Chapter 76
International Legal Aspects of Protecting Civilians and Their Property in the Future Cyber Conflict

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

ABSTRACT

The post-Cold War reality has brought many changes that challenge political leaders, planners and operators. Using cyberspace to accomplish their political objectives, non-state actors and states have opened serious legal debates over the applicability of the international law of armed conflict principles in cyberspace. In this context, the article explores how the basic principles of International law of armed conflict will apply to the protection of the civilian population from the future cyber conflict. To accomplish this article addresses the ius ad bellum and the ius in bello aspects of cyber conflict.

INTRODUCTION

The process of globalization and technological development has significantly affected international relations and operational environment. The re-distribution of power as a result to these dynamics has introduced new asymmetric challenges. Non-state actors, but also some states, have started to employ new technologies and the new environment in order to further their objectives, thus posing unconventional and hybrid threats to the states and universally accepted international order. As a result to all of these trends and dynamics political leaders, planners and operators face unusual challenge. On one side they have advanced capacities to accomplish military objectives and end-states like never before. On the other side they face many challenges that could not be answered with the conventional approaches, matrixes and procedures like before. Consequently, legal community is struggling to come to adequate solutions to these complex questions too.

DOI: 10.4018/978-1-5225-5634-3.ch076

Using cyberspace non-state actors and states have opened serious legal debates over the applicability of some legal standards and principles created for physical space to regulate relations among states and international institutions formed by them. Feeling threatened some states and organizations (USA and NATO for example) have published strategic documents preserving the right to use physical force if necessary. Such approaches according to some views have caused shockwaves within the legal community. While some argue that principles and standards of the International law of armed conflict are applicable to cyberspace, others believe that these regulations are woefully inadequate to regulate states activities in cyberspace. There those, however, who call for multidimensional approach to the effects that cyber attacks could cause. Instead black and white these scholars and experts believe that the nature of cyberspace urges one to consider different stages and applicable laws to respond to the effects from cyber attacks.

Regardless of these debates practice shows that, although the use of force under international law is limited to a few exceptions states and non-state actors have not hesitated to use force in order to accomplish their ambitions. According to the 2010 ICRC's study during the past 60 years the main victims of war have been civilians. These findings comply with the contemporary security studies and analyses claiming that during the modern conflicts the battlefields have moved into the urban areas and civilian infrastructures. Furthermore asymmetrical and the hybrid nature of modern threats stem from the methods that non-state and some states have recently started to employ in accomplishing their military objectives and political end-states.

Non-state actors (groups and individuals) defy mightier enemies relying on modern ICT technologies threatening to attack or attacking civilian populations. These attacks can have direct and indirect cascade effects with severe consequences. The complexity nevertheless, does not end here. Some states reportedly have also chosen to act similarly and through similar domains. Hence, they have started to pose hybrid threats that blend conventional war fighting, irregular warfare and cyber warfare. Given that cyberspace is highly interconnected and interrelated and that military ICT systems depend on civilian infrastructures the issue of protecting civilians from potential conflict through cyberspace raises serious legal concerns.

Therefore the article will focus on providing answers to several legal questions important to understand the obligation to protect civilians and their property in the future cyber conflict. The goal of this approach is to contribute to the overall debate for protecting civilian populations from potential abuse in the future cyber conflicts. In this context the central question of the article will focus on the state and non-state actors' obligation under the existing principles and standards of international law to protect civilians and their properties in the future cyber conflict. However, to be able to adequately address this question the article will briefly address several questions as a pre-requisite to the former. These are the questions that will be addressed in order to provide answer of the central issue. Under which circumstances can a cyber attack be attributed to a state? Can a cyber attack exceed the threshold of use of force established in the UN Charter? Furthermore, can a cyber attack constitute an armed attack that would justify the right of self-defense? As the Internet is not a centralized networking system and as the ICT sector is highly interconnected and interrelated, one of the questions that will be answered is how to defend against cyber attacks that overlap different jurisdictions? As cyber attacks require a high level of knowledge of information technology and as some states have already assembled civilian cyber defense forces the article will address the debate of combatant privilege and direct participation in hostilities. In this context the article will also test the basic principles of ILOAC and their applicability in protecting civilian population from the future cyber conflict. Hence additional questions will also dominate