Chapter 13
#TerroristFinancing: An Examination of Terrorism Financing via the Internet

Michael Tierney
University of Waterloo, Canada

ABSTRACT

This article describes how the internet has come to play a central role in terrorist financing endeavours. Online channels allow terrorist financiers to network with like-minded individuals, in order to increase support, raise funds, and move wealth across the international system. For instance, the Islamic State, Hezbollah, and other groups have become adept at using these channels to finance their activities. Therefore, increased examination is required of the ways in which terrorists use the internet to raise and move funds. This study assesses some of the current trends and risks associated with online terrorist financing. Some policy options are also outlined, in order to reduce the threat of terrorist financing via the internet moving into the future.

1. INTRODUCTION

The internet has become one of the major ways in which terrorist groups worldwide recruit individuals, gain support for their causes, and finance their operations (Jacobson, 2010; Okolie-Osemene & Okoh, 2015). As a result, there have been a myriad of studies in recent years which attempt to investigate terrorists' use of the internet, and develop methods to effectively counter this activity (Jacobson, 2010; Okolie-Osemene & Okoh, 2015; Gates & Podder, 2015; Fisher, 2015; Freeman & Ruehsen, 2013). There have also been concerted efforts by governments worldwide to implement legal regimes to deter terrorists' use of the internet. For instance, Canada recently enacted legislation enabling intelligence agents to disrupt known terrorist websites, in order to deter radicalization and attacks (Zimonjic, 2016). The United States has similarly worked with social media and technology companies to deter violent extremism as part of its wider Counter Violent Extremism (CVE) strategy (Kang & Apuzzo, 2016). It has also been argued that relatively new terrorist organizations, such as the Islamic State, have gained an advantage over other groups by utilizing the internet more successfully than its counterparts (Berger

DOI: 10.4018/978-1-5225-6201-6.ch013

& Morgan, 2015; Blaker, 2015). Yet while there has been increased focus as of late on the recruitment and propaganda aspects of online terrorist activity, there has been relatively little focus on the ways in which terrorist groups use the internet to fund operations. The goal of this study is to provide a better understanding the ways in which terrorists fund their activities through the internet. As such, it will also focus on potential methods to more effectively combat terrorist financing through the internet as well.

The paper proceeds in five parts. The second section looks at some of the current literature on online terrorist financing. The third section examines specific cases in which terrorists have used internet methods to raise and move funds. New risks and potential strategies to effectively combat online terrorist financing are then discussed. Conclusions ensue with necessary areas for future research on the subject of online terrorist financing.

2. TERRORIST FINANCING AND THE INTERNET

As mentioned, terrorists' use of the internet has become a major concern for security officials across the world in recent years. Like many other users, terrorists have found that the internet is an invaluable tool to share information quickly, in order to disseminate ideas and link up with like-minded individuals (Jacobson, 2010; Okolie-Osemene & Okoh, 2015). In this manner, terrorists use the internet for a variety of purposes, including recruitment, propaganda, and financing. As scholars have also noted, the internet is an attractive option for extremists due to the security and anonymity it provides (Jacobson, 2010). Yet while there have been a growing number of studies completed on the ways in which terrorist organizations use the internet to recruit and indoctrinate others, there has been relatively little focus on the methods by which terrorists finance themselves through online activities. Some researchers have attempted to fill gaps in this area by broadly studying internet aspects of terrorism financing. However, research on this particular aspect of terrorism financing still appears to be lacking, with little focus on new methods of terrorist financing via the internet or a marrying of strategies to combat online financing trends available to practitioners in the field.

For instance, Sean Paul Ashley (2012) assessed the mobile banking phenomenon, which is prevalent in regions such as the Middle East and Africa, and provides extremists with the ability to easily connect to the internet and remit funds around the world. The decentralization of this kind of banking, due to the fact that brick-and-mortar facilities are not needed to conduct transactions, has allowed terrorist financiers to more efficiently move funds while avoiding detection from authorities. Other researchers, such as Michael Jacobson (2010), have studied the ways in which terrorists engage in cyber-crime to raise and move funds. For example, Jacobson (2010) found that online credit card fraud was a fairly major source of terrorist financing. By stealing a victim's private credit information, terrorists are able to co-opt needed funds and provide support to themselves or their counterparts. Yet as James Okolie-Osemene and Rosemary Ifeanyi Okoh (2015) note, the internet is mostly used to augment and assist activities which occur in the physical world. In this way, it would appear that the internet is far more useful as a means to move funds globally in support of terrorism, rather than simply as a method to raise funds.

Many have argued that terrorists can use a variety of means to launder money and move funds as needed. The Council of Europe (2013) stated that while online gambling does not seem to be a major venue for terrorist financing activity, there are risks associated with these online businesses. Terrorist financiers have the opportunity to develop their own online gambling sites, registered in one jurisdiction with servers in another to hinder law enforcement investigations. They can then launder funds through