**From Waze to Stuxnet – Strategy in the Cyber Era**

**M.A. Course for the INDC – 2020**

**Prof. Eviatar Matania**

School for Political Science, Governance and International Relations

Tel Aviv University

Adjunct Prof. at the School of Government at Oxford University

Founder and Former Head of the National Cyber Directorate (2012-2017)

**Introduction**

We are witnessing a new phenomenon: **The cyber phenomenon**. A phenomenon that began at the very end of the previous century and was created from the almost complete linkage between computer and communication systems, internet access for nearly every person across the globe, the processing speed that allows transferring huge amounts of information, the reduced prices of calculating and memory components and the ability to store information and process it in unimaginable quantities.

All these have caused major changes in the worlds of industry and economy, and in the fabric of life itself, including new kinds of threats (the cyber threat), which influence our lives as a collective, as individuals, as a society and as a state.

The implications of the **cyber phenomenon** may be compared to those of the industrial revolution: As much as the industrial revolution liberated man from the constraints of working with his hands, and influenced humanity with far reaching consequences, so does the cyber revolution free man from a dependency on the physical space, and moves a significant portion of the human activity to the virtual space. Within merely several decades, the world’s biggest companies are companies that specialize in cyber and digital, and not companies of the industrial era. Conflicts take place more and more through social media and computer systems. And this is just the beginning: We are moving very quickly to the development of artificial intelligence technology based on big data, which the ability to reach, shape, analyze and draw insights from that do not appear at any of the data endpoints – this ability is a result of the **cyber phenomenon** – the complete linkage and computing capability.

The problem is that the transverse influence of this phenomenon requires knowledge and information in not only technological disciplines, but also its strategic aspects. Knowledge in these fields is critical for the ability of managers and decision makers in both the public and security spheres to safely lead their work and their organizations in this post-industrial era – the cyber era.

**Academic Objectives of the Course**

1. Expanding your horizon in knowledge of the field of cyber that is not necessarily technological.
2. Developing a systemic view of the cyber threat and cyber defense on all levels – national, sectorial and organizational.
3. Granting tools for leading individuals, companies and governments in the cyber era.

**Lesson Layout:**

Due to constraints of the lecturer, the course will be delivered in only four meetings:

February 26th, 13:00-17:30

March 4th, 13:00-17:30

March 11th, 13:00-17:30

March 18th, 13:00-17:30

**The classes planned for the other two dates, March 25th and April 1st, will not take place.**

 **Participants who choose this seminar will finish at 12:00 on those dates.**

**The Main Modules**

**First Module (Lessons 1 +2) – The Duality of Cyber:**

From the industrial revolution to the era of cyber: New value pyramid – new economy, new threats; space and phenomenon; towards a change in the global powers.

Background material (marked – important reading; unmarked – additional reading):

1. Naughton John, "The Evolution of the Internet: From Military Experiment to General Purpose Technology", Journal of Cyber Policy 1, No. 1 (2016): 5-28. http://dx.doi.org/10.1080/23738871.2016.1157619
2. **Matania Eviatar, "Cyber Generates New Possibilities", Israel Globes (Israel Business Arena), December 2016.**

http://www.globes.co.il/en/article-eviatar-matania-cyber-generates-new-possibilities-1001166640

1. Prince Matthew, **"Why We Terminated Daily Stormer"**, Cloudflare (2017). https://blog.cloudflare.com/why-we-terminated-daily-stormer/

**Second Module (Lesson 3) – Power in Cyber:**

Cyber as a space of warfare, maneuver and fire in cyber, superiority in the cyber space.

Background material (marked – important reading; unmarked – additional reading):

1. **Applegate S., "The Principle of Maneuver in Cyber Operations", 4th International Conference on Cyber Conflict, June 2012, NATO (Tallinn).**

<https://www.researchgate.net/publication/236020494_The_Principle_of_Maneuver_in_Cyber_Operations>

1. Greenberg A, “The Unfold Story of NotPetya, The Most Devastating Cyber-Attack in History”, Wired, August 2018.

<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

1. Cyber Kill Chain. Lockheed Martin.

<http://www.lockheedmartin.com/us/>

**Third Module (Lessons 4, 5, 6) – The Topology of Cyber Threats and Defense:**

Kinds of attacks and defenses, advanced attacks, weaknesses, immunization, case studies, evolution of the threat, principles of defense – the three layers, from organization to state, cyber market, public policy, analyzing a sector as an example.

Background material (marked – important reading; unmarked – additional reading):

1. **Matania Eviatar, Yoffe Lior and Mashkautsan Michael, "A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy", Georgetown Journal of International Affairs XVII, no. 3 (2016): 77-84.**

https://muse.jhu.edu/article/649450/pdf

1. Matania Eviatar, Yoffe Lior and Goldstein Tal, "Structuring the national cyber defence: in evolution towards a Central Cyber Authority", Journal of Cyber Policy 2, no. 1 (2017): 16-25.

<http://dx.doi.org/10.1080/23738871.2017.1299193>

**Fourth Module (Lessons 7, 8, 9) – The Israeli Case:**

National strategy, government decisions, the Cyber HQ, the struggle for establishing the National Cyber Directorate, national eco-systems, cyber as a political leverage.

Background material: (marked – important reading; unmarked – additional reading):

1. **Adamsky, D., "The Israeli Odyssey toward its National Cyber Security Strategy", The Washington Quarterly, June 2017.**
2. **Matania, E., "Israel – The Making of a Cyber Power – Case Study", Trends in Technology and Digital Security, Digital Threat Symposium, Fall 2017, Center for Cyber and Homeland Security, The George Washington University, p24-27.**
3. Leitersdorf, Y., Schreiber, O. "The Israeli Cybersecurity Industry in 2018: Special Review", Israel Defense, January 2019.
4. Zehavi, R. "How Israel is carving out a corner of the cyber-security market", ipolitics, April 2016.

<https://ipolitics.ca/2016/04/03/how-israel-is-carving-out-a-corner-of-the-cyber-security-market/>

**Fifth Module (Lessons 10, 11, 12) – Advanced Issues in Cyber:**

The global race for cyber-digital superiority, data regimes and aspects of democracy, artificial intelligence in the cyber era, the national project for intelligent systems.

Background material: (marked – important reading; unmarked – additional reading):

1. **Lansiti M., Lakhani K. R., "Competing in the Age of AI", Harvard Business Review, January-February 2020.**
2. Benkler Yochai, "The Internet: Degrees of Freedom, Dimensions of Power", Daedalus 145, no. 1 (2016): 18-32.
3. **Staltz Andre', "The Web Began Dying in 2014: Here's How", Staltz.com, (2017).** https://staltz.com/the-web-began-dying-in-2014-heres-how.html
4. Wright Nicholas, "How Artificial Intelligence will Reshape the Global Order?", Foreign Affairs, July 2018 (snapshot).

**Evaluation:**

A written assignment of 2000-2500 words on the topic of cyber strategy, including several different courses of action, or a discussion between opinions. The paper must present the topic, the possible courses of action (or opinions), to discuss them and to present a recommendation or a preferred option. More details and examples will be given in class.