What Lawyers Want: Legally Significant Questions that Only IT Specialists can Answer

Yaroslav Radziwill, University of Warwick, Coventry, UK

ABSTRACT

During the last decade international lawyers and IT specialists are brought together to conferences on issues of cyber-security. With various topics covered from such different perspectives, a clash of educations occurs. Lawyers are rarely able to understand the deep technological discussions, while legal presentations might seem too philosophical for the IT professionals, leaving them wondering, what do lawyers want and why. In this environment legal questions that cannot be answered without the deep technological knowledge possessed by the computer experts, should be formulated carefully and very precisely. Therefore, with emphasis on the jus in bello, this article aims to outline a list of issues that inevitably require joint lawyer-IT specialists dialogue and explain their significance from the point of view of international law. These issues include possibilities for digital “marking” of internationally protected objects online required under the existing humanitarian law, developing a “distinctive sign” for cyber-combatants, forewarning the enemy of incoming attacks (“carrying arms visibly”) and re-evaluating the concept of “vicinity” to dangerous installations in the context of cyber-space.

Keywords: Armed Conflict, Cooperation, Cyber-Attacks, Cyber-Combatants, Cyber Warfare, Jus In Bello

1. INTRODUCTION

The present article is a deviation from the mainstream form of legal writing and represents an attempt at direct interdisciplinary engagement of an international lawyer with computer experts. It concentrates on what the author sees as the three most important questions in international humanitarian law vis-à-vis cyber-attacks that jurists cannot answer themselves. Serious clarifications from the IT specialists are therefore required on all three of these issues. The article further tries to explain in non-philosophical terms why these questions are so important.

2. APPLICABILITY OF THE INTERNATIONAL HUMANITARIAN LAW

Contemporary international humanitarian law does not require the existence of a formal state
of war and applies to all situations of armed conflict or military occupation. The absence of specific references to cyber-attacks does not exclude them from the scope of the laws of war, since the latter were clearly developed to tackle futuristic means and methods of warfare. Therefore, cyber-attacks can trigger the applicability of international humanitarian law “to the extent that they can give rise to all required constitutive elements of an international or non-international armed conflict” (Melzer, 2001). From the way international humanitarian law conflict treats kinetic and non-kinetic weapons it would seem that consequences of any cyber-attack that can result in destruction, damage, injury or death between states would automatically initiate an international armed conflict. Though certain scholars like (Dörmann, 2004) refer to Additional Protocol 1 (hereinafter AP1) to the Geneva Conventions (hereinafter GC) and claim that cyber-neutralization of crucial military targets would do the same, there is no practical reason why international humanitarian law has to apply immediately to such situations if not followed by an actual attack, since these actions do not raise direct humanitarian concerns. The same logic applies to minor cyber-attacks on objects crucial to the financial well-being of a country (banks, stock exchanges etc.): merely “damaging” state economy is not sufficient to initiate an international armed conflict. On the other hand, what will likely trigger it is a cyber-strike that can “destroy” state economy completely – since it might indirectly, but inevitably cause significant suffering among the general population. The precise level of mental or physical anguish needed to automatically start an international armed conflict is debatable. The threshold for “initiating” an internal conflict is much higher and remains unlikely in the cyber context, since it requires violence to be protracted, attackers formally organized and exercising control over a part of territory. On the other hand, the application of international humanitarian law to cyber-attacks which are carried out in the context of ongoing international or internal armed conflict is almost never objected. Consequently, cyberstrikes in support of conventional military operations must conform to the laws of war in all possible scenarios where a sufficient nexus between cyber-attacks and an ongoing war exists.

3. TECHNICAL QUESTION 1: HOW TO MARK MEDICAL TRANSPORT?

International humanitarian law creates an obligation to mark air- and seaborne medical transport with distinctive emblems or in special cases to use distinctive signals in order to guarantee their adequate protection. Since long-distance cyber-attacks are conducted in an isolated fifth dimension of warfare (cyberspace), visual contact with the attacked physical object may be lacking (unless conducted as part of a larger operation with reconnaissance units or satellites). That raises the question how to “mark” the computers of medical transport online in order to inform the attacker of their special status, as well as to ensure its respect (Melzer, 2011).

3.1. Importance from a Legal Perspective

The degradation of civilian technology and electricity shortages, that inevitably follow any serious armed conflict, make computerized pharmaceutical factories, hospitals or food preparation facilities an unlikely luxury for any of the belligerents. On the other hand, modern medical ships and aircraft (but not medical vehicles), are prone to cyber-attacks. A cyber-attack can interfere with the proper work of navigational systems of a medical ship or otherwise jeopardize the safety onboard. The sinking of Italian cruise ship Costa Concordia in January 2012, though not a medical vessel, demonstrated the tendency to sometimes entirely rely on computers for maritime navigation and the disastrous consequences it may bring. Although even minor cyber-strikes may be said to be violating the obligation to “respect” hospital-ships set down in Article 1 of the 1907 XII Hague Convention (hereinafter...
International Journal of Cyber Warfare and Terrorism (pp. 46-59).
www.igi-global.com/article/cyber-security-crime-and-punishment/209673?camid=4v1a