Chapter 13
Terrorism and the Internet:
Do We Need an International Solution?

Gilbert Ramsay
University of St Andrews, UK

ABSTRACT

Over the last few years, it has often been suggested that use of the Internet for a variety of terrorist purposes constitutes a serious threat, and requires action of some kind at the international level. This chapter begins by examining the threat. It argues that the looseness of "terrorism" as a phenomenon – particularly as represented on the Internet – means that the problem may have been exaggerated. The issue, after all, is not in and of itself that terrorist organizations or individual "terrorists" are using the Internet, but rather, whether there is more terrorist violence happening as a result. This question is far from resolved, but there does not seem to be compelling evidence that there is. The chapter then considers the proposition that an "international problem" like terrorist use of the Internet requires an "international solution." It provides the observation that this formula assumes a symmetry between actions available to terrorist actors and states which may, in itself, make for unimaginative counter-terrorism policy. It then considers whether there is a residue of issues arising from terrorist use of the Internet which can genuinely not be countered at a local level, and which are not already relevant to existing international counter-terrorism provisions. Given the serious changes action here would imply for Internet governance, and the uncertainty of the gains that would be delivered in terms of security, there is probably not good reason yet for drastic international action against specifically terrorist misuse of the Internet.

DOI: 10.4018/978-1-61520-831-9.ch013

1. INTRODUCTION

Cyberterrorism is presently a matter of growing concern. This is despite that fact that it is still far from clear whether there is any such thing, and what it would be if there was. Even so, the debate has, it appears, moved from asking "what if" questions and towards the discussion of solutions. This has been evidenced in recent years by a spate of publications and initiatives dealing with "countering" various aspects of the threat of Internet-enabled terrorism. At the more technical end of the spectrum of threats this has included the foundation of IMPACT - the International Multilateral Partnership against Cyber Threats, hosted in Kuala Lumpur and, still more recently, NATO's cyber defence centre of excellence in Talinn, Estonia. The Council of Europe has issued a wide ranging report, "Cyberterrorism: The Use of the Internet for Terrorist Purposes' reviewing the adequacy of its existing conventions in the face of a cyberterrorist threat. Moving progressively further from the specter of true "cyberterrorism", concern over terrorists using the Internet for more humdrum ends has begun to produce its own literature over the question of finding solutions. Gabriel Weimann - one of the area's earliest and weightiest authorities has turned his hand (Weimann and Knop: 2008) to this with a paper which argues for the mobilization of the communications studies concept of noise as a counterterrorist weapon on the Internet. In Europe, Ryan (2007) has argued influentially for a somewhat softer approach, rooted in the mobilization of end users and "enabling stakeholders" as a means of tackling online "militant Islamism", while in the US Davis (2006) - to name but one - has contributed a strategy for 'ending the cyber-jihad' based on a wide-ranging program for strengthening global governance of the Internet. The most recent addition to this literature, at the time of writing, has been Stevens and Neumann's recent report from the Centre for the Study of Radicalization and Political Violence at King's College London on "Countering Radicalisation on the Internet".

No such ambitious program will be set forth in this chapter. Rather, the aim will be to examine to what extent "cyberterrorism" or, more generally, the confluence of terrorism and the Internet presents a genuinely new set of phenomena such as to require a special type of counterterrorist response and, in particular a response within the context of the current actions on terrorism being carried out by the United Nations. This will be a somewhat more speculative exercise than might, perhaps, be hoped. Necessarily so, however, as the phenomena which are being addressed are, it will be argued, still rather more nebulous than they are sometimes presented as being.

2. CONCEPTUALIZING USE OF THE INTERNET FOR TERRORIST PURPOSES

In order to determine what type of response might be appropriate in the face of terrorism arising from use of the Internet, it is necessary first to determine what such a situation would actually mean. For one thing, it is now a matter of fairly widespread scholarly agreement that not all uses of the Internet which relate to terrorism are meaningfully described as "cyberterrorism". This point has been made emphatically by both Denning (2001) and Weimann (2005), who argue for a relatively constrained definition of cyberterrorism to include only terrorist attacks accomplished electronically by means of the Internet (there is some question in Weimann's analysis as to whether physical attacks on Internet infrastructure might also be included). This means, by contrast, that use of the Internet in a support role by groups carrying out terrorist attacks in other ways or, on the other hand, politically motivated "hacktivist" activities which are annoying but which fall short of the level of carnage and scariness required of a terrorist attack do not qualify.