2017, George Washington University. https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/DT%20paper%205%20Matania%20issue%20brief%20final.pdf
2. Chris O'Brien, "The evolution of the cyber threat landscape – what's next?", Security 2018
   https://www.itproportal.com/features/the-evolution-of-the-cyber-threat-landscape-whats-next/
3. Jason Andress and Steve Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners", Second edition Elsevier 2014

Recommended Textbooks / Readings:

1. Matania Eviatar, Yoffe Lior and Goldstein Tal, "Structuring the National Cyber Defense: In evolution towards a Central Cyber Authority", Journal of Cyber Policy, 2017, Chatham House.
   https://www.tandfonline.com/eprint/wzru3dWmBnI4n3zQfyEY/full

2. Jeffrey Carr, "Inside Cyber Warfare: Mapping the Cyber Underworld" ,O'Reilly Media 2011.
3. Christopher Bronk, "Hack or attack? Shamoon and the evolution of cyber conflict", James A. Baker III institute for public policy, Rice university, 2013.
4. Heather Harrison, "Cyber Warfare and the Laws of War ", Cambridge University Press 2012.
5. Steve Winterfeld and Jason Andress, "The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice", Elsevier 2012.
6. Pauline C. Reich and Eduardo Gelbstein, "Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization", IGI Global 2012.
7. Nick Ismail, "Securing the future: The Evolution of Cyber Security in the Wake of Digitalization", 2018.

   https://www.information-age.com/evolution-cyber-security-wake-digitalisation-123470747/
8. Sean Collins & Stephen McCombie , "Stuxnet: the emergence of a new cyber weapon and its implications", Journal of Policing, Intelligence and Counter Terrorism, 2012.
9. Nikolai Hampton, "Ransomware: Emergence of the cyber-extortion menace", Edith Cowan University 2015.