ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

CYBERDETERRENCE AND CYBERWAR

Fatma ÇAKIR[*]

[*] Research Assistant, Department of International Relations, Selcuk University-Konya-Turkey, can be accessed via fatmacakir021@gmail.com

Martin C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, 2009.

Cyberspace that emerged as a new field parallel to technological developments has become an indispensable part of modern societies. Although conceptualizations in this new man-made area are similar to those in the physical world, it is actually difficult to transfer these concepts in the same way because of the nature of cyberspace.

In recent years, studies on cybersecurity have often included the concepts of cyberwarfare, cyberattack / defense and cyberdeterrence. However, it is argued that these concepts, like those in the physical world, can not fulfill the expected effect. At this point, Martin C. Libicki and his work *Cyberdeterrence and Cyberwar* have a prominent place in the literature. Libicki has a lot of work on cyberspace and cybersecurity and is a professor at the US Naval Academy in the field of Cyber Security Studies. Libicki also works as a leading scientist at RAND Corporation.

The aim of the *Cyberdeterrence and Cyberwar* is to guide US policymakers and Air Force leaders in preparing cyberwarfare and cyberdefense objectives, strategies, policies and operations. Focusing on the policy dimension of cyberwarfare, the study analyzes what the cyberwar means, what it requires, and whether it is possible to prevent others from resorting to it. (p.5)

The study consists of nine chapters and, in general terms, suggests the following basic arguments: Cyberspace is a separate field with its own rules. Conceptualizations in this area differ from those in other domains such as land, air, sea, space (p.11). For instance, cyber warfare is separate from wars in physical domains. Firstly, cyber attacks are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Secondly, there are ambiguities about who is attacking, what they have achieved, and whether they will do it again. Thirdly, a working attack today may not work tomorrow with changes in technology and security measures. In addition to these distinctions, Libicki also talks about the concepts of strategic cyberwarfare (p.117) and operational cyberwarfare (p.139). While he warns the US government and the Air Force not to consider strategic cyber warfare as a priority investment area due to unpredictable consequences, argues that operational cyber warfare should only be used under a support function.

On the other hand, Libicki points out the concept of cyberdeterrence and emphasizes that it is different from nuclear deterrence and other military deterrence in general. (p.39) These differences reveal the problematic aspects of cyberdeterrence. First of all, it is necessary to distinguish the purpose of an attack in order to be effective in cyberdeterrence. An attack may have been made by a certain intention or by mistake. Also, it is important to note that if a retaliatory attack occurs after an attack, the missile may be attacked against the wrong target, because it is hard to know exactly who launched the attack (p.41).

In his analysis of whether a state will consider retaliation, Libicki concludes that the state should consider whether they will win or lose by retaliating. States' actions can prevent more attacks, but they can also push the attacker to take the war further(p.53). In addition, whether the retaliation is open or hidden is a point that should be considered separately. Because of all these problems, Libicki states that the US administration and the Air Force should consume other options such as diplomatic, economic and prosecution before they go to the cyberwar.

In general, when examined, it seems that *Cyberdeterrence and Cyberwar* was written in a clear and understandable language and handled with a theoretical perspective. Therefore, this study can be read easily by the students of cyberpolitics, cyberspace and cybersecurity. Also, the author's section titles in the form of questions can be evaluated positive in terms of stimulating curiosity in the reader and having a general idea of which questions the author answered in the study. Finally, parallel to the purpose of it's preparing, the study is a good source of mind-opening for politicians and researchers interested in this subject.

STAYING AHEAD IN THE CYBER SECURITY GAME: WHAT MATTERS NOW

Mohammed ISHMEAL[*]

[*] PhD candidate at Selcuk University in the Department of International Relation, Konya, Turkey. Can e accessed via blkqatari@gmail.com