Chapter 82
Trends in Peace Research:
Can Cyber Détente Lead to Lasting Peace?

Nenad Putnik
University of Belgrade, Serbia

Mladen Milošević
University of Belgrade, Serbia

ABSTRACT

In this chapter, the authors discuss the phenomenon of interstate conflicts in cyber space. In the last twenty years, this issue has become more explicit, and countries are making increasingly frequent mutual cyber warfare and cyber espionage accusations. The political and military elite of conflicting countries perceive the situation as very serious and are preparing not only for defending their segment of cyber space, but for developing offensive strategies for cyber warfare, as well. The authors endeavor to contribute to peace research by examining the possibilities for achieving cyber détente, the idea promoted by Henry Kissinger in 2011. In this chapter, the authors identify and analyze problems whose solution should be the focus of the States Parties to cyber détente: the question of denotation and potential desecuritization of technical terms, the question of identification and classification of cyber threats and the problem of the legal framework for their opposition. In addition, the authors give guidelines for their solution, based on securitization theory.

INTRODUCTION

The tendency to maintain or achieve peace becomes especially significant in the second half of the twentieth century. Due to tragic experiences of two world wars, together with growing critical and humanistic awareness of apocalyptic dimensions and possibilities of modern wars and conflicts, conflict resolution and termination became the subject of numerous studies within different sciences and disciplines during the fifties of the twentieth century. To this end, a number of research institutes were founded, including the first and most significant Center for Research on Conflict Resolution, established in 1959 at the University of Michigan. The question of conflict resolution became an integral part of a special line of

DOI: 10.4018/978-1-5225-5634-3.ch082

research called Peace Research, which in the 1950s brought together most eminent scientists from all over the world.

After the world division into blocks was terminated in the early nineties of the last century, unpredictability and escalation of various forms of social conflicts (war, class and racial) turned scientifically and humanistic minded public to a different approach in research and resolution of social and interstate conflicts. In addition to a number of national and international research institutes, there emerged a strong development of the non-profit sector, which on different levels of generality and specialization became interested in problems of peace research and resolution of all types of conflict – from interstate, ethnic and religious to business and family.

Among the new security risks, challenges and threats in this period, the threat of cyber conflicts has taken a significant place. The first problems related to the security of cyber space were identified upon releasing the Internet for public use in 1991. A continuous increase in the number and type of malicious codes, as well as techniques and tools for carrying out attacks in cyber space, led to a certain expansion of conflicts in this virtual space. The attackers have been numerous; they are individuals, ideologically motivated groups of civilians – hacktivists, criminal and terrorist groups, national armies and their intelligence services. They are driven by various motives the desire to prove themselves, the eagerness to inflict damage on a country perceived as hostile, illegal acquisition of goods, the realization of political and ideological goals, and achieving military and strategic advantages in cyber space.

Attacks that affect information infrastructure are considered to be very dangerous to the security of the attacked state, for its operational disruption can lead to violation of its sovereignty, as it was shown in case of Estonia in 2007 (Kešetović, Putnik & Rakić, 2013). Ever since, in all the world's highly computerized countries, a fear of cyber-attacks on information structure has been growing. For every serious attack, the official army of the state perceived as opposing is to be blamed, always without previously conducted thorough cyber-forensic analysis (Kešetović, et al., 2013). In recent years this has resulted in countries (most often the United States, the Russian Federation and the People's Republic of China) making frequent mutual accusations regarding cyber warfare and cyber espionage.

Due to the evident tensions, whose consequences are reflected both at political and diplomatic, military, and economic fields, the doyen of American diplomacy Henry Kissinger proposed a new method for easing tensions among the countries concerned with cyber détente. Kissinger did not precisely define the term of cyber détente, nor did he determine the implied sequence of steps and set of actions. Kissinger's proposal did not significantly stir the academic community. For that reason, as the aim of this chapter, the authors set the task to consider whether cyber détente could be an adequate method for achieving and maintaining peace in cyber space, and what set of activities it would involve.

BACKGROUND

From a theoretical perspective it is significant that, until the nineties of the twentieth century, peace and social conflict research was based on classic interstate conflicts as well as global fixation on superpowers of the time, and military blocks. This approach proved to lack adequacy for overemphasizing political and ideological aspects while overlooking economic, environmental and cultural aspects. "Low intensity" conflicts were also ignored, being observed through the lens of the superior "high intensity conflict between East and West".