Chapter 88
Psychological and Behavioral Examinations of Online Terrorism

Sheryl Prentice
Lancaster University, UK

Paul J. Taylor
Lancaster University, UK

ABSTRACT

It has long been recognised that terrorists make use of the internet as one of many means through which to further their cause. This use of the internet has fuelled a large number of studies seeking to understand terrorists' use of online environments. This chapter provides an overview of current understandings of online terrorist behavior, coupled with an outline of the qualitative and quantitative approaches that can and have been adopted to research this phenomenon. The chapter closes with a discussion of the contentious issue of ethics in online terrorism research. The aim of the chapter is to equip readers with the necessary knowledge and skills to conduct their own research into terrorists' online behavior, taking best ethical practices into consideration when doing so.

INTRODUCTION

This chapter is the first of its nature to bring together separate applied approaches to the study of online terrorist behavior, which all ultimately seek to establish patterns in and between the online behaviors of particular individuals and/or groups. These patterns are studied with a view to gaining insights into the terrorist mindset (or rather, the mindset of specific groups or individuals), their beliefs, motivations, and influence tactics. It is important to note that these approaches tend to rest on the theoretical assumption that one's behavior (such as the language one uses) reflects one's psychology, an approach advocated by scholars such as the social psychologist Michael Billig. However, this position is not without its critics, due to a concern that the relationship between cognition and behavior may not be as direct as is often assumed (Carruthers, 2002). Nevertheless, such approaches have value in the sphere of cyber security,

DOI: 10.4018/978-1-5225-7909-0.ch088

in that they aim to assist in the identification and tracking of behaviors associated with certain terrorist groups or individuals online for the purpose of monitoring risk and deploying targeted counter measures.

The internet has created a myriad of opportunities for both would-be and established terrorists. These opportunities range from communication, to dissemination, to fundraising, and online warfare. With the diversification in terrorists' use of the internet, it has become of paramount importance for both academics and practitioners alike to create, or have at their disposal, a range of approaches for tackling the threats posed by terrorists online. The aim of this chapter is to provide an overview of recent advances in both manual and automated approaches to examining terrorists' online behavior, drawing on work from a variety of disciplines, including psychology, linguistics, computing, criminology, religious studies, politics, and international relations. To fulfil this aim, the chapter will be split into two separate, yet complementary sections: one emphasising online terrorist behavior, and the other reviewing methods.

The section on terrorist behavior will begin by discussing varying definitions of terrorism and evaluating how well such definitions capture modern developments in online terrorism. This will be followed by a description of online terrorist users and their source and content preferences. The section on methods will begin with an overview of manual approaches to online terrorist behavior (including content, discourse, report and framing analyses), before moving to an outline of automated approaches (such as the corpus linguistic approach, the automated psycholinguistic approach, sentiment analysis, social network analysis and data mining approaches). The method section will include focused studies to give the reader a clearer understanding of how the manual and automated approaches are applied in practice. The chapter will conclude with a section on ethical considerations. The aim of the section will be to demonstrate best procedure in online terrorism research by highlighting the factors that individuals must consider when undertaking research of this nature. As such, the central objective of the chapter will be to equip researchers and practitioners with the tools to conduct their own research into online terrorist behavior.

BACKGROUND

Before turning to the main content of the chapter, it is first of importance to understand what is meant when one refers to online terrorism. With this in mind, this section of the chapter will explore differing definitions of terrorism and discuss their suitability for the description of contemporary online terrorist behavior. Numerous scholars have discussed the difficulty of arriving at one overarching definition of terrorism, given the complexity of this phenomenon (Dedeoglu, 2003; Schmid, 2004; Weinberg, Pedahzur & Hirsch-Hoefler, 2004). Indeed, according to Ruby (2002), this complexity is due, in part, as to whether one is attempting to define terrorism in legal, moral or behavioral terms. Defining terrorism in online environments suffers from the same inherent difficulty as defining terrorism in offline environments in this regard.

Terrorism is legally defined in the UK within the Terrorism Act 2000 as:

An action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause. (HMG, 2011, p. 108).