Chapter 17
"On the Internet, Nobody Knows You're a Dog": The Online Risk Assessment of Violent Extremists

Neil D. Shortland
University of Massachusetts – Lowell, USA

ABSTRACT

Online behaviour can provide a unique window from which we can glean intent. From an intelligence standpoint it provides an important source of open-source information. However, making inference of intent from online activity is inherently difficult. Yet elsewhere progress is being made in incorporating information online into decisions regarding risk and offender prioritisation. This chapter synthesises lessons learnt from studies of risk assessment of violent extremists, risk assessment online, and the form and function of extremist materials online in order to begin to approach the issue of online risk assessment of violent extremism. In doing so it highlights issues associated with the diversity of online extremist behaviour, the diversity of offline extremist behaviour and the general lack of understanding related to the interaction of online and offline experiences, and how this contributes to the wider psychological process of 'radicalisation'. Implications for practitioners are discussed.

INTRODUCTION

Computers have enabled people to make more mistakes faster than almost any invention in history, with the possible exception of tequila and hand guns. (Mitch Ratcliffe)

This chapter focuses on the potential utility that online-gleaned information (i.e., information pertaining to an individual's online activities) offers for issues regarding the prioritisation and investigation of individuals who are or may in the future undertake extremist activities. Specifically this chapter presents the results of a systematic review that integrates a diverse range of literature covering extremism online, risk assessment online, and the risk assessment of extremists.

DOI: 10.4018/978-1-5225-0156-5.ch017

The earliest discussions of extremist materials on the Internet focused on how extremist organisations might use this new technology as a weapon or as a target (see Collin, 1996). Terms such as 'computer terrorism', 'cyberterror' and 'cyberjihad' have all been used to refer to activities that involve the destruction or sabotage of corporate assets achieved through hacking into computer systems (Bowman-Grieve, 2015). While cyberterrorism remains a top-tier security threat, 'cyberattacks' by extremist organisations have, as of yet, not materialised (Weimann, 2004). The more pressing concern however is the use of information technology as a facilitator for offline extremist activities rather than as a weapon or target in and unto itself. Extremist organisations currently use information technology, specifically the Internet, as a platform to recruit, deliver threats, release instructional materials to facilitate the actions of others, and plan and coordinate violent extremist attacks (Weimann, 2006). Currently the Internet is playing a central role in facilitating the process through which western individuals join foreign insurgencies (such as the Islamic State in Iraq and Syria [ISIS]) by facilitating contact and planning between would-be-recruits and recruiters. Extremist materials on the Internet have also facilitated attempts to launch domestic attacks (see Lemieux, Brachman, Levitt, & Wood, 2014). When discussing the impact of online extremist media, such as the well-known *Inspire* magazine (a media outlet of Al-Qaeda in the Arabian Peninsula [AQAP] which advocates and provides instructional materials to facilitate 'lone actor' attacks), the United Kingdom's domestic security service (MI5) states that:

... we can now say that Inspire has been read by those involved in at least seven out of the ten attacks planned within the UK since its first issue [in 2010]. We judge that it significantly enhanced the capability of individuals in four of these ten attack plots… this is pernicious. It radicalises, it exhorts violent action and it gives recipes or instructions on how to do so.

It is clear then that the Internet facilitates extremist activity. However it is also a double-edged sword. For example, in 2012 when Ted Poe, chairman of the United States Subcommittee hearing on the evolution of terrorist propaganda on Internet, requested that the Federal Bureau of Investigation (FBI) do more to counter extremists' use of the Internet, the FBI refused, stating that "they gained intelligence about groups and individuals from their social media activity, even though it is apparent that this social media activity recruits terrorists who want to kill"[1]. Discussing whether such materials should be on the Internet (and the legal/technological efforts to remove it) is outside the scope of this chapter but is covered elsewhere (e.g., McNeal, 2008); instead this chapter focuses on how, if at all, this type of materials can be used by law enforcement agencies to facilitate efforts to protect the public from the threat of terrorism.

THE ISSUES OF BEING 'ONLINE'

Issue 1: Anonymity

In 1993 Peter Steiner published a cartoon for the New Yorker titled 'On the Internet, nobody knows you're a dog'. This cartoon highlighted the core principle of the Internet that users can act with relative anonymity. While anonymity has clear counter-security benefits (see Weimann, 2004, 2006), it also has a profound psychological effect on our behaviour. Zimbardo (1969) argues that anonymity (amongst other factors) leads to de-individuation and disinhibition resulting in hostile behaviour. Prentice-Dunn and Rogers (1982, 1989) state that a reduction of 'accountability cues' and self-awareness leads to a