Saaif Ahmed

HACKING INTO INTERNATIONAL HUMANITARIAN LAW: THE PRINCIPLES OF DISTINCTION AND NEUTRALITY IN THE AGE OF CYBER WARFARE

By: Jeffrey T.G. Kelsey

Reading Analysis

This article continues on the discussion of cyber warfare, its origins, place in our world, and what we can do to regulate it. Much like nuclear warfare, once cyber warfare began to emerge as a low risk high reward form of combat, nations began to pour resources down this path. However, since this is the world’s second time around dealing with a rapidly rising form of combat scholars have already done research and issued precautions about the usage of cyber warfare in the future.

The structure of this article begins with how cyber warfare has been used in a past present future sense, followed by the conflicts and limitations in regards to cyber warfare as states by the IHL, and finally ends with suggestions on how to alter the IHL to keep up with cyber warfare. The first thing I learned was that traditionally, sending large scale cyber-attacks through the word net, will always affect neutral countries’ access to the internet. However, I believe that in the past 10 years, there have been many updates to the infrastructure of the internet such that this may not be a problem. I also learned that cyber warfare will violate the clause of the IHL that states nations may not use a weapon that cannot distinguish between civilian and hostile. A cyber-attack through a DOS for example, will usually involve civilians regardless of the target.

The evidence for this article is plentiful. The pages are filled with footnotes that allow the reader to continue their own research if they so choose. The flow of the argument is well described and portrayed with the author including sufficient support for each major point. The one flaw that I would point out in this argument is that since it is quite old, and technology has advanced so far in the past 10 years, these arguments may not hold much merit today.