Chapter 16
Cyber Warfare and NATO's New Security Concept: Smart Defense

Ibrahim Karataş
Turkish Airlines, Turkey

ABSTRACT

This study analyzes NATO's efforts for defending itself and member states against cyberattacks originating from cyber space, which is the fourth domain of operations now, and the smartization of defense policies, respectively. It then elucidates whether the cyber defence can be ensured via practicing the smart defence paradigm. While the smart defence is already applied in military production and operations, and there is some success to a certain extent, to what extent smartizing cyber defence will be successful is a question whose answer is yet to be found. This chapter searches for the answer by applying NATO's smart defence concept to its cyber defence domain and tries to learn the possibility of the achievement of the new paradigm. In addition, it lays down its proposals such as imitating successful models and enlarging NATO so that it can include other partners in cyber space. Methodologically, a literature review was used to prepare the chapter.

INTRODUCTION

NATO was established by 12 countries located in the transatlantic region as a military alliance to protect member states from the Soviet threat in 1949. The alliance, consisting of 16 members until the end of the Cold War, could become a deterrent organization thanks to its strong members from the developed world, and destructive arms like nuclear weapons, ballistic missiles, large fighter fleets, and so on. Across the Cold War, threat meant a military attack from basically the Soviet Union-led Warsaw Pact, founded by the Soviet bloc as a counter alliance to NATO in 1955. On the other hand, weapons meant only military arms that were used in land, air, sea, and later space domains. In addition, actors were mainly states. Thus, a country or an alliance could feel safe if any foreign military attacks were deterred, repelled or the enemy was defeated. With the end of the Cold War, the most dangerous threat (the Soviet bloc) collapsed

DOI: 10.4018/978-1-7998-7118-7.ch016

but NATO continued to exist. However, threats did not end though they were not as dangerous as those of a superpower and its allies. Regional conflicts in the Balkans and the Middle East, the emergence of new actors like China, the rise of terrorism, migration and so many other big and small threats were before NATO to struggle with.

Further to the diversification of threats, a new threat originating from cyber space came into being due to fast advancements in communication technology. Particularly developments in internet technology connected the world and led to states, non-states, organizations, institutions, and people create networks and communicate easier with each other. While cyber space facilitated life, business, and military affairs, virtual networks also became a means of infiltration into digital infrastructures by malicious actors to steal data, deny service, attack servers, or destroy networks. Cyberattacks became apparent in the late 1990s and victimized anyone using a computer with an internet connection. As can be predicted, the world's largest military alliance NATO would not be immune from attacks. NATO incurred to cyber attacks by Serbian hackers for the first time during the Kosovo operation in 1999 (Burton, 2015: 305). Attacks continued over time and forced the organization to tackle them through creating concerning departments and finally declaring it as a new domain in 2016 (Emmott, 2018). On the other hand, while NATO took a defensive position in cyber space, it was also encouraging its members to work together in order to increase efficiency, cost-saving, and producing sophisticated weapons. This move was conceptualized by NATO Secretary-General Anders Fogh Rasmussen as 'Smart Defence', the new paradigm advising members to prioritize and specialize in certain sectors and boost cooperation among themselves.

The smart defence is a new concept but NATO members were already enforcing similar methods previously. Yet, as will be explained below, not all attempts regarding smart defence were successful due to some side effects that made members reluctant about clustering for certain projects. However, this chapter argues that unlike other sectors, the smart defence principle can be applied to cyber defence thanks to several advantages. First, while member states accept prioritization and cooperation principles in smart defence, they avoid specialization due to sovereignty concerns as assigned roles might make them dependent on other states for non-assigned roles in the future. This is not the case in cyber defence since there is not much need for specialization because of the compact and simple nature of the domain. In other words, a cyber defence project does not require the dedication of the work to various actors. Second, the cost of cyber space-related projects is quite low as opposed to other areas since the output is not a weapon but a virtual computer program or hardware. What matters in cyber defence is know-ledge rather than know-how or weapons. Based on these facts, this study contends that collaboration among member states to reduce costs and sharing technical knowledge in cyber space is an easy mission that all members will accept. On the other hand, while the study admits that 'smart cyber defence' implementation is not without problems, it asserts that obstacles are not major enough to impede cooperation.

Methodologically, I made a literature review concerning books, articles, reports and NATO documents to support and prove my arguments. This study's first section will discuss the basic keywords of the article, namely NATO, cyber warfare, and smart defence from a theoretical perspective. The second section will analyze NATO's cyber warfare efforts, followed by the third section examining the concept of cyber defence. Finally, the fourth section will elucidate how smart defence can be enforced in cyber defence and its likely success level.