Chapter 20
Right to Life and Cyber Warfare:
Applicability of Legal Regimes during Counterterrorist Operations (International Humanitarian Law)

Vesna Poposka
Mit University, Macedonia

ABSTRACT

Referring to the cyber space as the new dimension of warfare opens many legal challenges. Those challenges can be settled in two main clusters: first one related to the usage of cyberspace as a weapon itself, related the environment in which terrorist attack occurs (meaning that cyber infrastructure and cyber are used for terrorist attacks, or as an asset during counterterrorist operations), and the second drives on ancillary usage of the cyber infrastructure, means and methods for the same purposes. The cyberspace is lacking specific legal regime that is applicable, same as cyber attacks. While the specific applicable regime is lacking, as well as any consensus upon that issue, what has to be considered is if any parts of the currently ongoing legal regimes are applicable. Put into the context of cyber warfare, it can lead to different solutions, examined in the chapter.

INTRODUCTION

"Cyber" is a complex term. Dictionaries describe cyber as "Relating to or characteristic of the culture of computers, information technology, and virtual reality: the cyber age" (Oxford dictionaries, online dictionary) or as "of, relating to, or involving computers or computer networks (as the Internet)" (Merriam-Webster, online dictionary).

Cyberspace has been referred in the recent years as the new, 5th dimension of warfare- the only one dimension that is not material, but can produce more material and human damages than every other mean or method or warfare. Former secretary of defense of the United States of America, Leon Panetta, once said that "Next Pearl Harbor we confront could very well be a cyber-attack"(Lee, 2011).

On the other hand, technical development is not anymore luxury-it is a need. It defines and improves the quality of life of individuals and societies. This makes our society and every in-

DOI: 10.4018/978-1-4666-8793-6.ch020

dividual more vulnerable in every possible way- our public privacy is a share between the need for security and pursuing of the liberal concept of individuality and human rights. Access to the internet is becoming, slowly but surely, recognized human right- as well as the right to be informed as a global citizen. WikiLeaks is a good example of this, as well as the effects of social media on social movements and their influence in the creation of public opinion. The balance between ensured security and human rights implementation is receiving dimensions that are harder and tougher to be reached.

The infrastructure of the cyberspace makes things even more difficult: the new battlefield is transposed into a viral dimension that has no borders or territory, making the cyber warriors invisible and hard to be reached. Attribution of responsibility and legal aspects of state sovereignty are just a part of the problem. More than a decade has passed after the 9/11 events, and there is still a huge debate in the academic community if the Global War on Terror could be legally classified as a war at all. Terrorism itself lacks coherent definition and specific legal framework. State practice and legislation differ from one extreme to another. When combined with cyber-attacks, legal headaches become more and more intensive. Although United States of America (USA) and NATO (North Atlantic Treaty Organisation) have recognized a possibility that a cyber - attack may constitute an act of war, wider consensus is lacking. Besides that, self-defense as a recognized exception for a use of force in the context of the United Nations Charter, is receiving practical and factual concerns when applied in cyber context. Unfortunately, preemptive self-defense in cyber context can sometimes be the only defense possible and effective, but it can also constitute a scary precedent. Cyber itself has pretty wide meaning and context, so eventually applied in self-defense, it might get uncontrolled dimensions.

Cyber challenges opened many debates in the legal world. One of the main topics is if new legal norms are required rather than application and adaptation of the existing ones. Eirik Øwre Thorshaug, the former Norwegian state secretary noted in his opening remarks for a seminar in Oslo in 2012 the following:

Henry Dunant did not know much about smartphones and drones at the time of the battle of Solferino. Neither did the Swiss government at the time have problems with targeted cyber operations against vital infrastructure. As president Barack Obama mentioned in the debate this week: there are fewer horses in the American military than it used to be. The means and methods in war are constantly changing. We need to make sure that the rules of war are updated to meet these new challenges… (Øwre Thorshaug, 2012)

However, consensus is harder to be reached even in theory. Terms as "cyber-attacks," have no internationally agreed legal meaning and are used in different contexts. In such situation, in the absence of a specific legal regime and definition of cyber warfare, simultaneous analogy can be deadly dangerous in some situations. The broader cyber context and the high tech development makes things even more complex- and this issue should receive special devotion in the context of targeted killing practice and the usage of drones in counterterrorist operations, when the utmost right, protected by both international humanitarian law and international human rights law- right to life is endangered.

So, due to the lack of specific legal regime for the cyber space in counter-terrorist context, and the complexity of reaching possible consensus, current counterterrorist operations even in cyber context have to be conducted under the rules of one of the existing legal regimes that are applicable: international humanitarian law either international