Chapter 6
National Security Policy and Strategy and Cyber Security Risks

Olivera Injac
University of Donja Gorica, Montenegro

Ramo Šendelj
University of Donja Gorica, Montenegro

ABSTRACT

This chapter gives explanation on theoretical framework of the national security policy and strategy. Moreover, it analyzes selected countries approaches to cyber security in national policy and how countries build their capacities to face with risks, and address objectives in some cyber security policies. Also, in this chapter are described different sorts and sources of cyber threats, techniques of cyber attacks and frequently used tools (software and hardware) by cyber attackers. In addition, according with Symantec's and Kaspersky's annual report about Internet security threats for 2014, were analyzed the most important cyber threats and attacks during 2013. Furthermore, the chapter shows organization structure of cyber security system of Montenegro, statistical analysis of users activities in cyber space and cyber incidents that happened in Montenegro during 2014.

INTRODUCTION

In informatics age, where online communication has become the norm, internet users are facing increased number of threats and becoming the targets of cyber-attacks. We are witnesses of the global phenomenon of the rise of threats based on the main aspects of globalization (e.g. ICT) and security threats in the age of globalization are in connection with different dimensions of globalization (economic, political, cultural, ICT, ecological).

Cyber security threats are one of the biggest challenges for national security systems, because they tend to destroy economic and national security in the 21st century.

DOI: 10.4018/978-1-5225-0808-3.ch006

There are many reasons which contribute to the rise of cyber security threats, such as growing dependence of information technologies, interconnections of critical infrastructures and different weaknesses in some sectors (government, industry, financial system, etc.).

While cyber criminals continue to develop and make their techniques more advanced, they are also shifting targets focusing, for example, on theft of financial information, business espionage and accessing government information.

As it was stated by Stevens (2012), in contemporary time we have huge prevalence of information communications technologies, and what is paradoxically it became a symbol of the "uncertainty and irreversibility of the patterns of global emergence" (Stevens, 2012, p.1).

Importance of cyberspace for national security, has expressed US President Barack Obama in his speech in May 2009, saying that it is ironic to have technologies which at the same time could support world development and being misused for the world destruction.

Cyber security has strategic and tactical dimensions in national security, because it affects all levels of society. The cyber threats and their performance techniques are continuously evolving, and it represents threats to data security, electronic systems and personal privacy, what makes challenging tasks for states to response on them.

Some of the past occurred cyber-attacks (Estonia and Georgia), were directed on different organizations including parliaments, banks, ministries, newspapers, and broadcasters and even the effects were localized to those countries, they do show what a cyber-attack can produce (Miklaucic, M. & Brewer, 2013).

There could be expectations that danger will grow in a future and cyber-attacks will be able to destroy state infrastructure, what could directly threaten citizens and significantly block state system under attack.

Expectations from the states are to be prepared and to work on their own capacities for cyber protection and for response on cyber threats, and in addition to that, it is necessary to adapt comprehensive national security policy and strategy.

The term cyberspace covers enormous field of the technology and networks, including Internet, telecommunications networks, computer systems and processors in critical industries. The usage of the term cyberspace also refers to the virtual environment of information and interactions between people. The globally interconnected and interdependent cyberspace is main sphere which provide support for modern society, the world economy, civil infrastructure, public safety and national security.

As some experts stressed, cyberspace protection requires strong vision and leadership, as well as changes in priorities, policies, technologies, education, laws and international agreements (Branon, 2014). Confronting to cyber threats require strong commitment of all actors to be innovative and adopt efficient technologies that can be adequate to contribute on enhancing national security, the global economy and individual freedoms.

Cyber threats and challenges can causes significant effects for the states, and it force them to find new solutions, to develop tools and mechanisms for prevention and response, and also to adapt adequate security policy for cyber threats.

The thesis of chapter is that states have different approaches towards cyber security policy, and if it is guided by security sector reform and national security policy development, than states are mainly concentrated on institutional building and resources improvement. That is shown on the case study of Montenegro.