The Information Warfare, Cyber Warfare and Open Sources Intelligence: An Interdisciplinary Approach

An Intensive Program Proposal for Spring/Summer of 2012

Assoc. Prof. Ahmet KOLTUKSUZ, Ph.D.

Yaşar University

School of Engineering, Dept. Of Computer Engineering

Izmir, Turkey

The Aim & Rationale

The Information and Communication Technology (ICT) is rapidly and continuously changing and re-shaping the concepts such as the arena, theater, combat, engagement and warfare into some unprecedented terms like cyber-space, cyber-war, information warfare and, open source intelligence. Therefore, it would be best if we start with the definitions of those new terms.

Some Definitions for Cyberspace, Cyber Terrorism and for Cyber War

United States, Department of Defense defines cyberspace as: "The notional environment in which digitized information is communicated over computer networks." Moreover, In the U.S. Federal Government, the FBI describes cyber-terrorism as: "Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population,with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.", Yet another definition is: "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives." [1]

On the other hand, Parks and Duggan defines the Cyberwarfare as: "the sub-set of information warfare that involves actions taken within the cyber world. The cyber world is

[1] "Cyber Operations and Cyber Terrorism, Handbook Number 1.02", US Army Training and Doctrine Command, Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence – Threats, Fort Leavenworth, Kansas, 15 August 2005., p. II-2.

any virtual reality contained within a collection of computers and networks. There are many cyber worlds, but the one most relevant to cyber-warfare is the Internet and related networks that share media with the Internet. The closest military definition to our term, cyber-warfare, is a combination of computer network attack and computer network defense, and, possibly special information operations." [2]

Enter Open Sources Intelligence (OSI)

Intelligence has been defined by numerous dictionaries as all kinds of data and information collection and evaluation efforts against the adversaries and/or potential enemies. 85% of all intelligence data come from the open sources. On the other hand, the remaining 15% which cannot be collected from the open sources constitute the espionage or spying effort.

"The publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access" is the official definition for Open Sources Information.[3] While Central Intelligence Agency (CIA) declares that the open sources data comprises 40% of the final all-source intelligence, Defence Intelligence Agency (DIA) gets 30% from open sources. And for Canadian Security and Intelligence Service (CSIS), the open sources comprise 80% of the final all-source product.

Nowadays, all of the ICT efforts toward a successful open source intelligence works can be grouped under the term of Competitive Intelligence (CI)

The main compounds of Information Warfare; which are (i) the cyber-war and, (ii) the open sources intelligence, are actually impacting every notion of national and/or international security. Along with this paradigm, NATO has underlined the cyber threats and the actions that will be taken against, in its new strategy dated May 17th of 2010 [4], and the new NATO Strategic Concept as well. [5]

Nothing could be more right and timely then this new strategy of NATO which was underlined by STUXNET WORM which is now considered as the marker malware that delineates the beginning of the cyber-war era under the terms of information warfare.

Thus, the dissemination of information is now more important than ever and, an Intensive Program; which aims the awareness for aforementioned issues, if nothing more, will serve throughly to the purpose of NATO's current efforts for security and stability.

[2] Raymond C. Parks and David P. Duggan, "Principles of Cyber-warfare", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001. P.122.

[3] CIA, Director of Central Intelligence Directive 2/12 (effective 1 March 1994).

[4] Nato 2020: "Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for Nato".

[5] Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, 20 November 2010.

On the other side, the issues related to by whom and for what reasons cyber-threats have been moved to the agenda of the governments, how governments assess, prevent, defend and response against the implications of the cyber dimension of modern conflict are of utmost importance. The nature of the new threat requires decision makers to adapt themselves to properly respond to the uncertainities of the new national and international security challenges unfolded by the cyber space.

Contents (to be detailed later on)

- Basic Concepts in Information Warfare
    - Information Theory
    - Decision Theory
    - Knowlegde Management
    - Theory of Computer Networks

- Policy, Strategy and Operations
    - Strategic Analysis
    - Strategy - Policy Creation & Management
    - Understanding the globalization

- Malware: Worms-viruses

- Network/Internet Attacks

- Offensive Information Operations
    - Network/Internet Attack Tactics
    - C4I Warfare Tactics
    - Denial of Service Tactics

- Defensive Information Operations
    - Information Systems Assurance
    - Authentication & Access Control
    - Firewalls
    - Cryptographic measures: Digital Signatures & Key Management
    - Secure Operating Systems
    - Intrusion Detection & Prevention
    - Incident Detection & Response

- Competitive Intelligence
    - Open Sources Intelligence applications
    - Inteligence / Counterintelligence
    - Tools for OSI

- Cyberwar Simulation
    - Simulation tools
    - Attack scenarios
    - Choosing victim critical infrastructures
    - DOS and DDOS attacks
    - Response and defense
    - Report and cyber security strategy generation

Target Audience

Due to very complex nature of the concepts that we would like to discuss, not only the graduate as well as the senior undergraduate students of the departments of Computer Science, Computer Engineering & of Software Engineering are required, but also the senior undergrad and/or graduate level students of the department of International Relations will be heavily involved.

Capacity

We, the Computer Engineering department of the School of Engineering and the depatment of International Relations of Yaşar University, would like to host 50 students for this Intensive Program.