Chapter 13
What is Cyberterrorism and How Real is the Threat?
A Review of the Academic Literature, 1996 – 2009

Maura Conway
Dublin City University, Ireland

ABSTRACT

This chapter critically analyzes the academic literature on cyberterrorism produced between 1996 and 2009. It begins by detailing the origins of the concept and follows up with a brief overview of the cyberterrorism literature produced to date. The remainder of the chapter is divided into five major sections. The first of these is concerned with the definitional debates surrounding cyberterrorism, particularly the question of whether disruption of data is too minimal, given the necessary motivational factors are present, to be classed as cyberterrorism and destruction is necessary. The second and third sections are devoted to untangling cyberterrorism from hacking and cyberterrorism from cybercrime, respectively. Section four is focused upon strategies for separating the cyberterrorism hype from the reality, while section five departs from the cyberterrorism literature to draw attention to an argument from the "terrorism as communication" approach that, although it dismisses cyberterrorism as an imminent threat and thus bears similarities to much of the literature discussed in this chapter, introduces a new and different rationale for same.

1. INTRODUCTION

When it comes to the intersection of terrorism and the Internet, three phenomena are distinguishable:

1. Attacks upon or via the Internet
2. Dissemination of terrorist content
3. Other uses (e.g. the use of Internet telephony and virtual financial transfers in attack preparation, etc.)

Often, the aforementioned are grouped together under the umbrella term of "cyberterrorism". This is particularly the case in media reports where it is, in addition, sometimes difficult or

DOI: 10.4018/978-1-4666-5942-1.ch013

outright impossible to distinguish the "terrorism" component of events described as "cyberterrorism". Journalists are not the only offenders in this regard, however. A 2007 report from the Council of Europe entitled *Cyberterrorism: The Use of the Internet for Terrorist Purposes* (Sieber & Brunst), at least one of the purposes of which is to seek to bring some clarity to the area, instead complicates matters further by commingling these separate issues in the report's title. The present author has repeatedly argued for distinguishing between (1) previous list, so-called cyberterrorism, and (2) and (3), which may be deemed terrorist "use" (or "misuse") of the Internet (Conway, 2002a; 2002b). Although immediately post-9/11 fears about the threat posed by cyberterrorism rose sharply, in the years since the focus has shifted to terrorists' everyday uses of the Internet for information provision, radicalization and recruitment, financing, networking and information gathering, and a host of other purposes. A particular emphasis is now placed on (2) previous list, the dissemination of terrorism-related content and its impacts, which are felt to include the facilitation of both violent radicalization and attack preparation (See, for example, Conway & McInerney, 2008; Ganor, Von Knop & Duarte, 2007; Kimmage, 2008; Kimmage & Ridolofo, 2007; Stevens & Neumann, 2009). The changes wrought by the events of 9/11 and their aftermath in this area are therefore considerable, with my observation in 2002 that "Terrorist 'use' of the Internet has been largely ignored…in favor of the more headline-grabbing *cyberterrorism*" (Conway, 2002a, p. 3) having been almost entirely reversed since, with the effect that a large part of the literature on cyberterrorism discussed herein dates from an approximately five year period immediately pre- and a small window post-9/11.

The waning of both scholarly and public interest in cyberterrorism the further we are removed from the attacks of September 2001 is reflected in the number of hits returned for the search term "cyberterrorism" in Google at different points in time. When I first began recording these figures in 2001, the number of hits returned was just 28,100; the same search conducted in summer 2005 returned some 319,000 hits, while the most recent search–conducted in early October 2009–returned only a slightly increased 347,000 results. On the other hand, it is worth pointing out here too that, despite the presence of large numbers of terrorist organizations and their supporters online, no act of cyberterrorism–narrowly defined, of which more below–has ever yet occurred. The point is not that cyberterrorism cannot happen or will not happen, but that it has not happened yet and, I will argue in my conclusion, is unlikely to occur in the near future.

Why persist then in addressing the cyberterrorism issue? Because, to reiterate, it is important to be clear with respect to what types of acts might constitute cyberterrorism and to distinguish these from contemporary terrorist "use" of the Net, which does not. On a more personal note, but relatedly, it has been the author's experience–at conferences, in lectures, etc.–that a failure to address the cyberterrorism issue causes considerable confusion for audiences who are then under the misapprehension that when one is speaking about contemporary terrorist Internet use, one is actually referring to "cyberterrorism," but there is some unspecified difficulty in employing the term. It seems to me that these difficulties are likely to be exacerbated further by the renewed interest in cyber conflict arising out of the 2007 Estonian cyber attacks, which were most often referred to in the press as a "cyberwar," but were also described by more than a few news outlets as "cyberterrorism." See, for example, Simon Finch's (2007) "Cyber Terrorism is Real – Ask Estonia" in the UK *Telegraph*. It is absolutely crucial because of this and similar misapprehensions, which are not just restricted to journalists but afflict some scholars also, to devote some considerable space to a description and analysis of the cyberterrorist threat and attendant literature with a view to