Chapter 13

Changing the Approach to Deterrence in Cyberspace while Protecting Civilians from Cyber Conflict

Metodi Hadji-Janev
Military Academy "General Mihailo Apostolski", Macedonia

ABSTRACT

Many incidents in cyberspace and the response to those incidents by victim states prove that the cyber conflict is a reality. This new conflict is complex and poses serious challenges to national and international security. One way to protect the civilian populace is by deterring potential malicious actors (state and non-state) from exploiting cyberspace in a negative way. Given the changed reality and complexity that gravitates over the cyber conflict classical deterrence that have worked during the Cold War is not promising. The article argues that if the states are about to protect their civilians from the future cyber conflict by deterring potential attacker they need to change the approach to deterrence.

INTRODUCTION

The Cyber conflict has become a reality. Contemporary dynamics in international relations and operational environment show that a major cyber attack aimed at disrupting critical infrastructures and thus producing cascade effects with material damage and mass casualties is highly possible. Non-state actors and states have started to look into cyberspace as a channel to maximize their efforts and to defy their perceived enemies. These attacks, however, are not through conventional means and with conventional weapons alone. Practice shows that the attacks to achieve strategic objectives could be done through cyberspace alone or through a combination of cyberspace and physical space with traditional means and methods of warfare. Hence the potential cyber conflict poses serious challenges to the states' and international security.

To protect civilian populace states should consider deterrence through active defense measures focused on limited counter-strikes in self defense.

DOI: 10.4018/978-1-4666-8793-6.ch013

For these reasons the article will first explain why cyber conflict is a complex form of conflict and how this conflict challenge international security. The rationale is that in the absence of legal, technical, economic, or other punitive measures against attackers, potential attackers have few incentives to refrain from launching attacks. Deterring malicious challengers thus represent a promising option to protect civilians from the potential cyber conflict.

Many argue that the Cold War (or as some called it classic) deterrence is ineffective. Therefore the article will explain whether or not classic deterrence could work in cyberspace. Based on the conclusion the article offers a comprehensive set of challenges for deterrence to be successful.

To make deterrence functional while protecting the civilian populace from the future cyber conflict states need to consider a combination of conceptual technical, procedural and legal changes. Diplomatic, economic, operational and informational efforts must comprise conceptual changes to cyber conflict. Procedural and technical challenges should aim to upgrade passive defense measures with building security through diversity. The idea of security through diversity is to automatically generate variants of a defender to alter certain properties of the environment in which specific measures might not work. To achieve this passive defence measures are welcomed but they are not enough. Procedural and technical changes to adapt moving target defence and active defence measures hold potential to influence cognitive part of the attacker's decision making process and eventually to withstand from the malicious activity.

Finally, the article will try to prove that if the states are about to establish successful cyber deterrence among others, they need to improve regulatory regimes regarding the cyberspace. The new laws and regulations should also govern the use of moving target defense and active defense technologies.

1. CYBER CONFLICT IS REAL AND COMPLEX

The end of the Cold War has marked a new era in international security. The processes of intensified globalization and the technological development as a result to this tectonic shift have positive and some negative effects. Those who champion globalization and technological developments emphasise the efficiencies and opportunities in the business environment, improved technology of transportation and telecommunications, improvement in movement of people and capital, diffusion of knowledge, emphasised human dimension of the security, etc. On the other hand critics of globalization and technological development focus on the "deregulation of commodity" and the balance that has evaporated with the end of the Cold War (Fotopulos, July 2001). These processes according to some views have destroyed the "walls" and have "flattened" the world for good and for bad (Friedman, 2005, Ch-1).

The new flattened environment has ignited the process of power redistribution. As a result, states have significantly lost the monopoly of power. In this new, fundamentally transformed security environment, some actors have seized the opportunity and have started to acquire unconventional means to achieve strategic ends. Recent practice shows that competitors in the current security realm are ready to employ all forms of war simultaneously. Utilizing tactics to use modern technology (primarily designed to bring commodity and wealth) state and non-state actors multiply their power and create multidimensional threats.

Many governments, but also international organizations recognize the complexity of the contemporary security reality. In this line threats from cyberspace occupy security debate among the pundits, scholars and policy makers. This is reasonable since activities in cyberspace are