# AI-Based Cyber Defense for More Secure Cyberspace

Dimitar Stevo Bogatinov, Mitko Bogdanoski and Slavko Angelevski

Source Title: Nature-Inspired Computing: Concepts, Methodologies, Tools, and Applications
 |Pages: 19
DOI: 10.4018/978-1-5225-0788-8.ch056

## Abstract

The growing network attacks and intrusions have put the government organizations at a great risk. In cyberspace, humans have great limitations in data analyze and cyber defense because of the amount of data they have to process and the limited response time. Considering these parameters one of the best solutions is when the cyber defense mechanisms are AI (Artificial intelligence)-based because they can easily determine and respond to the attacks that are underway. The responses can be easily managed using man in the loop or fully atomized techniques. This chapter gives brief review of the usage of artificial intelligence in support of cyber defense, explains some useful applications that already exist, emphasizing the neural nets, expert systems and intelligent agents in cyber defense. Furthermore the chapter will propose a technical AI-based cyber defense model which can support the governmental and non-governmental efforts against cyber threats and can improve the success against malicious attack in the cyberspace.

## Introduction

The development of the internet and communication systems started the new era of cyber movement that has fundamentally changed the way of work of the governmental and non-governmental organizations. People, governments, and firms now almost fully rely on the use of the internet for their activities. The integration of information technology into today's systems and functions has improved efficiency and led to significant change in daily life, but this reliance on integrated information technology system has also led to greater risk from cyber threats of many developed nations. The increased use of technology and interconnectivity means that the vital components of various countries critical infrastructures are exposed to cyber-attacks (Chandia, 2007). Protecting the information and communication critical infrastructure from such disturbances and attacks is highly important for every government and non-governmental organizations, and is one of the major challenges in the future.

The perpetrators can be individuals, small groups and states. They differ significantly in their intentions and in their technical and financial resources. State or state-financed players generally have greater financial, technical and personal resources and are better organized, which explains their relatively high potential for causing damage. With their attacks, they seek to spy on, blackmail or compromise a state, individual authorities, the armed forces, the private sector or research institutions. They can also act in various ways against national or economic interests in order to achieve political power and economic interests. Individual and state actors primarily seek to achieve financial benefit or recognition in their communities.

Many different tools are used for cyber attacks. Malware can be deployed in a targeted manner and installed on third-party computers without the user's knowledge. The malfunction of insufficiently protected and maintained operating systems and applications (e.g. Internet browser or specialist applications) enables the attackers to take control of the affected computers. These computers can be controlled remotely via the Internet, and systems can have additional malware installed that is capable of accessing stored data and enabling the attackers to modify, delete, or transfer data to other computers controlled by the attackers as happened in the case of GhostNet (Moore, 2009; Markoff, 2009).

Moreover, attackers can also exploit organizational weaknesses of the company to break into protected systems. Perpetrators often break into the corresponding systems exploiting insiders' unawareness or vulnerabilities in data processing procedures and insecurely designed or poorly maintained systems (e.g. leaving the default password).

Attackers employ several features of the cyberspace to protect themselves and their attacks from early discovery and prosecution. For example, they take advantage of: anonymity, geographic location, legal barriers, and removal of traces. By forging technical data and increasing the complexity of their attack methods, using tools like tor project and tor browser (AnonymityOnline, 2014), attackers can hide their activities or identities. Based on such tools and methods, it is often impossible to find the motives for their acts.

Cyberspace is also being used by terrorists to spread propaganda and disinformation, radicalize followers, recruit and train members, fund raising, plan campaigns and provide information on them. Up to now, the focus has been on using information and communication infrastructure, but not on attacking it: terrorists still aim mainly at carrying out serious physical attacks against life and limb as well as infrastructure by conventional means. Terrorist cyber attacks with very high consequential physical damage may appear unlikely from today's perspective, but it cannot be excluded that terrorists could try to launch cyber attacks on a country's critical infrastructure in the future.

The internet uses a large amount of data that cannot be handled and analyzed manually by humans and requires considerable automation so it can be effectively defended. Creating software with conventional, fixed algorithms (with logic on decision making) to defend the network against the dynamically evolving attacks. This situation can be handled by applying