Chapter Ten
Proportionality and Precautions in Cyber Attacks

Michael A Newton

The purpose of this chapter is to re-examine the doctrinal formulation of the proportionality principle in the context of its emerging applications in cyber attacks. David Turns’ chapter dealt at length with the contours of cyber attacks; to be clear, this chapter will use that formulation yet also address the larger context of ‘cyber operations’. In doing so, I take the liberty to extend Matt Waxman’s formulation and treat a ‘cyber operation’ as ‘… efforts to alter, disrupt, degrade, or destroy computer systems or networks or the information or programs on them’. A cyber operation may rise to the level of an ‘attack’ if it results in violence or effects comparable to conventional military attacks. Revealing that a foreign intelligence service successfully hacked into a defense contractor’s system and stole some 24,000 computer files related to a weapons system under development, the former US Deputy Defense Secretary William J Lynn III stated that it is up to Congress and the President to decide when a cyber-event has severe enough consequences that it requires a military response. All States possess an inherent sovereign right to defend themselves from aggressive acts, irrespective of the nature of the attack, and an accompanying domestic process for initiating and controlling such responses. International law on

Professor of the Practice of Law, Vanderbilt University Law School. To contact the author visit Michael A Newton, Vanderbilt University Law School, <http://law.vanderbilt.edu/newton>. The inevitable errors, omissions, and oversights of this article are solely attributable to the author.


the other hand supplies the normative standards applicable to cyber operations, which inevitably flow from the established body of *jus in bello* principles when necessary. In particular, the concepts of distinction and proportionality provide the necessary predicate for planning cyber attacks, defending their legality, and assessing their role in the conflict. This chapter largely omits discussion of such non-State actors as the infamous ‘hacktivist’ group known as Anonymous, which is reportedly responsible for cyber attacks against public and private targets in the United States, Israel, China, and Britain, among other victims. The application of *jus in bello* standards to non-State actors in the context of cyber attacks flows from customary international law rather than by treaty norm, and the debates about status and immunity of such non-State actors are addressed in the chapter by Heather Harrison Dinniss. The proportionality analysis, in my view, remains largely consistent in cyber operations vis-à-vis State or non-State actors.

The modern globally connected era driven by information and interconnected civilian and military communications infrastructures presents wholly new challenges for the lawful conduct of relations between States. From the modern perspective, the overall mission will often be intertwined with political, legal, and strategic imperatives that cannot be accomplished in a legal vacuum or by undermining the threads of legality that bind together diverse aspects of a

5 ‘Hacktivist’ is defined as a person who gains unauthorized access to computer files or networks in order to further social or political ends. See ‘Oxford Dictionaries: “Hacktivist” (OUP, 2012) <http://oxforddictionaries.com/definition/english/hacktivist?q=hacktivist> accessed 01 August 2012.


