Cyber Warfare: Challenges within the Cyber domain

Regner SABILLON [1], Jordi SERRA-RUIZ Ph.D[2], Victor CAVALLER, Ph.D[3], Jeimy CANO, PhD[4]

ARTICLE INFO	ABSTRACT
	This article analyzes the cyber warfare phenomenon in all its dimensions by reviewing the most notorious and recent cyber warfare cases, in order to provide a wide conceptualization of factors and elements, strategies, generations and theoretical models. The first part of the article includes the analysis of the cyberattacks in Estonia (2007) and Georgia (2008) - considered from many scholars' point of view, milestones in the dawn of the cyber warfare era-, in Iran (2010), and in addition, the Operation Clever - that has been running worldwide since 2012, and different cases of cyber warfare and cyberespionage attacks from China. On the second part of the article, a synthetic set of definitions is introduced in order to gain a common field of conceptual agreement for the explanation of the main theoretical models that have been developed so far. The third section introduces the Dual Cyber Warfare Model applicable to military and organizational environments. This paper concludes that cyber Warfare is perhaps the most radical consequence of the Knowledge Era and must be systematically analyzed from both perspectives: empirical-practical and theoretical-conceptual.

Contents

♦♦♦♦♦

[1] Doctoral researcher, Universitat Oberta de Catalunya, Internet Interdisciplinary Institute, Calgary, Canada, regners@athabascau.ca.

[2] Professor, Universitat Oberta de Catalunya, Internet Interdisciplinary Institute, Barcelona, Spain, jserrai@uoc.edu

[3] Professor, Universitat Oberta de Catalunya, Department of Information and Communication Sciences Barcelona, Spain, vcavaller@uoc.edu

[4] Professor, Universidad de los Andes, Bogota, Colombia, jcano@uniandes.edu.co