Chapter 11
Internet Use and Violent Extremism:
A Cyber-VERA Risk Assessment Protocol

D. Elaine Pressman
Carleton University, Canada & International Centre for Counter-Terrorism (ICCT) – The Hague, The Netherlands

Cristina Ivan
Mihai Viteazul National Intelligence Academy, Romania

ABSTRACT

This chapter introduces a new approach to the risk assessment for violent extremism that is focused on cyber-related behaviour and content. The Violent Extremist Risk Assessment (VERA-2) protocol, used internationally, is augmented by an optional cyber-focused risk indicator protocol referred to as CYBERA. The risk indicators of CYBERA are elaborated and the application of CYBERA, conjointly with the VERA-2 risk assessment protocol, is described. The combined use of the two tools provides (1) a robust and cyber-focused risk assessment intended to provide early warning indicators of violent extremist action, (2) provides consistency and reliability in risk and threat assessments, (3) determines risk trajectories of individuals, and (4) assists intelligence and law enforcement analysts in their national security investigations. The tools are also relevant for use by psychologists, psychiatrists, communication analysts and provide relevant information that supports Terrorism Prevention Programs (TPP) and countering violent extremism (CVE) initiatives.

INTRODUCTION

The use of the Internet around the world is increasing. Internet use world-wide has grown from an estimated 2.03 billion users in 2010 to over 3 billion users in 2014 (Internet World Statistics, 2014). In some countries, the percentage of those accessing the Internet on wireless handheld devices has almost doubled in a scant two year period (Statistics Canada, 2013). The Internet serves as a platform for interaction between and among users, regardless of their physical locations around the world (Leiner et al., 2009) and regardless of their interests and intentions.

DOI: 10.4018/978-1-5225-7912-0.ch011

Cyber-expert Richard Clarke, who served as the White House Security Chief during the Clinton and George W. Bush administrations, has observed that terrorists use the Internet just like everybody else (as cited in Conway, 2006). Terrorist websites are proliferating and the use of the Internet by violent extremists is likewise increasing. The Internet offers anonymity, easy access, a lack of censorship, fast information sharing, dissemination of ideological propaganda, an inexpensive web presence and the distribution of terrorist training materials (Ogun, 2012). Ban-Ki-moon, the Secretary-General of the United Nations observed that the Internet is a prime example of how violent extremists and terrorists behave in a truly transnational way (United Nations Office on Drugs and Crime [UNODC], 2012). The United Nations is focused primarily on responses at the state level. Responses at the individual level are also essential. The individual focus is required to assess the relative risk posed by suspected or known agents and this can be accomplished with risk assessment protocols developed for national security applications.

Knowledge of the differential risk levels of potential violent extremists, returning foreign fighters and others identified as vulnerable to violent extremist actions is critical in the current volatile security context. The increasing numbers of individuals who are under some sort of surveillance and/or who may require closer monitoring is problematic for security forces with fixed resources. In order for national security personnel to keep pace with the increasing demand for monitoring of individuals, some prioritisation of these 'persons of interest' is necessary. Such prioritisation must be defensible and the decision process must be transparent in case of challenge. The current migrant situation in the Black Sea and Mediterranean regions, some of whom may represent national security risks, also calls for risk assessments. Risk clearance may become a pre-requisite demanded by European and other countries prior to resettlement.

Reliable risk judgments undertaken in a sound manner can assist in discriminating between individuals who are the target of radicalisation and recruitment from those who are disseminating terrorism related information or inciting violent extremism. Reliable risk judgments can assist in quantifying the different levels of risk that individuals may represent for a jurisdiction. These assessments are based on evidence which is available. This evidence will, in many cases, include information obtained from the subject's Internet use.

Reliable risk assessment approaches offer a framework in which one can analyse risk and determine the specific elements and indicators most pertinent to individuals. Reliable assessments can identify changing risk trajectories of individuals using controlled and repeated measures. These assessments can be supported by data acquired from Internet content, other observed behaviours, reports and background information. The prioritisation of persons identified for national security related surveillance is achievable and facilitated by the application of well-structured risk assessment protocols specific to violent extremism. The addition of detailed cyber-behavioural indicators or evidence will make such approaches more robust and relevant for the current cyber-age.

RISK ASSESSMENT, CYBER ELEMENTS AND VIOLENT EXTREMISM

Cyber information often provides the most accessible empirical evidence on individuals under surveillance. The FBI is reported to be ramping up the monitoring of Twitter and they have cited the use of suspects' tweets in several recent terrorism cases (Reilly, 2015). In one case, Bilal Abood, age 37, was arrested in Texas in part due to his Twitter activity. He had used his Twitter account to 'pledge obedience' to Abu Bakr al-Baghdadi. Although Abood originally denied that he had made the pledge of allegiance