Chapter 9
Analysis of Possible Future Global Scenarios in the Field of Cyber Warfare:
National Cyber Defense and Cyber Attack Capabilities

Flavia Zappa Leccisotti
Security Brokers SCpA, Italy

Raoul Chiesa
Security Brokers SCpA, Italy

Daniele De Nicolo
Security Brokers SCpA, Italy

ABSTRACT

At a global level, various risks have increased due to the intensification of globalization, and in this scenario Cybercrime is becoming a more important and dangerous threat. When discussing about Cyber Space threats, it is not an issue if critical national infrastructures, private companies and private citizens will be violated, but rather when it will take place, when it is realized that this has happened, and which is the extent of the attack. Through the collection and analysis of open source documents, institutional organizations, think tanks, academic and experts' papers, the goal of this chapter is to highlight and understand what and how it is changing, if new scenarios will take place on the international cyber chessboard, and which dynamics will regulate the new threats that we must prepare to fight or, at least, mitigate.

INTRODUCTION

Today one of the most difficult aspects of national security policies is certainly the risk management. The study of risk and crisis management is playing, in recent years, an increasingly strategic role in the governance of the States. At the global level the various typologies of risks have become increasingly important, due to the intensification of globalization, and it is precisely in this scenario that Cybercrime represents an even more dangerous threat. The consequences of the

DOI: 10.4018/978-1-4666-8793-6.ch009

new risks have become cross-boundary, and are potentially devastating and unpredictable. The global interconnection makes any economic and productive national system vulnerable.

It is known that the progress of society has always been followed by the evolution of all of its aspects, such as economy, technology, and, unfortunately, war. This evolution tough, over the time, is always faster; what we are prepared to fight today will be already obsolete tomorrow, and generations of threats always run out in less years, or even months.

The future wars are likely to be made partly or entirely, in Cyber Space. Cyber Space, however, has its own specificities. First of all, one of the most strategic is undoubtedly the ability to hit anonymously, aspect of course unthinkable in conventional wars. The protection of Cyber Space has become a crucial national interest for its importance, both for the economy and for the military.

The so-called Cyber War also produces different effects, more effective, global, that change the dynamics of attack and defense: for example, making faster and faster reaction time and giving the opportunity to the victim to equip with the same technological weapon to return the attack. It is cheap and can be managed and implemented at a distance and it can create a huge echo in the media system. Cyber Attacks, whether by States, criminals or terrorists can inflict with a single click massive damage to the interests of a country, such as its critical infrastructure.

Cyber Space is also subject to increasingly rapid technological changes and as the "new wars" scenario, as Mary Kaldor calls it, is replacing more and more the physical space, and its geography is ever-changing and usable by anyone, not only by Nation States, that are no longer holding the monopoly of force in the fifth domain of combat (Kaldor, 2012).

Cyber War is, without a doubt, the quintessential asymmetrical warfare and the asymmetry lies in the fact that we are in a situation where the threats of the twenty-first Century hit a substantially seventeenth Century structure. The potential of Cyber Warfare become more destabilizing than a conventional war.

The success of an attack carried out by computer is directly proportional to the rate of reaction and to the use of countermeasures. That's why it is crucial that these are prepared before the attack takes place, with an operational mode that-precisely because of the global nature of malware and the wide variety of people who may be involved- needs to go beyond national borders, following the logic of integrated security, involving all security stakeholders.

It points out that the contrast to the Cyber Threats for the security of a Country, should rank a high priority. Both in political and national interest protection terms, it is evident that the lack of a consistent and timely review of the national security strategies involves a serious risk for everyone. It is therefore necessary to stay updated and keep abreast with the development of Cyber Weapons and skills in the field of Cyber Warfare, Cyber Defense and Cyber Attack of the various Nation States during this evolution.

BACKGROUND

Nearly after two years from the beginning of the study about Cyber Warfare, Cyber Defense and Cyber Attack doctrines and strategies of National States by Flavia Zappa, is aimed to produce a different study, aiming to analyze the evolution of those doctrines and strategies, and assuming future scenarios.

The motivation beyond the rise on the analysis spectrum is somehow very simple: "Nation-State driven" Cyber Attacks can be nowadays regularly found on a global scale, no matter if they are officially endorsed, sponsored or "tolerated" by a National State. Someone spoken about a new Cold