Abstract

Cyber Security is the most complex field of the Information Technology and Communications (IT&C) domain. It encompasses all the IT&C areas demanding specialists working as cyber security experts to understand, to a very high degree, the majority of its sub-domains.

With the scale of current cyber-attacks and with the proliferation of cyber-kinetic attacks, NATO's decision to treat Cyberspace just like any other strategic dimension comes as a natural reaction to the current tactical and political context. This implies that the importance of cyber security operations has increased a lot. Now, a large Denial of Service (DoS) attack targeting a nation's critical infrastructure can be judged as a reason to invoke the 5th article of NATO's Washington treaty which refers to collective defense. In such a case a "simple" DoS attack could be the start of a new World War.

We study, in this thesis, the current context regarding cyber conflicts at national level and cyber-attacks at organizational or individual level for determining the scale cyber events have reached. In addition, we review the legal aspects concerning cyber conflict at both national and organizational levels for determining when a specific cyber incident could determine an armed response for a nation state.

This thesis describes the implementations of biological principles which are applied to cyber security operations alongside artificial intelligence primitives for automating and leveraging risk management in the field of security event triage. Moreover, we propose a platform for cyber defense operations in a software defined network (SDN) context as well as a malware analysis platform for protecting against 0-day exploits and Advanced Persistent Threat (APT) attacks that are generated from the Dark Web or are deployed using the Tor network. Furthermore, we propose an implementation for displaying information regarding an organization's current cyber security status by using cognitive visualization techniques. Also, we propose a modification to the Structured Threat Information Expression (STIX) protocol for including our biologically defined danger signal in the threat exchange information. Lastly, we propose some modifications to the current legal framework that regulates cyber-conflict.

For every proposed implementation we present detailed case studies and relevant experimental results published in ISI indexed journals and conference proceedings.