Chapter 14
From “Cyberterrorism” to “Online Radicalism”

Maura Conway
Dublin City University, Ireland

ABSTRACT
This chapter explores the changes that have taken place in the role and functioning of the Internet in terrorism and counter-terrorism in the past decade. It traces the shift in focus from a preoccupation with the threat of so-called “cyberterrorism” in the period pre- and immediately post-9/11 to the contemporary emphasis on the role of the Internet in processes of violent radicalization. The cyberterrorism threat is explained as over-hyped herein, and the contemporary focus, by researchers and policymakers, on the potential of the Internet as a vehicle for violent radicalization viewed as more appropriate albeit not without its difficulties. This change in emphasis is at least partially predicated, it is argued, on the significant changes that occurred in the nature and functioning of the Internet in the last decade: the advent of Web 2.0, with its emphasis on social networking, user generated content, and digital video is treated as particularly salient in this regard. Description and analysis of both “negative” and “positive” Internet-based Counter Violent Extremism (CVE) and online counterterrorism measures and their evolutions are also supplied.

INTRODUCTION
This chapter explores the changes that have taken place in the role and functioning of the Internet in terrorism and counter-terrorism in the more than a decade since 9/11. 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 gathering, information provision, radicalization, recruitment, financing, and a host of other purposes. Particular emphasis is now placed on the dissemination of violent political extremist and terrorism-related content and its impacts, which are felt to include the facilitation of both violent radicalization and attack preparation (Bermingham et al., 2009; Conway & McInerney, 2008; Ganor, von Knop, & Duarte, 2007; Stevens & Neumann, 2009). The changes wrought by the events of 9/11 and their aftermath in this area are therefore considerable, with my 2002 observation that “Terrorist ‘use’ of the Internet has been largely ignored . . . in favor of the more headline-grabbing ‘cyberterrorism’”
(Conway, 2002, p. 3) having been largely reversed since albeit the cyberterrorism threat continues to fascinate and divide.

This chapter is composed of three main sections. The first section is concerned with cyberterrorism, and contains three arguments on the basis of which it is believed that cyberterrorism is unlikely in the near future. Section two is therefore concerned with the contemporary violent online Jihadi milieu and the changes that have taken place within it in recent years. The current focus on the Internet as a potential vehicle for some individuals’ violent radicalization rather than for cyberterrorism purposes are the correct focus; albeit an area in which there are many controversies, some of which are outlined in this section. The chapter’s third section briefly describes and discusses Internet-based Counter Violent Extremism (CVE) and present-day online counterterrorism measures.

ON CYBERTERRORISM

Dorothy Denning’s (2006) definitions of cyberterrorism are probably the most well known and respected. Her most recent attempt at definition refers to cyberterrorism as composing

...highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction or disruption against digital property (Denning, 2006, p. 124).

Analyses of cyberterrorism can usefully be divided into two broad categories on the basis of where the producers stand on the definition issue: those who wish to incorporate not just “use,” but a host of other activities into the definition (Macdonald et al., 2013). The literature can also be divided on the basis of where the authors stand on the magnitude of the cyberterrorism threat. Dunn-Cavelty (2007) uses the term “Hypers” to describe those who believe a cyberterrorist attack is not just likely, but imminent, and the term “De-Hypers” to describe those who believe such an attack is unlikely. Most journalists, excepting dedicated technology journalists, are hypers as are sizeable numbers of academics. In a recent survey, carried out by the University of Swansea’s Cyberterrorism Project, for example, 58% of researchers surveyed view cyberterrorism as a significant threat whilst, in response to a separate question, 49% evinced the view that cyberterrorism has already taken place (Macdonald et al., 2013). Despite the presence of large numbers of terrorist organizations and their supporters online, it is this author’s position that no act of cyberterrorism has ever yet occurred and the threat is over-hyped. I am thus emphatically a de-hyper; below, I lay out the three major reasons why.

Three Arguments against Cyberterrorism

The three most compelling arguments against cyberterrorism are:

1. The argument from Technological Complexity;
2. The argument regarding 9/11 and the Image Factor; and
3. The argument regarding 9/11 and the Accident Issue.

The first argument is treated in the academic literature; the second and third arguments are not perspectives to which either journalists, scholars, or policy makers appear to have devoted a lot of thought or given adequate consideration, but ought to.