Chapter 14

Using the Internet to Plan for Terrorist Attack

David Romyn
Griffith University, Australia

Mark Kebbell
Griffith University, Australia

ABSTRACT

In this chapter, we discuss how terrorists can use the Internet as a source of information to plan for terrorist attacks. Online anonymity services such as virtual private network (VPN) are discussed, along with advantages and disadvantages of using these services. We also discuss online bomb-making instructions and highlight ways in which these can be used to the advantage of law enforcement. Finally, the use of the Internet as a reconnaissance tool for target selection is discussed, with descriptions of current and past research in this field to identify key information that is available to terrorists, and how this information can be manipulated to reduce the likelihood or severity of a terrorist attack.

INTRODUCTION

The Internet has been used in a variety of ways by terrorists, including the provision of information to others, financing terrorist organisations, communication between terrorists, the recruitment of new potential terrorists, and as an information gathering tool (Conway, 2006; Keene, 2011; United Nations Office on Drugs and Crime [UNODC], 2012). It has also been argued by some that the Internet provides a mechanism by which individuals, who would otherwise not have conducted a
terrorist attack, can self-radicalise and access the information they require to carry out an attack (Benson, 2014).

In this chapter, we will discuss aspects of how the Internet can be used by terrorists to prepare for terrorist attacks. We will also discuss how the Internet can be used by law enforcement to increase the chance of detecting terrorism before it happens, or to reduce the effectiveness of attacks when they occur. Specifically, we will discuss the use of online anonymity services such as virtual private network (VPN) and the onion router (TOR). We will also discuss the use of the Internet for instructions on how to make explosive devices. Prior research based on a ‘red-team’ design to investigate terrorist target selection and the use of the Internet as a reconnaissance tool will also be described. Finally, ways that these factors can be manipulated to reduce the likelihood and effectiveness of terrorist attacks will be explored. We conclude that while the Internet is a valuable source of information for those planning a terrorist attack, the accuracy and availability of this information can be manipulated to reduce the likelihood and effectiveness of an attack.

**TRACING TERRORIST ACTIVITY ONLINE**

While some authors (e.g., Conway, 2006; Keene, 2011; Thomas, 2003) discuss ways in which the Internet can facilitate aspects of planning and conducting a terrorist attack, other authors (e.g., Benson, 2014; Kenney, 2010; Torres-Soriano, 2012) argue that the Internet poses a risk to terrorists that use it, and a method by which law enforcement can identify and track terrorists. Both of these conclusions are partly correct.

Benson (2014) notes that while the Internet can give the perception of anonymity to those who use it, it is still possible for law enforcement to trace where information has come from and where it has gone. While this is true of the ability to monitor and trace general Internet traffic, this assertion may not be true in all cases if someone takes steps to remain anonymous online and hide their identity. An investigation of the use of online anonymity practices amongst those involved with online piracy, found a portion (17.8%) of those involved with the practice, used services such a VPN to hide their identity online (Larsson, Svensson, de Kaminski, Rönkkö, & Olsson, 2012). Antoniades, Markatos, and Dovrolis (2010) note that there are over 100,000 Internet users who are using TOR on a daily basis to hide their identity. Those involved with terrorism, who are also motivated to hide their identity online, could use these same methods to make tracking them more difficult.

The use of a VPN is a reasonably robust method to ensure online anonymity. All traffic sent between a user and a VPN is encrypted, so that the content of this traffic is hidden from the Internet service provider (ISP) or any other agency that may be
Related Content

Open Infrastructure for a Nationwide Emergency Services Network
[www.igi-global.com/article/open-infrastructure-nationwide-emergency-services/4011?camid=4v1a](www.igi-global.com/article/open-infrastructure-nationwide-emergency-services/4011?camid=4v1a)

Soft Computing Modeling of Wild Fire Risk Indices: The Risk Profile of Peloponnesus Region in Greece
[www.igi-global.com/chapter/soft-computing-modeling-of-wild-fire-risk-indices/90765?camid=4v1a](www.igi-global.com/chapter/soft-computing-modeling-of-wild-fire-risk-indices/90765?camid=4v1a)

Coalitions: The Future of Healthcare in Public Private Partnerships
[www.igi-global.com/chapter/coalitions/124661?camid=4v1a](www.igi-global.com/chapter/coalitions/124661?camid=4v1a)