Chapter 4
Hacking and Hacktivism as an Information Communication System Threat

Katerina Zlatanovska
Ministry of Defence, Macedonia

ABSTRACT

The distribution of information technology is a step forward in accelerating rapidity and efficiency of transferring information. As each system, that is subjected on different anomalies, so that computer information systems are also subjected to different disorders to make a stop or destruction of it. There is a question: who would like to do harm to the system which is produced for people and society needs? HUMAN BEING is the response. However, it is not every human being, but a person, popularly called a hacker, who is educated in the information technology field and who makes damage, using computers and the Internet. Hacking and hacktivism as a function of information systems and technologies, expressed as a pattern of ethical or unethical hacking, represent a global menace, for some people, as well as whole institutions and arrangements. The actual problem, imposing here, is how creators and users of computer information systems can find a solution, or compatible protection and preventive acting in those areas where such a problem appears.

INTRODUCTION

Cyberspace

According to Bruce Sterling (1993): "Cyberspace is (Figure 1) a "place" where it looks like there is a phone conversation going on. Not inside your phone, plastic device of your screen. Not inside your talker's phone, in another city. The place between two phones. Undefined place, over there, where both of you, human beings meet and communicate."

The term cyberspace is used for the first time by William Gibson, in 1984, in his roman "Neuromancer", when he tried to give a name to describe his vision for a worldwide network, the connection of all people, machines and sources of data in the universe, through which he can act or trick us in the virtual universe.

Attempting to define cyberspace exactly, the authors cannot find a compatible definition. It is mutual that in the entire cases cyberspace exists only in theory, actually it is an illusion.

DOI: 10.4018/978-1-4666-8793-6.ch004

Figure 1.

1. Cyberspace refers to the virtual computer world, actually to an electronic medium used for a global computer network forming to create it easy the online communication. It is a large computer network composed of many world computer networks that include TCP/IP protocol to help in communication and data change activities. Its basic function is an interactive and virtual background for a wide range of users (Cory Janssen, n.d.)
2. Cyberspace is characterized by the usage of electronics and the electromagnetic spectrum to save, modify and data exchange through computer systems and physical infrastructures connected. Respectively, it can be considered as interconnection of human beings by computers and telecom, irrespective of geographic prevalence (Rouse Marin, 2008).

According to definition, cyberspace is a virtual computer world, global computer network, which through the electromagnetic spectrum enables forming, saving, modifying, data exchange through information communication systems that are reciprocally connected.

The data system is any written, electronic, or graphic method of communication systems. The base of information system is partitioned and processing data and ideas. Computers and telecom technology are important parts of this system. The term information system is information technology that is used for performing certain organization or individual objects (Seneva S., 2009).

By reason of its own nature, that contains an easy data access, fast data flow, texts combination, weak law regulative that results with easy access etc., cyberspace is subjected to different attacks.

These attempts are called cyber-attacks and they mean an intentional using of computer systems and networks. They use malicious code to change computer codes, logic or data that results in alarming consequences that can compromise data and lead to cyber-criminal, such as data phishing. Cyber-attack is also known as a computer network attack. Cyber-attack involves:

- Data phishing, fraud or extortion;
- Malicious software, phishing, spamming, Trojans, viruses etc.;
- Stolen hardware;