EYLÜL ÖZYURT

HOW TERRORISTS USE THE INTERNET Bilkent University 2021

HOW TERRORISTS USE THE INTERNET

A Master's Thesis

By

EYLÜL ÖZYURT

Department of International Relations
İhsan Doğramacı Bilkent University
Ankara

September 2021

To My Mother and Grandmother

HOW TERRORIST ORGANIZATIONS USE THE INTERNET

The Graduate School of Economics and Social Sciences

Of

İhsan Doğramacı Bilkent University

By

Eylül Özyurt

In Partial Fulfillment of the Requirement for the Degree of

MASTER OF ARTS IN INTERNATIONAL RELATIONS

The Department of

International Relations

İhsan Doğramacı Bilkent University

Ankara

September 2021

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in International Relations.

(Assist. Prof. Dr.Tudor A. Onea)

Supervisor

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in International Relations.

(Assoc. Prof. Dr. Ozgur Ozdamar)

Examining Committee Member

I certify that I have read this thesis and have found that it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Arts in International Relations.

(Prof. Dr. Oktay Tanrisever)

Examining Committee Member

Approval of the Graduate School of Economics and Social Sciences

(Prof. Dr. Refet Soykan Gürkaynak)

Director

ABSTRACT

HOW TERRORISTS USE THE INTERNET

Özyurt, Eylül

M.A., Department of International Relations

Supervisor: Asst. Prof. Dr. Tudor A. Onea

September 2021

The advent of technology has offered various advantages to terrorist and insurgent groups as well as it has done to the states, business world, and ordinary individuals. Terrorists have been using the Internet with the purposes of propaganda; training, planning, and execution; and financing. This thesis aims to analyze how terrorists actually do use the Internet for those purposes, by which means. In that context, case studies are reviewed to explore the methods employed. Findings of this study reveal that terrorists still use the real world to carry out attacks more than they make use of the Internet for this aim. Therefore, the Internet use of terrorists has come as an adjunct to their real life activities. In that consideration, this thesis emerges as a preliminary survey trying to illustrate the link between terrorism and cybersecurity studies.

Keywords: Cybersecurity, Internet, Terrorism Financing, Terrorist Propaganda, Terrorism Training

ÖZET

TERÖRİSTLER İNTERNETİ NASIL KULLANIYOR

Özyurt, Eylül

Yüksek Lisans, Uluslararası İlişkiler Bölümü

Tez Danışmanı: Dr. Öğr. Üyesi Tudor A. Onea

Eylül, 2021

Teknolojinin ortaya çıkışı, devletlere, iş dünyasına ve sıradan bireylere olduğu kadar terörist ve isyancı gruplara da çeşitli avantajlar sağlamıştır. Teröristler interneti propaganda, eğitim, planlama ve faaliyetlerini yürütme, ve finansman amacıyla kullanıyorlar. Bu tez, teröristlerin interneti bu amaçlar için nasıl kullandıklarını ve hangi yöntemlere başvurduklarini analiz etmeyi amaçlamaktadır. Bu bağlamda, kullanılan yöntemleri araştırmak için vaka çalışmaları gözden geçirilir. Bu çalışmanın bulguları, teröristlerin hala saldırıları gerçekleştirmek için gerçek dünyayı, bu amaç için interneti kullandıklarından daha fazla kullandıklarını ortaya koymaktadır. Bu nedenle, teröristlerin internet kullanımı gerçek yaşam faaliyetlerine ikincil olarak gelişmiştir. Bu bağlamda, bu

tez, terörizm ve siber güvenlik çalışmaları arasındaki bağlantıyı göstermeye çalışan bir ön araştırma olarak ortaya çıkmaktadır.

Anahtar Kelimeler: İnternet, Siber Güvenlik, Terör Eğitimi, Terör Finansmanı, Terör Propagandası

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor Assist. Prof. Dr. Tudor A. Onea for his invaluable expertise, guidance, patience and encouragement throughout this process. I have been really lucky to have such an advisor with immense knowledge as well as great personality.

I would like to also express my gratitudes to Assoc. Prof. Dr. Özgür Özdamar and Prof. Dr. Oktay Tanrısever for taking part in my thesis committee. Their feedbacks were so precious and helpful for me to finalize my thesis.

I dedicate this thesis to my mother and grandmother who are the two most extraordinary women I have ever known in my entire life and both have thought me to stand up to any difficulty I would come across, and come out resilient. They have always been a role model to me as strong, beautiful, and independent women. I also wish to express my gratitudes to my father whom I always enjoyed engaging in intellectual conversations and talking about life itself, and to my brother who has been a lot more than a sibling to me; a best friend, if only the word can explain our peculiar communication and relationship.

I also want to thank two of my closest friends; Ecem Sıla Karslı and Deniz Selçuk. They are the craziest and unique people one could ever get to be friends with.

Their friendship since the high school years has meant a lot to me, and I could not ask anything but them always being a part of my life.

Finally, I would like to thank Suheil Damouni for his help and support to me in adopting into a new city, job, and life. He has shown me what great things are awaiting, once I choose to step out of my comfort zone. He is one of the best news editors a young journalist would be lucky enough to work with and learn a lot from. The last of the gratitudes goes to Laurie Timmers and Daniel Padwick. I am blissful to have such colleagues who have made great friends with their continuous support, encouragement and valuable views.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

"Welcome to the internet
Have a look around
Anything that brain of yours can think of can be found
We've got mountains of content
Some better, some worse
If none of its of interest to you, you'd be the first"

Above lyrics are from the first passage of Bo Burnham's recently released song, *Welcome to the Internet*. When it had been released on April 2021, it was not quite welcomed, as it did not sound like an ordinary song. However, admitting that nothing is quite ordinary with Bo Burnham, the song was accepted as it is and started to be perceived as a social criticism. It indeed confirms that we have mountains of content on the Internet and anyone can find anything in accordance with personal interests. That is to say that terrorists are no exemption from tempting nature of the Internet either. On the one hand, the advent of Communication and Internet technologies have served as a medium for

businesses, consumers, and governments to communicate with each other where one can meet and exchange ideas, perspectives, and world vision freely as democratic regimes would expect and appreciate to have. On the other hand, the very same technological advancements have immensely appreciated by terrorist organizations (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 3), and have provided these groups with the capacity to go physically disconnected and freedom of movement. For instance, terrorist groups have been publishing online magazines such as Inspire by Al Qaeda where they get to disseminate their messages, justify their causes, and show targets. They have also been spreading instructions and online manuals serving as a virtual training camp and providing information on explosives, kidnapping, cell organization, guerilla warfare, and secured communication techniques (Cohen-Almagor, 2017, p. 59). There are reports showing that ISIS members have solicited and held cryptocurrencies totaling in millions, which has allowed the organization to find necessary sources to keep operating (as cited in Tierney, 2018, p. 5).

David C. Benson (2014) lists the three primary characteristics of the Internet perpetuates the connection between terrorism and the Internet as “anonymity, abundance of information, and cheapness of communication and those work through two mechanisms to expand the operational capacity of transnational terrorism which are increased networking and increased capability” (p. 298). By its very nature, the Internet is an ideal platform for terrorist organizations

operating in the transnational context as the Internet supplies anonymity. This is essential for terrorists to go untracked while taking care of what they need to obtain through the Internet ranging from psychological warfare to recruitment, networking to fundraising (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 1; Benson, 2014, p. 298). Moreover, there is an abundance and flow of information in the Internet which only the military personnel once had access to necessary information regarding training and operational techniques and tactics. However, now, such information is relatively easier to obtain on the Internet where terrorist organizations publish online manuals to make bombs, detonate them properly, target buildings and civilians, and carry out various attacks in general. Lastly, the Internet provides terrorists with one of the cheapest way of communication. Because transnational terrorist organizations are separated by great distances, long-range communication and cheaper contact are key for the sake of operating across national borders (Benson, 2014, p. 300). Having provided these primary reasons, it is not difficult to understand why terrorists have been increasingly going online. However, the main question is how are they actually making use of the Internet? For what purposes? What are the disadvantages of terrorists' increasing online presence to states and individuals? Are terrorist groups evolving in terms of the methods they have been employing, and what are the latest trends? Do they use the Internet to carry out acts of terrorism as much as they do in real life? What kind of cooperation would it require to take countermeasures? All these aspects will be subject to a close study throughout this thesis.

1.1 Definitions

Before proceeding with the main tenets of this thesis, it is essential to establish clarity for definitions of the terms and concepts that will be subject to this very research such as terrorism, the Internet, propaganda, training and execution, terrorism financing, cyberspace, cyberterrorism, and Dark Web and Deep Web. To begin with, the Internet is a global wide area network that connects computer systems across the world. It includes several high-bandwidth data lines that comprise the Internet "backbone." These lines are connected to major Internet hubs that distribute data to other locations, such as web servers and ISPs. In order to connect to the Internet, there must be access to an Internet service provider (ISP), which acts as a channel between user and the Internet. Most ISPs offer broadband Internet access via a cable, DSL, or fiber connection. When connected to the Internet using a public Wi-Fi signal, the Wi-Fi router is still connected to an ISP that provides Internet access. Even cellular data towers must connect to an Internet service provider to provide connected devices with access to the Internet. The Internet provides different online services (IT 102 2020 Paper, 2020).

To name a few, Chrinstensson (2015) and Oxford IT Paper (2020) states that;

> *web* which a collection of billions of webpages that can be viewed with a web browser, *e-mail* which is the most common method of sending and receiving messages online, *social media* which are websites and apps that allow people to share comments, photos, and videos, online gaming – games that allow people to play with and against each other over the Internet, and lastly *software updates*

> which is an operating system and application. In the early days of the Internet, most people connected to the Internet using a home computer and through a dial-up modem. DSL and cable modems eventually provided users with "always-on" connections. Currently, mobile devices such as smartphones and tablets make it possible for anyone to be connected to the Internet anywhere and anytime. The Internet of Things has turned common appliances and home systems into "smart" devices that can be monitored and controlled over the Internet.

Moving with our main topic, most people have a vague idea of what terrorism is or what distinguishes a terror attack from others, yet they lack a concrete and precise definition of what it actually is. Indeed, there is no single definition of terrorism that can be accepted as universal and is above all others to be qualified as binding. The fact that intelligence agencies, international organizations operating in global and regional security realm, and states provide with various definitions of that very concept stem from that meaning of it has been constantly changing over the past two hundred years, and variety in definitions reflect priorities and different interests of any agency involved (Hoffman, 2006, pp. 1, 31-32). Contrary to its contemporary use, when it was first popularized as a word, terrorism had positive connotations back in French Revolution times. Initially, it was utilized to establish the order during the period of uprisings of 1789 in France (Hoffman, 2006, p. 3). David C. Rapoport (2004) referred to this era as the "Anarchist Wave" in his famous writing *The Four Waves of Modern Terrorism*. The Treaty of Versailles which put an end to World War I had paved the way for the second or "Anti-Colonial Wave". It has been marked by the principle of self-determination where empire states in mostly Europe dissolved and new states emerged. Compared to the first wave, anti-colonial causes were more legitimate to those included than the causes of the first wave. The term terrorist had gained

so many negative connotations that such a situation created a definition problem (Rapoport, 2004, p. 52). Rebels stopped calling themselves terrorists, and there appeared new descriptions such as freedom fighter that puts emphasis on purpose rather than the means. Governments took the advantage of such a loop, and began to describe rebels resorting to violence as terrorists. On the other hand, the media corrupted this language even further, and in order to avoid being repetitive some media channels referred to those as terrorists, guerillas, freedom fighter, and sometimes soldiers (Rapoport, 2004, pp. 52-53). It was around those times that the term terrorism and terrorist have gained its meaning which is more or less same with today's. When the world affairs had been witnessing the emergence of radicalism as well as nationalism during the Cold War period, it was no surprising that the third wave came into being as the "New Left Wave". As revolutionary terrorists were defeated in one country after another, the third wave began to gradually disappear at the end of the 1970s that have hosted two important events in 1979, the Iranian Revolution and the Soviet invasion of Afghanistan. This was when the fourth and current wave began to be influential, and was called as the "Religious Wave" (Rapoport, 2004, p. 54). Without a doubt, Islam has been the most important religion in this wave.

Under the light of those and particularly 9/11 terror attacks which came out to be as an indicator of evolving religious extremism which is yet to significantly influence the 21st century, Bruce Hoffman (2006) provides a criteria

distinguishing terrorists from other criminals, and terrorism from other types of crime. According to Hoffman, terrorism is;

- necessarily political in aims and motives;
- violent or use violence as a threat
- designed to have psychological impacts on not only immediate victims or targets, yet far beyond
- carried out by either an organization operating in a chain of command fashion, despite transnational nature of terrorist organizations of the 21st century, or by individuals inspired by some terrorist movement and/or leaders
- conducted by a subnational group, or non-state entity (Hoffman, 2006, pp. 40-41).

To put into pertinent sentences, Hoffman (2006) defines terrorism as "the creation and exploitation of fear through violence of the threat of violence in the pursuit of political change". He also states that "through the attention they draw by violent activities, terrorists seek to obtain leverage, influence, and power they would otherwise lack to influence political agenda in a local or international level" (Hoffman, 2006, p. 41).

Based on this detailed definition of Hoffman (2006), it is essential to touch upon how terrorism differs from crime, to be more precise organized crime, insurgency,

and guerilla warfare. The debated over the crime-terror nexus is not new; in fact, it traces back to the 1990s in the context of a discussion over the appearance of new phenomena and accompanying changes happening in conflicts, insurgency and security in general (Carrapico, Irrera, & Tupman, Transnational organised crime and terrorism: different peas, same pod?, 2014). According to the United Nations Convention Against Transnational Organized Crime,

> Organized criminal group is a structured group of three or more people, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences, in order to obtain, directly or indirectly, a financial or other material benefit (United Nations transnational organized crime assessment form (stage 2), 2000).

The fact that terrorist organizations are necessarily driven by political aims, and ready to utilize psychological methods to create fear and keep it alive diverges it from organized criminal groups. In his influential article *Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter?*, Boaz Ganor (2002) discusses;

> Insurgency is a political movement aimed at realizing a specific political goal which can be overthrowing a regime, and is subject to substantial support from local communities, when it comes to guerilla warfare it also proposes a different focus where armed small forces mostly resort to asymmetrical warfare techniques against belligerent state's conventional army". (Ganor, Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter?, 2002, pp. 290-292; Tamer, 2017).

Compared to those, the aims, motives, goals and methods of terrorism is a lot more comprehensive.

As a means by which the Internet is utilized for terrorist purposes, propaganda comes to the forefront. As a dictionary meaning, propaganda is defined as "the information, especially of a biased or misleading nature, used to promote a political cause or point of view on any specified group to benefit the sponsor either directly or indirectly" (Chatfield, Reddick, & Brajawidagda, 2015). So far, terrorism and propaganda seem going alike since they both aim for creating an impact on a mass audience to benefit the sponsor (Tugwell, 1986, p. 5). As propaganda can serve various purpose ranging from religion to politics to business, terrorism is very much politically oriented. Chatfield, Reddick, & Brajawidagda argues;

> In its relationship with terrorism, terrorist networks use the propaganda by the deed targeted against society at the global level in order to spread fear, to support the moral legitimacy of terrorism violence, to engage wider audiences with their ideologies and actions and to shift the perspectives of outsiders and potential sympathizers such as by framing suicide attacks as operations in the pursuit of martyrdom (2015).

In the recent years, terrorist organizations are increasingly turning to the Internet as an alternative training and execution option for terrorism. There has been a gradual shift from old-school terrorist training camps which is a facility established with the aim of training individuals and teaching them the methods and tactics of terrorism in accordance with both physical and psychological requirements in a very similar fashion with an army building to what has been called as *virtual training camps*. A virtual training camp for any purpose is defined as;

> Structured delivery of digital learning content and instructor interaction through the practice of distance education or online learning by an instructor or instructors outside of the a formal learning environment where there would be physical interaction with the instructor to multiple users either at the same time or different times that encourages participants to reach deep processing levels (Clayton, ARE U.S. BASED 'JIHADI' INSPIRED TERRORISTS TRANSITIONING AWAY FROM PHYSICAL TRAINING CAMPS TO ONLINE TRAINING CAMPS?, 2018, pp. 5-6).

For a virtual training camp to be associated with incitement of terrorism, there have to be practical guides in the form of online manuals, audio and video clips, information and advice (The use of the Internet for terrorist purposes, 2012, p. 8). It is also highly likely to come across detailed instructions that is easily reachable in multimedia format and various languages specialized in topics such as how to join a terrorist organization, how to construct explosives and other weapons, and how to plan and execute a terrorist attack (The use of the Internet for terrorist purposes, 2012, p. 8).

Without any doubt, terrorism costs money, although the costs of specific operations and carrying out the attacks may not be very expensive, terrorist organizations necessitate fair amount of budgets in order to function (Freeman, The Sources of Terrorist Financing: Theory and Typology, 2011, p. 461). As the Internet became a key factor for modern terrorists who had been operating in a transnational fashion, terrorism financing through the Internet has also come to the forefront for terrorism funding methods. The International Convention for the Suppression of the Financing of Terrorism defines funds that are raised and collected for terrorist purposes as “assets of every kind, whether tangible or

intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but limited to, bank credits, travelers checks, money orders, shares, securities, bonds, drafts, letters of credit" (Anika, 2019).

Through new developments in Information and Communications Technologies (ICT), cybersecurity has become crucial in the policy-making process in the recent years (Gilmour, 2014, p. 144). The Internet not only makes it easier for terrorists to communicate, coordination within terrorist cells, exchange information, plan attacks, and recruit new members, but also increasingly used as a way to commit acts of terrorism (Kadir, Judhariksawan, & Maskun, 2019, p. 334). They exchange their knowledge on online platforms that are protected by passwords and protocols, hence inaccessible to security agents and terrorism analysts to monitor shared information. This takes place within the domain of cyberspace. Cyberspace is defined as "an abstract domain, and a conceptual reality with none of the physical reality that space denotes" (Gilmour, 2014, p. 145; Kadir, Judhariksawan, & Maskun, 2019, pp. 334-335). Because cyberspace is local and global at the same time, new traditions are created within its boundaries, and it is fair to raise that traditional laws would never imagine such probabilities. Additionally, cyberterrorism is understood as "the convergence of terrorism and cyberspace" (Kadir, Judhariksawan, & Maskun, 2019, pp. 334-335). The American computer security expert Barry Collin first coined the term "cyberterrorism" back in the 1980s. Kadir, Judhariksawan, & Maskun (2019)

explains that “threats or attacks on computers where the network and information stored on it has the aim to intimidate the government and/or society for political and social purposes” (pp. 334-335). For an attack to qualify as cyberterrorism, it must cause violence against people or property, or at least cause enough harm to generate fear. Attacks that lead to death or injury, explosions, plane crashes, or water contamination would be examples. Such activities also take place in Deep and Dark Web that are not necessarily the same concepts. It has been stated that “Deep Web content is often dynamically generated, usually password protected, and otherwise not conventionally indexed by search engines. It includes “databases, web services, private information, or restricted data such as membership only websites, whereas Deep Web uses a different set of protocols and software to access content including Freenet, a peer-to-peer network designed for media and information sharing, I2P, a communication platform using encryption for anonymous connections, and the most widely used access known as onion routing using the Tor browser” (Gross, Jr., 2020, p. 343; Whittaker & Macdonald, 2020).

1.2 Hypothesis

This thesis analyzes how terrorist organizations contemporarily use the Internet with the aims of propaganda; training, planning and execution; and financing. The United Nations Office on Drugs and Crime which has been in collaboration with the United Nations Counter-Terrorism Implementation Task Force adopts a

functional approach regarding the classification of the means by which the Internet is often utilized to promote and support acts of terrorism. Accordingly, there appear six categories of the Internet use for terrorist purposes “propaganda, financing, training, planning, execution, and cyberattacks”. It has been aimed to study training, planning, and execution together due to their sometimes overlapping nature. Moreover, for an act of terrorism to be carried out, they may be perceived as the necessary points along a continuum. This thesis will not put a focus on cyberattacks by terrorists as it is believed to require an area of expertise based on Computer and Information Technology, and criminology to be able to make a thorough and reliable analysis, and it is beyond the scope. The importance of this thesis stems from the fact that it aims to reveal the latest trends in online terrorist propaganda, virtual training camps and carrying out attacks through the Internet, and online terrorism financing, since there is not a comprehensive study illustrating these latest trends through detailed real life examples. How do they make use of the newly emerging social media platforms? How do terrorist groups train themselves especially in an era where onsite training can reveal their location if they are detected? Do they use the advantages of virtual currencies as it has also become an everyday concern of ordinary individuals for investment-related purposes? The answers of those and similar other questions are believed to address the latest trends of terrorists’ use of the Internet throughout this research. Having had most of the answers to those questions, it will take us to the essential point; how can the use of the Internet by terrorists countered? Since the point is to bring clarity to the undiscovered trends of terrorists’ use of the Internet, it is

necessary to figure out what and with whom states, security and intelligence agencies, and international organizations have to deal.

Although cyberattacks have not been aimed at dedicating a space, implications of cyberterrorism and cyberwarfare are planned to be brought into discussion if deems necessary with respect to the involvement of Deep Web and Dark Web, and the use of ransomware which in fact display little overlap with cybercrime. By doing so, it is also intended to show where this research stands vis-à-vis cybersecurity studies. In consideration with all these, this thesis emerges as a preliminary survey that further research can be built from as more data that is recent is provided. There are not many scholarly pieces attempting to explore the link between terrorism literature and cybersecurity studies based on empirically accumulated data and methods revealed. This thesis also could not benefit from empirical information simply because there is not any provided. However, what this thesis signifies for the literature, despite the absence of empirical data regarding the performance of terrorist organizations on the Internet and cyberspace to carry out an actual attack, is that the latest trends of terrorist propaganda, training, and financing methods are all explored and systematically brought together in this study. Should one needs to research on the subject matter, this thesis would be a beneficial starting point to probe where to begin and what more to build on in accordance with the latest developments.

1.2.1 Propaganda

Terrorist organizations are currently using the Internet for many different purposes, and one of the primary uses is for the dissemination of propaganda. Propaganda usually takes the form of multimedia communications that provide with ideological and/or practical instruction, explanations and justifications of the causes, and promotion of terrorist activities. Terrorist propaganda serves the vital purposes of recruitment, incitement and radicalization. Moreover, The Internet has significantly increased the opportunities for terrorists to assure publicity that they used to rely on attracting the attention of traditional media such as television, radio, and print media.

1.2.2 Training, Planning, and Execution

It has been iterated that training, planning and execution categories have many overlapping attributes and, therefore, can rather be seen as a follow-up process. On that account, this thesis addresses training, planning, and execution in a single chapter. There are increasingly newly emerging media platforms that can provide terrorists with the dissemination of practical guides in the form of online manuals, audio and video clips, information and recommendation that can appear as a virtual training camp. Those Internet platforms in a way creates a community among individuals from different geographical locations who could exchange

instructional and tactical material (The use of the Internet for terrorist purposes, 2012, p. 8). Preparation and carrying out of attacks through the Internet offers logistical advantages as it also reduces the likelihood of being detected.

1.2.3 Financing

Financing aspect of terrorists' use of the Internet is one of the main tenets of this research, primarily because it constitutes a big portion of their online engagement. Without a doubt, terrorism costs money as terrorist organizations could not conduct their operations or simply maintain their existence without a stable financial inflow. Among possible sources of terrorist financing, literature does not thoroughly address the role of the Internet despite its increasing capacity to be a part of fundraising for terrorist purposes, especially with the advent of online presence in the 21st century. Conventional methods of funding terrorism on the one hand, terrorist organizations have gradually been opting for innovation in financing themselves through online donations, online credit card fraud, exploiting charitable giving, virtual currencies and the use of ransomware.

1.3 Research Design and Methodology

In this thesis focusing on terrorist organizations' use of the Internet with the aims of propaganda; training, planning and execution; and financing, various case

studies have been used for each chapter. John Gerring (2004) defines the case study as “an intensive study of a single unit for the purpose of understanding the larger class of (similar) units” (p. 342). He emphasizes that the case study method is correctly understood as a specific way of defining cases, not a way of analyzing them or a way of developing causal relations. Since this study aims to illustrate the ways that terrorist organizations go on the Internet for specific purposes, it is believed to be in best interest to choose a pertinent case study for each category of the Internet use to demonstrate what happened is actually how happened instead of accepting the literature with the current gap and merely repeating what has been already known, which apparently is not adequate to provide countermeasures.

This research is designed to hold onto small-N findings. Tarrow (2010) puts forward that “Although it is harder to generalize small-N findings, the small-N method allows researchers to examine their selected cases more comprehensively” (p. 243), and what deems necessary for this thesis to address the current gap in the literature is to examine small number of cases in depth. Lijphart (1971) says, “Science is a generalizing activity and small number of cases cannot completely constitute the basis for a valid generalization” (p. 691). Nevertheless, he also admits, “focusing on small number of cases can be a great advantage as they can be intensively examined even when the research resources at the investigator's disposal are relatively limited” (Lijphart, 1971, p. 691).

Subsequently, in chapter 3, three case studies will be reviewed to demonstrate how online terrorist propaganda is carried out with the purposes of radicalization, recruitment, and inciting to terrorism. The case of Roshonara Choudry is an important example of online radicalization. Not only is she the first British woman sentenced of a violent Islamist attack, also it has reflected a self-radicalization process based completely on online material spread by the radical cleric Anwar al-Awlaki and Sheikh Abdullah Azzam. The case displayed that without a need for communication with potential or actual terrorist supporters, the online propaganda available has been adequate for her to radicalize to an extent that she planned an attack targeting her local MP because he voted for war in Iraq in 2003. On the other hand, the case of Shannon Maureen Conley was preferred as an example of how online terrorist propaganda has almost ended up in overseas recruitment. The way that this terrorist has communicated to her was persuasive enough to get training in US military tactics and in firearms as well as first aid and nursing all with the purpose of using them in ISIS camp she was supposed to join. She was announced as one of the first attempted foreign fighter for ISIS. It was almost necessary to include the of the Christchurch attack by Brenton Tarrant in this chapter, as it was the pure example of propaganda by deed. What was unique about his case is that he livestreamed the whole attack on Facebook, and this was the first time that an actual terrorist attack has been filmed in its duration. What this case signified is that Brenton Tarrant has taken propaganda by deed into a unique level through livestreaming the atrocity on Facebook, aiming that

current technology would facilitate his message to be spread and incite like-minded individuals to terrorism.

Chapter 4 will also focus on three case studies revealing the methods of terrorists' use of the Internet with the purposes of training, planning, and execution. The case of Emerson Winfield Begolly was picked to demonstrate how an individual has involved in the Internet and, particularly, jihadist forums with the aim of expressing his radical views and providing various training materials to be an active inspiration for like-minded individuals. Until he came under the radar of an FBI agent, he has provided substantial material on "bomb-making, use of weapons of mass destruction, and solicitation to commit bombings of places for public use, government buildings, and public transportation systems within the US". Another case involving two individuals who were imprisoned for preparing an act of terrorism in the UK was chosen because it is one of the most detailed cases revealing planning and preparation process of terrorists. This case showing the plans of individuals to carry out an attack on behalf of the designated foreign terrorist organization ISIS, if not being caught prior to their plans, demonstrated that how rich the Internet is for terrorists in terms of "bomb-making techniques, security measures, guerilla tactics, weapons training and all other jihad related activities". In order to examine the methods to perform a terrorist activity through the Internet, Westgate Attack by al-Shabaab was preferred as they also presented a unique example of executing an ongoing terror attack on Twitter lasted for four days. The communication to carry out such an attack required the use of Twitter

for sending texts, asking questions, verifying the current situation sometimes via the images and videos, coordinating for the next steps, and confirming the continuity of the operation.

The cases that were picked up for Chapter 5 based on online terrorism financing came from various sources. To exemplify online donations, Nafir al-Aqsa Campaign will be examined because the group based in Israel and Palestine has been quite active in fundraising on social media sites such as Twitter and YouTube by asking for donations online. The group has disseminated religious messages and repeatedly called for funding by listing needed supplies, which in a way showed that their religious messages based a justification to demand financial support. For online credit card fraud, the case of Younis Tsouli will be analyzed, as he claimed to become "the undisputed king of internet" by terrorism experts in only two years. His case will draw the attention to how the "cellular" model of global jihad complicates the war on terrorism financing, as he was an affiliate rather than a member of AQI and has operated overseas to raise funds to sponsor both his online presence for the maintenance of terrorist content and support for the jihadi fighters. In order to figure out how charitable giving has been exploited, the activities of Pakistan-based Al-Rahmah Welfare Organization (RWO) will be subject to observation. It stands out as one of the recent cases, and they have provided financial, material, or technologic support to more than one group that namely are Al Qaeda, Taliban, and Lashkar-e-Taiba. For virtual currencies section, two different cases were picked up in order to see if this very

latest technological advancement has started to be employed by different terrorist groups. Both of the cases, one called Al-Qassam Brigades Campaign and the other one being Al Qaeda Campaign, confirmed the use of Telegram and other social media platforms with the purpose of soliciting cryptocurrency donations. The last case which will be reviewed under ransomware section was preferred not only because it is one the few cases available as an example of this very recent use of the Internet to raise funds, also the case of the Albanian Hacker created one of the "first kill lists" circulated by ISIS to generate fear and ensure publicity by pointing out targets.

Accordingly, as Gerring (2004) would suggest, all these case studies used in this research to illustrate how terrorist organizations currently use the Internet with the purpose of propaganda; training, planning, and execution, and financing do not intend to develop causal explanations, as this thesis is not based on explanatory research either. In comparison with explanatory research, descriptive research tends to ask "What is going on" and prepare the ground accordingly which involves providing historical and/or contemporary analysis of some research topics by drawing together and merging the available data (Conway, 2017, p. 78). Before making progress in developing causal explanations in the subject matter, the literature must be adequate to provide a base in its descriptive part. Maura Conway (2017) puts forward that "it is not possible to answer the question of *why* the Internet is playing a greater role in contemporary violent extremism and terrorism and provide more complex theory-informed approaches seeking to show

causal connections absent prior knowledge of *what* role the Internet is playing" (Conway, Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research, 2017, pp. 79-80). Admitting that basic descriptive research is largely missing from the field and case studies generally prove confirming evidence exactly where statistical methods and formal models fall short to come up with an explanation (George & Bennett, 2005, pp. 40-41), it is the justification of basing this thesis methodologically on descriptive research through the small numbers of case studies.

1.4 Summaries of Chapters

Chapter 2 will be devoted to the literature review where both main trends in terrorism, terrorism and the Internet, and cybersecurity literature are to be reviewed. Since the focus of this thesis is the role of the Internet in terrorist propaganda; training, planning and execution; and financing, it is essential to illustrate where this research is going to differ from cybersecurity studies as well as how it is to benefit from it in order to bring clarity to terrorists' online presence. It should be also noted that terrorism and the Internet is not one of those subject matters that has recently come under study. However, what this research aims to reveal vis-à-vis current literature is the latest trends supported by recent case studies demonstrating the innovative techniques terrorists have adopted for those purposes listed.

Chapter 3 will be covering propaganda as a method that the Internet is often employed to promote and support acts of terrorism. It will be examined how and why the contemporary models of terrorist propaganda opt for the Internet. The chapter will also be discussing how the Internet has significantly expanded the opportunities for terrorists to secure publicity through various forms of propaganda tools online. Propaganda disseminated in the form of multimedia communications providing ideological or practical instruction, explanations, or justifications has three main purposes; recruitment, radicalization, and inciting to terrorism. Accordingly, the case of Roshonara Choudry as the first British woman sentenced of a violent Islamist attack will be analyzed as an example of radicalization through online terrorist propaganda. In order to illustrate how terrorist groups get to recruit potential supporters, the story of Shannon Maureen Conley as an attempted foreign fighter for ISIS will be given. Lastly, the chapter will cover the Christchurch attack carried out by Brenton Tarrant as a unique case because of the fact that it was the first attack that an actual terror attack has been livestreamed on Facebook in its duration. Along with his aim at gaining publicity through a pure example of propaganda by deed, goals listed in his manifesto displayed an example of inciting to terrorism.

Chapter 4 will be dedicated to terrorist organizations' use of the Internet with the purpose of training, planning, and execution. Given that there are increasingly newly emerging media platforms for the dissemination of terrorist guides, it is to

be analyzed how those platforms perform as a virtual training camp for terrorist organizations. Accordingly, a few tweets leading to necessary links and information posted by ISIS trainers, and the case of Emerson Winfield Begolly will present examples of virtual training camps. Planning and preparation phases of an act of terrorism utilizing the Internet will be illustrated by a case involving two individuals who were imprisoned for preparing an act of terrorism in the UK. Subsequently, it will be analyzed that how the use of the Internet with the purpose of execution of acts of terrorism may offer logistical advantages and reduce the likelihood of perpetrators being detected. The Westgate attack by al-Shabaab will come along to reveal how a terrorist organization has made use of the Internet through Twitter for an ongoing attack lasted for four days.

To finalize, chapter 5 will examine how terrorists make use of the Internet with the purpose of raising funds. The ways in which terrorists use the Internet to raise and collect funds will draw attention to those trends in terrorism financing literature does not much address innovative methods employed through the Internet. Conventional ways of financing terrorism such as state sponsorship, popular support, legal activities& legitimate investments, and illegal activities will be reviewed. Then, early examples of terrorism financing through the Internet will be given some space in order to show the evolution of terrorism financing activities taking place online and in cyberspace. The reasons to opt for the Internet as a source of finance will establish the base before moving with the most used methods of fundraising through the Internet. Online donations, online credit card

fraud, exploiting charitable giving, and, with a special focus, use of the virtual currencies as well as ransomware will be analyzed with a pertinent case study for each method listed.

Chapter 6 which is the conclusion section of this research will be putting findings from each chapter in order to make sure that readers by this point would have a clear sense of how the Internet has been utilized by terrorist organizations with the purposes of propaganda; training, planning, and execution; and financing. Concluding remarks will make it clear to see the analysis and what sort of evidence confirms the role of the Internet within this specific context of terrorism, how this research contributes to the literature on terrorism and cybersecurity at the very least, and what kind of policy implications come to the forefront in order to combat the use of the Internet for terrorist purposes.

CHAPTER 2: LITERATURE REVIEW

9/11 terror attacks targeting the World Trade Center in New York have been accepted as a milestone in terrorism and security scholarship because of the fact that what it has represented as well as the damage and casualties it has left behind. Taking this breakthrough in the way that any state has come under attack until 9/11 as his focus, Lawrence Wright (2007) bases his book *The Looming Tower: Al-Qaeda and the Road to 9/11* on the context in which al-Qaeda emerged. In order to draw attention to the story of those in the CIA and FBI who have witnessed the emergence of the organization and tried to assess the threat, but fell short of the attempt due to the lack of cooperation and unwillingness to share intelligence from the beginning, he also illuminates the US officials who confronted Al Qaeda such as the FBI agent John O'Neill. Similarly, Daniel Benjamin and Steven Simon (2002) in *The Age of Sacred Terror* introducing radical Islam, terrorism, the Middle East, and the US foreign policy shaped with respect to those provide us with an analysis revealing miscommunication within the pertinent US institutions. It was revealed that there was a big miscommunication between the FBI and White House at a time, and the FBI did

not even perceive Al Qaeda as a national security concern (Benjamin & Simon, 2002, pp. 300-306).

As the head of the CIA's "bin Laden Unit" until 2004, Michael Scheuer (2006) provides us with a valuable account of Osama bin Laden, his background, and organizational structure in *Through Our Enemies' Eyes* [1]. Scheuer (2006) criticizes the American and other Western leaders for describing bin Laden as a "terrorist problem instead of a manifestation of a religious issue". According to him, the presence of Osama bin Laden and threat he has been posing should not be contextualized as a political or social phenomenon. Scheuer (2006) puts forward that Osama bin Laden has perceived the Middle East policies of White House and George W. Bush as a justification of staying close to oil resources and keeping their private companies in business. Bin Laden also assesses that if they had not retaliated, neither the US nor the rest of the world would have comprehended how traumatic effects the US has left on the region. On that note, what 9/11 terror attacks have aimed has in fact nothing to do with getting revenge from the American people in a tit-for-tat manner, rather to show the whole world what the Middle Eastern people of Lebanon, Palestine, Iraq and Afghanistan have gone through, and how they have suffered since the 1980s. As a supportive argument, Martha Crenshaw (2017) discusses that the tendency to opt for terrorist

[1] First published in 2002, it was anonymous. Through Our Enemies' Eyes was written by a long-serving Central Intelligence Agency officer. The nature and importance of its author's national security work required that he remain anonymous. Michael Scheuer revised the version that is subject to review in 2006.

behavior of extremist groups stems from the strategic reasons rather than psychological or social factors driving such groups to emerge in the first place. Employing rational choice theories, to be precise the strategic choice framework, she argues that resorting to terrorism does not have to be perceived as the state of abnormality given that conditions may prepare it to be utilized as a reasonable and calculated response in order to obtain either an adjustment in the status quo or defense of the rights they feel highly threatened. Drawing parallels to the Osama bin Laden's defense, 9/11 terror attacks targeting the World Trade Center have been seen as a tool to demonstrate the rest of the world as well as the Americans how the Middle Eastern people have been subject to constant suffering.

On the contrary, Mark Jurgensmeyer (2000) perceives religious terrorism as symbolic rather than strategic, and in his view, there is an intention to impress an audience with specific terrorist acts (Juergensmeyer, 2000, pp. 160-163). His focus on "why bad things are done by people who otherwise appear to be good" (Juergensmeyer, 2000, pp. 7, 218) tends to overlook the rational choice and the degree of calculation of the groups before resorting to terrorism. Correspondingly, Jessica Stern (2003) defines a set of grievances that encourage people to employ and embrace terrorism in *Terror in the Name of God: Why Religious Militants Kill* composed of many interviews with terrorists and former terrorists (both in jail and on the loose). Those follow as alienation, humiliation, demographics, history, and territory. Her focus grievances refer to social, psychological, and political reasons leading groups to resort to terrorism, rather than employing terrorism as a

strategic act. According to her, social factors shaped by the political culture embedded in the history of countries tend to release individuals' potential to be radicalized and connect to a wider organization with a purpose of finding relief by that. In other words, there are deeper reasons than mere calculations and conducting a cost benefit analysis to decide if resorting to terrorism is more rational than continuing with the status quo. For the academics who perceives terrorism as a working means and, therefore, completely a rational choice to reach a political purpose, Max Abrahms (2006) comes up with a challenge to the controversial argument that terrorism emanates from strategically rational behavior. Basing his argument on 28 different terrorist groups, he asserts the following four hypothesis that terrorism is not the best option to resort to mainly because with respect to the targeting civilians have an exaggerated sense of terrorism's potential to lead to policy change, terrorist groups attach equal importance to achieving their intermediate objectives, even though terrorism is unlikely to pay off, it is a superior strategy to the alternatives, such as conducting a peaceful protest, and only comparatively weak groups target civilians, because attacking military targets requires a higher level of combatting techniques (Abrahms, 2006, p. 77).

Considering the push factors including social and economic reasons leading to terrorism, Krueger and Maleckova (2003) suggests that there is not much direct link between poverty or education, and involvement in terrorism. Based on their empirical analysis, members of Hezbollah's militant wing or Palestinian suicide

bombers are as well may be coming from economically advantaged families and have a relatively high level of education as there is the possibility of belonging to the economically disadvantaged and uneducated groups within the society (Krueger & Maleckova, 2003, p. 141). They highlight that "poverty at the national level may indirectly affect terrorism through the connection between economic conditions and the tendency countries to undergo civil wars". However, it does not suggest that individuals opt for involving in an act of terrorism and/or become a part of wider terrorist movements because of the lack of financial resources available to them. Hypothesizing on this, authors put emphasis on terrorism resembling a "violent form of political engagement" (Krueger & Maleckova, 2003, p. 141). They have concluded that educated people from privileged backgrounds are more likely to engage in politics, probably because political involvement requires a certain degree of interest, expertise, and commitment to the causes.

In the discussion of what leads to terrorism, Marc Sageman (2014) highlights that we are at the point of stagnation. Scholars lack primary data to be able to scrutinize empirical findings, as those are limited to undercover agents whose primary task is not necessarily fill the gap in the literature. There is this situation within terrorism research that intelligence analysts know everything but understand nothing, while academics understand everything but know nothing (Sageman, The Stagnation in Terrorism Research, 2014). For instance, for those who blame Islamic radicalism as a source to turn into political violence, Sageman

(2014) accepts that there is no doubt that ideology, including global neo-jihadi ideology, is an important part of any explanation in resorting to political violence, but still cannot explain why American government officials becoming obsessed with culture and the narrative, and how to counter it. At this point, the government funding strategy and its reluctance to share data with academia has created the division between the intelligence community and academia, preventing those who aim to shed a light on the reasons leading groups to opt for terrorism from developing useful and perhaps counter-intuitive measures. In this regard, more productive interactions between the two is encouraged.

Among the authors who address religious terrorism, Robert A. Pape (2006) presents an empirical and well-organized study within the scholarship of suicide terrorism in *Dying to Win*. He explicitly challenges the idea that Islamic radicalism is the principal cause of the expansion of suicide terrorism across the world. His key argument is "religion is barely the root cause of suicide terrorism; instead the main motive behind suicide terrorist attacks is to compel modern democracies to withdraw military forces from territory which terrorists see as homeland". As the argument holds "for suicide terrorism to be massively employed as a strategy, there must be a democratic force in the position of an occupier of a certain foreign territory". However, such an argument produced in 2005[2] falls short of explaining ISIS' preference of using suicide terrorism all

[2] The book was originally published in 2005; the paperback edition from 2006 includes a new afterword.

around the world without necessarily aiming at compelling anyone particular from a territory, as ISIS has been the force claiming control over a territory that used to belong to Syria and Iraq. Arguments that have been mostly shaped around the actions of Al Qaeda, although imported from four different case studies, have tendency to prove wrong the actions of its successor ISIS. In like manner, in his acclaimed study of *The Four Waves of Modern Terrorism* the analysis of David Rapoport (2004) on the following American intervention in Afghanistan and Iraq after 9/11 attacks proven to be a success has the similar tendency to hold inaccurate implications. Given that Rapoport's piece has been published in 2004, the focus terrorist group within the fourth wave of terrorism was Al Qaeda led and financed by Osama bin Laden. Upon his conclusion, Rapoport (2004) depicts the 9/11 terror attacks as the trigger to take necessary counterterrorism measures in order to end international terror, finally. He sees the following intervention in Afghanistan and Iraq by the Bush Administration has been a success to destroy Al Qaeda, and the organization's ability to create successors were highly unlikely which prove to be wrong to this present day. Despite temporary, the Islamic State's achievement of its caliphate in Syria and Iraq is adequately obvious evidence that neither Al Qaeda was unable to generate a successor because of an unwillingness to fight further nor they seemed to be destroyed after the American intervention in the Middle East. Therefore, it is fair to raise that Rapoport's tendency to give twenty to twenty-five years to run for the fourth way as its predecessors and, consequently, admitting that Al Qaeda seemed destroyed in the

early 2000s fell unrealistic of today's dynamics where terrorism has expanded its transnational character to the fullest.

As the subject matter started to touch more on ISIS, it would be enlightening to bring in the analysis of Cronin (2015). Her contribution to illustrate the strategic, tactical and rhetorical differences between Al Qaeda and ISIS, which can be seen as its successor, is addressed in a very straightforward manner. Given the prominent differences of ISIS which have control over the territory in both Syria and Iraq, keeping its extensive military capabilities up-to-date, funding itself, and engaging in sophisticated military operations, it justifies the argument that ISIS requires definitely different and more to-the-point counterterrorism and counterinsurgency strategies to be able to meet the threat (Cronin, ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat, 2015, p. 88). She also draws attention to the fact that cutting off Al Qaeda's funding as a countering measure worked really well which, yet, is not the case for ISIS as the organization does not need outside funding (Cronin, ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat, 2015, pp. 91-92). They are capable of financially sustaining themselves since they have been holding territory where they took key oil assets. In a way, it is fair to raise that there need to be different counterterrorism measures to prevent ISIS from financing itself, yet it does not solely stem from the fact that they do not need any outside funding. As this thesis aims to reveal how terrorist organizations use the Internet, the financing and fund raising aspect of it will be thoroughly

discussed in Chapter 5. The group has been using the Internet and cyberspace to raise funds, and especially using virtual currencies as they have become popular through the years due to their anonymous and untraceable character. Moreover, the amount of territory ISIS has been controlling has gradually diminished, and eventually the organization faced territorial defeat in 2017. What it means is that ISIS is no longer capable of financing itself through oil sales, yet it maintains operating. In that sense, countering measures need to be adopted into current conditions the way ISIS keeps financing itself in order to survive and continue operating.

Another piece from Audrey Kurth Cronin (2009) which is situated in counterterrorism literature questions policy implications and contributes to cover what has been missed and misguided in policy guidance. In *How Terrorism Ends*, Cronin (2009) examines how terrorist campaigns have met their objectives over the past two centuries, and applies these lessons to build a new strategy against al-Qaeda. According to author, the only way to understand how we would bring the end of terrorism is to analyze the three-folded relationship between group, target, and audience (Cronin, 2009, p. 8). Having provided a variety of case studies, she tries to figure out which lessons from those can be applied to Al Qaeda, and she makes this intriguing claim that although most of the previous terrorist organizations had very more or less similar characteristics in terms of modus operandi, Al Qaeda's ability to benefit the modern world as well as the traditional terrorist tactics differentiates it from the previous groups (Cronin, 2009, pp. 168-

169). In other words, she discusses that Al Qaeda has performed well at adopting at changing world, the increasing trends and the advent of the technology while enduring the core terrorist beliefs.

On the part of the fast changing world and the advent of technology, Bruce Hoffman (2006) alludes to the increasing trends through two separate chapters as *The Old Media, Terrorism, and Public Opinion* and *The New Media, Terrorism, and the Shaping of Global Opinion* in his distinguished book *Inside Terrorism*. What signifies in this comprehensive study is that he discusses how terrorists are now able to ignore conventional print and broadcast media through the Internet. Published fifteen years ago, he has foreseen that the spread of the Internet usage to terrorist organizations would provide them with the enormous communicative potential to further organizations' strategic aims, to facilitate their tactical operations, and gain and maintain publicity (Hoffman, 2006, p. 214). Bruce Hoffman (2006) points out that terrorists' tendency to use propaganda also serves for self-promotion. Gaining legitimacy among the public should be seen as a significant reason to employ terrorist propaganda while creating psychological pressure on targeted audience (pp. 198, 345).

At this point, it would be fair to raise that terrorism which comes into being as a means of political battle has always counted on several main elements which are resorting to violence, and creating and maintaining fear by that, publicly

presenting their ideas and objectives and gaining publicity meanwhile keeping up with the newest developments the modern world provides. The advent of technology has enabled terrorists to apply the most recent developments into their means of propaganda that have become an essential part of modern terrorism as it does not necessarily require terrorist organizations to resort to complex and dramatic acts of violence anymore. Boaz Ganor (2008) stressed, “Modern terrorism has become a psychological warfare where terrorists are able to reach out to their goals without a need to carry out an attack”. Through using all proper methods of psychological warfare based on the impact of media, broadcasting, and the Internet they can create panic and fear in public, affect the way targeted audience takes the subject matter, and make it seem like an ongoing threat (Ganor, Terrorism as a Strategy of Psychological Warfare, 2008, pp. 34-35). Therefore, in this modern era of terrorism, technological advancements enable terrorist groups to convey their messages very quickly and in an unfiltered fashion. Elena Pokalova (2020) explains that terrorists tend to manipulate the media and the Internet for propaganda purposes mainly because of four aims; “promotion of their ideas and causing fear among the audience, gaining support from international community as well as local population, hindering the reaction of the legal authorities and security forces, and mobilization, support and increase of the number of real or potential supporters” (p. 166).

Within the literature of terrorism and the Internet, James Okolie-Osemene and Rosemary Ifeanyi Okoh (2015) discusses that the Internet is mostly used as a

secondary source to help whatever is happening in the real world. According to them, as terrorists has been using the Internet, it has developed as an adjunct to their activities, therefore the attacks they are carrying out in real life matter more than the ones that are likely to happen on the Internet. Having doubts in that the Internet might have a significant role in violent and political extremism came from various scholars and journalists. Jason Burke (2011) stated, "Twitter would never be a substitute for grassroots activism, and it will not help al-Shabaab retake Mogadishu or the Taliban reach Kabul in any meaningful way". He also stressed that Twitter is "not much use on the, ground, where it counts" (Burke, 2011), however, in 2013, al-Shabaab has used Twitter specifically for carrying out an attack in Westgate that has lasted four for days. The use of Twitter by al-Shabaab during the attack has served the purpose of the various elements of the use of the Internet by terrorist organizations, as it will be discussed in next chapters, such as publicity and propaganda, recruitment and radicalization, commanding and control. Therefore, Burke's claim regarding Twitter seems to be refuted by that attack which took place two years after his article. Besides, Twitter has been of extensive use to terrorists for sharing training material and raising online donations, as chapter 4 and 5 will discuss with pertinent cases. Besides Twitter, in the literature there are not many studies addressing the role of Telegram and Instagram due to lack of data. As Telegram provides users with an encrypted platform and private channels, and Instagram gives freedom to circulate pictures and videos, a further research integrating the role of these two social media platforms would help having an in-depth analysis. Another important gap in the

literature of terrorism and the Internet is that there is no study showing the percentage of terror attacks using the Internet based on the performances of different terrorist organizations. This kind of evidence would bring clarity to the discussion if terrorists has been using the Internet as an adjunct to their other activities or not. Although it is generally accepted in that way, there is a little overlap between terrorists' use of the Internet and cybercrime, especially through the use of ransomware to raise funds which brings this research to the discussion of cybersecurity in general, and active ransomware groups in specific.

As Dan Patterson (2021) has recently written, it is discovered that several of the largest Russian ransomware cybercriminal gangs have collaborated and are sharing hacking techniques, data-breach information, malware code, and technology infrastructure. The most active collaborators are four groups known as "Wizard Spider, Twisted Spider, Viking Spider and LockBit". The gangs jointly control access to illicit data leak sites and custom ransomware code. It is stated, "They also associate with the larger criminal ransomware ecosystem, exert influence over smaller gangs, and license their tools to affiliates" (Patterson, 2021). What is known about their activities is that the groups Viking Spider and LockBit upload stolen information to a data breach site hosted and controlled by Twisted Spider. This information is used for phishing attacks meaning that delivering ransomware and posting to criminal name-and-shame sites used to embarrass and coerce victims. On the other hand, Kevin Collier (2021) has written on some ransomware gangs that have almost disappeared in recent months

after conducting a major attack that caught worldwide attention. He stated that "DarkSide", the group that hacked Colonial Pipeline on May 2021, disappeared from the Internet a few days later. "REvil" that is one of the most prolific ransomware gangs ever went quiet earlier this month after a sprawling attack that infected more than 1,500 organizations around the world (Collier, 2021). Those disappearances were not perceived as a big deal given how vast the ransomware underworld is. While many ransomware hackers are Russian as Patterson (2021) also pointed out, it was emphasized that the affiliates that deploy the ransomware may not necessarily be Russia-based.

Based on the potential threat ransomware groups are posing, it is fair to say that the challenges of controlling cyberspace are unique because it consists of many different actors such as government agencies, civil society, and multiple stakeholders including businesses. Considering that, the control over cyberspace is mostly in the hands of private companies, working together to secure it becomes even more complicated. In the first part of his devoted chapter in *The Oxford Handbook of International Security*, Ronald Deibert (2018) touches upon the definitional problems regarding cyberspace as it would be more effective to know how to approach, which methods to apply to secure it, and what kind of cooperation it would necessitate once we have an explicit idea of what it actually is, and is not. In the second part of his piece, Deibert (2018) takes a constructivist approach and questions cybersecurity is for whom and what. Here, threat perception comes as an essential concept since it can include different conceptual

assumptions about cyberspace as a space and place (Deibert, 2018, pp. 535-536). As the focus of the author is on trajectories of future research, he draws attention to whether applications developed in liberal democracies as well as other countries such as China contain similar policing functions, and governments are going to be allocate resources to new institutions necessary to monitor cybersecurity threats. Deibert (2018) provides audience with essential matters to consider further as the traditional response to any conventional threat factor would bring warfare and even armed conflict, yet what kind of measure needs to be taken given that there has not been a single cyber-attack resulting in loss of life (pp. 541-542). This also draws attention to the general consideration that if cyberterrorism is an exaggerated threat as Gabriel Weimann (2004) puts in his work of the early 2000s. Although there has been immense technological developments and innovations, the fact that cyberattacks do not result in actual violence remained same. However, what has changed is that way countries have increased their cyber capacities leading to that cyberwarfare currently is, almost, nothing but a recent way of waging war by states. Accordingly, Erik Gartzke (2013) offers an insight arguing that the importance of new technologies as a coercive tool is limited at best, and those favor the stronger parties, not the weak who has been desperately in war with those. Throughout the article, he touches upon that it is not enough to foresee what could happen in a world where anything and everything is possible, yet it should not lead to a fear of cyberspace. He has the belief that cyberwar promises major advantages for status quo powers like the US, although he gives the example of cyberattacks against the US computers

reportedly launched by Chinese servers. Author also discusses the warning of the former US Defense Secretary Leon Panetta that the next Pearl Harbor attack of our age could very well be a cyberattack (Gartzke , 2013, pp. 53-54). Having seen the stance of author with respect to the cyberspace's importance for states like the US, it is a bit confusing for audience to comprehend the roles of such counterarguments, as Gartzke (2013) does not seem to justify those in a systemic manner. As far as the article goes, the author seems to take a position that cyberwar is an extra to existing forms of warfare, and by itself, cyberwar would fail to conquer or compel. Although it inflicts harm to a certain degree, the effects of the Internet attacks are temporary compared to e.g. a rocket strike, or critical infrastructure targeted. Applying his view of cyberwar being a weapon of the strong, not the weak to terrorist groups, they would never have a chance to create damage to obtain their goals as they are the weak ones. However, given that there are occasional cases of damages created on states, which are not necessarily the weak actors, this argument of the author remains a bit too simplistic where he does not seem to address the importance of non-state actors, transnational entities, and the increasing capabilities of terrorists and insurgent groups on such a domain.

Jon R. Lindsay (2014) puts a specific focus on the cybertension between the US and China in his article *The Impact of China on Cybersecurity: Fiction and Friction*. Based on the intelligence leaks from Edward Snowden in 2013, he discusses that those news reflect a situation that should not be a great concern,

since it is revealed that “for every type of assertive Chinese cyber threat there are also serious Chinese vulnerabilities and Western strengths that can take an advantage of and maintain the political status quo by doing so” (Lindsay, 2014, pp. 8-9). His claim that cyberwar between United States and China is highly unlikely does not necessarily suggest that existence of cyber threats should be neglected, or the author underestimates them at all. Rather, he cautiously takes an optimistic view and proposes an analytical framework to make sense out of these threats. For this, Lindsay (2014) asks audience to see the complication between technological innovations and political environment in the relevant context (p. 11). He constructs a typology of cyber threat narratives based on different assumptions about what is possible to expect in technologically developing world. He concludes that the internet has made China and the West richer than they would otherwise be, and ambiguous friction in cyberspace is just the price of doing business (Lindsay, 2014, p. 45) which summarizes his overall view that the Chinese cyber threat to the US has been exaggerated, and China's cyber capabilities are surpassed by the West’s.

CHAPTER 3: TERRORIST PROPAGANDA ON THE INTERNET

3.1 Introduction

Terrorist organizations are currently using the Internet for many different purposes, and one of the primary uses is for the dissemination of propaganda. According to the United Nations, propaganda usually takes the form of "multimedia communications that provide with ideological and/or practical instruction, explanations and justifications of the causes and promotion of terrorist activities" (The use of the Internet for terrorist purposes, 2012, pp. 3-4). This chapter will examine how and why the contemporary models of terrorist propaganda opt for the Internet, the focus of propaganda aimed at potential or actual supporters that goes as radicalization, incitement to terrorism, and recruitment. Under each focus, there will be a case study to make the connection and illustrate how an act of terrorism with a certain motivation has been carried out. As terrorist propaganda distributed through the Internet manifests various objectives to the audiences, studying and analyzing it is surely going to give a better understanding of how to contain and prevent the exploitation of modern

communication technologies, especially the Internet, in order to recruit, incite, and radicalize individuals under the propaganda techniques.

3.2 Contemporary Models of Terrorist Propaganda

As many experts agree on, the Internet has become one of the most efficient tool for terrorist propaganda since it provides terrorist organizations with an opportunity to distribute contents directly and without a filter. Terrorist propaganda conducted through the Internet has different objectives and targets. It aims to reach out various types of audience who could be potential or actual supporters, extremists, direct or indirect victims of terrorist activities, and/or international community itself (Injac & Dojcinovski, 2015, pp. 84-85, 87). Terrorist propaganda aiming at reaching out to such groups mainly focuses on recruitment, radicalization, and incitement to terrorism (The use of the Internet for terrorist purposes, 2012, p. 4). Before moving on with the fundamental focuses of terrorist propaganda, it is vital to analyze why the Internet is perceived as an ideal domain to spread propaganda.

3.3 Why the Internet to Spread Terrorist Propaganda?

Terrorist propaganda is surely not a rare occurrence. Propaganda is as old as terrorism, and it has always used to reach political objectives. However, the

profile and techniques for terrorist propaganda have changed and adopted into developing conditions throughout the history just as terrorist organizations have benefitted the development of increasingly sophisticated technologies (Injac & Dojcinovski, 2015, p. 79). The Internet has significantly increased the opportunities for terrorists to ensure publicity that they once used to depend on the coverage of traditional media such as television, radio, and print media (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 6). Based on the frameworks of Ariel Victoria Lieberman (2017), Metodija Dojcinovski& Olivera Injac (2015), and Gabriel Weimann (2004), there appear six key ways that makes the Internet optimal tool to disseminate terrorist propaganda.

To begin with, the Internet and social media platforms provide terrorist organizations to produce and deliver numerous content directly to countless websites and individuals without any need to opt for a third party involvement (Lieberman, 2017, p. 101). If one speaks of the past when conventional media tools had been the main channel for the world to learn about terrorist incidents, it would be only specific media channels' version of covering, interpreting and broadcasting. However, terrorists currently have the ability to convey their propaganda messages to whomever, whenever and wherever they want. For instance, it is known that ISIS has been sending different messages to foreign Muslims living in the West than those who are of Middle Eastern origin. In order not to sound assertive and discourage foreigners, the organization tended to

portray jihad as a goal of reaching individual fulfillment, whereas the ones they have sent to Arabic people were reflected more like a duty of any Muslim living in the Middle East (Cottee, 2015).

In addition to be able to directly reach to anyone anywhere, contemporary terrorist propaganda through the Internet can spread to target audience with minimum effort. Geographical distance is no longer an impediment between terrorists and target groups of propaganda conducted. It requires minimum effort for both terrorists and supporters, they can easily access through the cheap means of communication (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 3). For an individual to reach to terrorism-related information, a smart phone with the Internet connection is what is needed. The Internet having global characteristics has saved terrorists considerable amount of time and energy, leading to high efficacy out of the Internet usage.

Thirdly, the fact that there is little or sometimes no regulation on the Internet and social media platforms has allowed terrorists to deliver any content that could be factually incorrect and highly manipulated (Injac & Dojcinovski, 2015, p. 87; Lieberman, 2017, p. 102). As the priorities of government organs working on national security and social media companies operating in a transnational context do not always go hand-in-hand in terms of cooperation, it is quite difficult to create a regulating and controlling mechanism for the social media platforms

where terrorists go full opportunist on these loopholes. Moreover, most social media platforms are owned and controlled by private companies, and what poses a problem with respect to that is the location in which act of terrorism is executed may fall under a different jurisdiction (Zeiger & Gyte, 2020, p. 375). Consequently, the stories posted online by terrorist are likely to go unchecked and have a certain impact on readers whose results could be too dangerous to take the risk.

As well as the abundance of terrorist propaganda material that is transmitted to supporters, the variety of those materials can also be expanded through the opportunities the Internet offers. Above all, the multimedia environment of the Internet provides content creators with an ability to combine text, graphics, audio, and video meanwhile users can get to download books, songs, posters, movies and many other forms of information (Injac & Dojcinovski, 2015, p. 87). Having limitless options to convey their messages, terrorists do not have to count on certain forms of communication and networks. Depending on their target audience, they can shape the content through which they choose to spread terrorist propaganda, and increase their impact factor significantly. As digital consumption constitutes a major part of our everyday life, it is vital for terrorists to be able to shape the content in the most effective way in order for potential supporters to be exposed to the strongest messages.

Anonymity is another element that the Internet offers as an advantage to terrorists in spreading propaganda (Blaker, The Islamic State's Use of Online Social Media, 2015, p. 2). As anonymity allows terrorists to bypass detection by law enforcement mechanisms, it is very beneficial for terrorists to deliver the content based on extremism and violence, and escape any punishment. In the past, terrorists had to use telephones or radios to disseminate propaganda that were likely to be monitored by police forces and reported to law enforcement mechanisms. Thanks to the Internet, they can hide their identities on different platforms, and if they are to be revealed they can always create other accounts to continue radicalizing individuals, recruiting potential members, and inciting to terrorism.

In relation with anonymity, encryption provides terrorist content with a more secure environment to remain unidentified, and allows terrorists to maintain private communication without being subject to an oversight of law enforcement mechanisms. In other words, the third parties cannot access networks of communication using encryption. Therefore, recruitment and radicalization efforts of terrorist organizations can be conducted in secrecy (Lieberman, 2017, p. 103). As more social media platforms, their mobile applications, and websites opt for encryption due to the concerns of the protection of individual data, it also enables terrorists to hide in the shadow while maintaining communication. Extremist propaganda can be filtered out on Facebook and Twitter because it includes violent nature displayed by graphics, although not completely cleaned out.

However, encrypted platforms such as WhatsApp and Kik that have been so popular within ISIS can smoothly transmit such kind of contents.

Having analyzed the six key ways how the advent of technology and the growing impact of Internet have changed the way terrorist organizations use propaganda, it is reasonable to continue with the fundamental focuses of terrorist propaganda. According to the report of the United Nations Office on Drugs and Crime (UNODC) published in 2012, those were listed as recruitment, radicalization, and incitement to terrorism "which can be viewed as points along continuum" (The use of the Internet for terrorist purposes, 2012, p. 6).

3.4 Radicalization

"Radicalization occurs not in mosques, but rather online, in secret…" (Blaker, The Islamic State's Use of Online Social Media, 2015, p. 4). It is a statement by Yasir Qadhi, who is a "Muslim cleric" living in the US and professor at Rhodes College in Memphis, relating to the fact that "contemporary terrorist groups are the first generation whose members were born into a world offering continuous access to the Internet and social media" (Zeiger & Gyte, 2020, p. 375). Therefore, it should not come as a surprise that social media platforms play a key role in their radicalization process whereas trying to reach out vulnerable people praying in mosques is too risky, and not needed any more. Radicalization primarily refers to

the process of persuasion that includes the transformation of potential supporters into the individuals who gets to the point of acting with violence based on extremist ideologies and objectives (The use of the Internet for terrorist purposes, 2012, p. 6). The use of terrorist propaganda can be seen as the most significant part of the series of action leading to be radicalized. The ability of terrorist organizations to produce and deliver inspiring and high quality propaganda on the Internet and social media is of great significance for their "brand management" in proper terms, and their approach to radicalization. In fact, Monica Maggioni (2015) puts into such words that "social networking sites such as Twitter, Facebook, and YouTube have become the modern day tools for disseminating the oldest core messages of terrorist organizations in a contemporary way" (p. 50). The length of time and the effectiveness of those as well as other convincing methods employed depend on individual circumstances and relationships such as push and pull factors (The use of the Internet for terrorist purposes, 2012, p. 7; Zeiger & Gyte, 2020, pp. 377-378). Pull factors in this matter can be taken as the personal objectives for joining terrorist groups whereas negative social, political, and economic conditions of the target audience constitute the push factors. All together, they contribute to an environment that is suitable for radicalization and recruitment.

When it comes to the radicalization process of individuals and sympathizers, one does not simply radicalize oneself given that lone actors are often not that alone during this phase. Although there is not a universally accepted definition of lone

wolf terrorism, there are some generalizations made out of commonalities of lone actors. Those can be put as;

> the threat or use of violence by a single perpetrator (or small cell), not acting out of personal material reasons, with the aim of influencing a wider audience, and who acts without any direct support in the planning, preparation and execution of the attack, and whose decision to act is not directed by any group or other individuals, although possibly inspired by others (Risk assessment of lone actors, 2017).

While a few individuals are described as loners and socially isolated, the literature on lone wolf terrorism tends to reveal that "there is a meaningful connection to the immediate and broader social contexts including family and friends, political movements, terrorist organizations, individual mentors, and virtual communities" (Risk assessment of lone actors, 2017). In fact, there are several typologies distinguishing types of lone actors according to their level of connectedness to a radical movement or terrorist organization, yet that is beyond the scope of research focus of this thesis. It has been stressed that most of the lone actors either had or wanted to have ties to a wider group or movements, and have been given some degree of assistance, instructions and importantly encouragement at some stage during their radicalization process (Bouhana, et al., 2018). Accordingly, two aspects of social embeddedness are taken into account; first, the lone wolves' connection to a designated organization, second, the role of the Internet and particular online publications, platforms, and/or influential figures such as Anwar al-Awlaki, whose impact on individuals' radicalization will be examined in a case study of a lone actor in the next section, in informing the lone actor's ideology. In lone wolf terrorist phenomenon, the emergence of the Internet usage as of today

and its capacity to allow holding conversation between isolated and like-minded individuals, and bring them closer to a bigger group or movement have been perceived as a factor of both *acceleration* and *incubation* (Bouhana, et al., 2018).

Given the motivations of the individuals and sympathizers, how does one access all the information needed in pursuit of radicalization and, sometimes, recruitment by a wider extremist group? Despite of their affiliation with extremist views, not every individual, in fact majority of them does not know how to access Dark or Deep Web where the actual terrorism-related activity in a transnational context lies in secured websites, chatrooms, and forums. Considering the number of people who commit acts of terrorism as lone actors or inspired by a specific terrorist group in the age of fast and accessible technology, it would be strategically wrong of terrorist organizations to remain inaccessible for the individuals who do not know where to start online or how to look for specific platforms. Therefore, many terrorist organizations and groups either have official websites where one can easily subscribe as a first step to be in touch as long as it is not suspended by law enforcement mechanisms, or extract information of the users who manage to find channels in Telegram, or retweet any related post and/or join in discussions in Twitter. Below are some pictures of Hezbollah's official website named "Eye on Hezbollah". Its setup is quite easy and guidance is straightforward to find whatever is looked for. One can get to see the history of the transnational Shiite Islamist group founded by Iran, organizational chart presenting an overview and the functioning of Shura Council, a timeline of their

advancement dating back to the early 1980s, their resources in the forms of blogs and reports written by Bob Feferman, David Daoud, or the research team of the organization, and a section entitled *perspectives* which posts weekly news round-up covering Hezbollah and Lebanon. On the top right corner, there is this part leading the user to a link that is about the objection of Hezbollah to the nuclear proliferation of Iran. Although there is not a donation part on the original webpage, *United Against Nuclear Iran* link of the website offers a donation section. It also offers a contact section as well as subscription (Eye on Hezbollah, n.d.). On the original webpage, there is a subscription section that pops up in any segment that can easily be subscribed by registering with a valid e-mail, then that user would come under the radar of digital team depending on the consistency of the interest. If the user or subscriber proves him/herself in a way that will not threaten the security, anonymity, and confidentiality of the organization, resources that are more pertinent are allocated to keep that individual as interested and sympathized as possible in pursuit of radicalization.

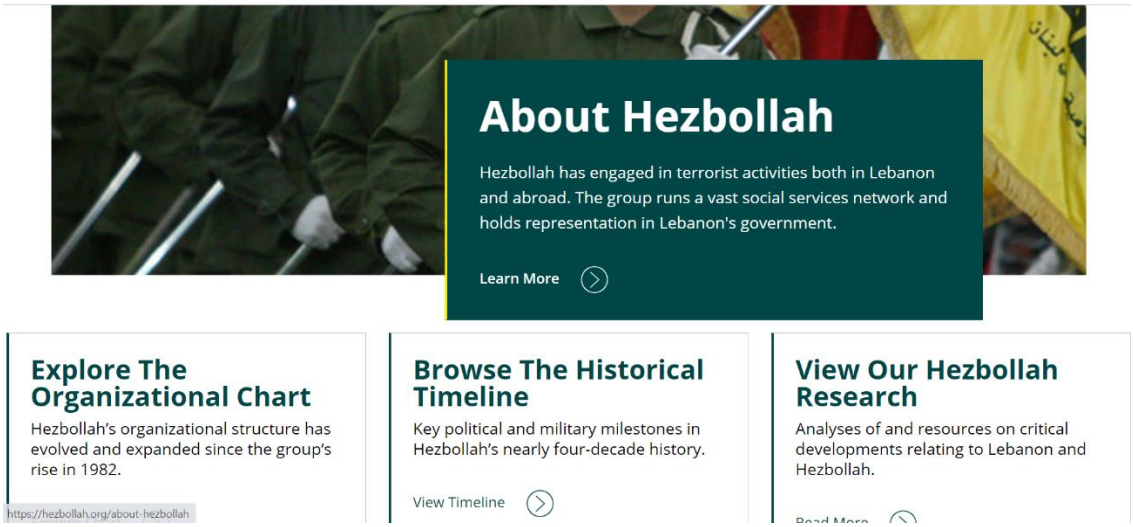

Figure 1: Eye on Hezbollah

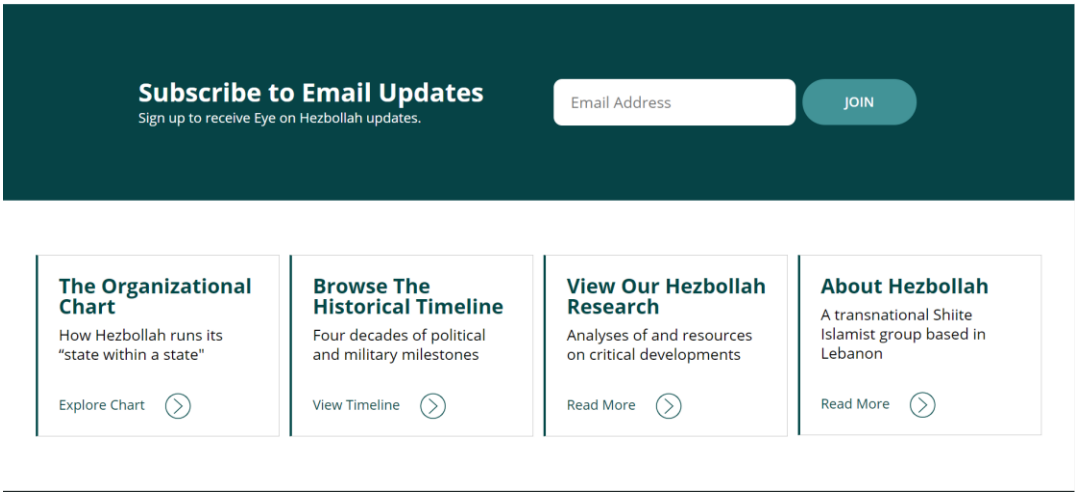

Figure 2: Subscription Part

Although the focus of this thesis covers organizational level of acts of terrorism utilizing the Internet, radicalization process starts at the individual level especially considering the impact of the Internet on becoming an extremist in an age where terrorist organizations do not necessarily consist of family members based on the

understanding on kinship anymore, yet it has true transnational nature bringing a variety of people with different backgrounds. Accordingly, the next section will examine a case study of a lone actor who has radicalized watching extremist material online, particularly the radical cleric Anwar al-Awlaki.

3.4.1 CASE STUDY: Roshonara Choudhry, the First British Woman Imprisoned for an Islamic Attack

Roshonara Choudry emerged as the first British woman sentenced of an attack motivated by radical Islam. Choudry, who was a 20-years-old university student at that time, stabbed her Member of Parliament Stephen Timms in 2010. As well as being the first British woman imprisoned of such an act of terrorism, what is significant in her self-radicalization is that the Internet appeared to be the key element in her case and, specifically, the online material spread by the radical cleric Anwar al-Awlaki has constituted the biggest part of her radicalization process (Pearson, 2015, p. 6). As it is to be stated in the case of Shannon Maureen Conley which will be reviewed under recruitment part, Awlaki was an American of Yemeni origin directly linked to Al Qaeda in the Arabian Peninsula (AQAP), and most importantly the prominent person disseminating extremist material online. His speeches had been translated into English as well, which enabled him to attract many Western supporters who are native English speakers (Pearson, 2015, p. 8).

Based on the interviews conducted by police, Choundhry emphasized her solitary exploration of Al Qaeda-related ideology, and she had revealed that it took six months for her to take a solid action after her initial exposure to extremist material, showing no signs of interest in Islam before 2009 (Dodd, 2010). According to the police examination, it was around that time she started to download of Awlaki's speeches. Choundhry told the police "she had stumbled upon his Internet sermons to the extent that watching them repeatedly even, sometimes, between lectures" (Pearson, 2015, p. 9). She has also become a frequent visitor of the extremist forum site *RevolutionMuslim* that she used the site in order to watch online footage of resistance fighting in Iraq and Afghanistan more than she has engaged in the extremist discussions (Pearson, 2015, p. 9). Around the time she dropped out of her studies as she regarded her university, King's College London, as anti-Muslim, she began planning the attack that was linked to YouTube videos of not of Awlaki, yet of Sheikh Abdullah Azzam whom she perceived as encouraging even women to fight and defend a Muslim land under attack. Choundhry has used the YouTube videos of Azzam as a justification for women to participate in fight whenever Awlaki fell short of addressing women as well as men to become fighters for Islam.

Through the website www.theyworkforyou.com, she chose her target who was her local MP Stephen Timms. She has highlighted that Timms voted for war in Iraq in 2003 and her planned attack on him came as a punishment for this

parliamentary vote. Choundhry stabbed him with a kitchen knife. He survived the attack and young woman got arrested. She claimed she has not told nobody about her plans and nobody has instructed her in her actions. She was convicted of life in prison for attempted murder (Pearson, 2015). This case demonstrated how powerful online platforms to initiate and develop lone wolf radicalization (Weimann, 2010, p. 46). It has been raised that what she represented is the emerging threat of violent extremism in a younger generation that is increasingly turning to the Internet for answers (as cited in Pearson, 2015, p. 11). The terrorist-related material online focusing on radicalizing and recruiting is so powerful and various that it is capable of providing answers for anyone interested regardless of age, gender, ethnicity, and geography. Although such case studies show how serious and risky the online attempts of sympathizers can get, governments and social media companies do not seem to engage in effective combat against continuous circulation of terrorist material available online. The lectures and speeches of Anwar al-Awlaki trace back to the early 2000s, yet ten years later it still is, somehow, available online and influential enough on its own to radicalize individuals who can eventually carry out an act of terrorism. It is important to draw attention that YouTube was not able to monitor online terrorism content posted and remove accordingly whereas governments, in this case the UK government, could not successfully scan the online movements of its citizens who show sympathy towards terrorist content and sooner or later get in touch with someone affiliated with a designated organization. Therefore, this case addresses the need of an effective cooperation between social media companies and

governments to counter terrorism propaganda online that leads to radicalization, recruitment, and incitement to terrorism.

3.5 Incitement

While propaganda by itself is not generally prohibited due to the freedom of speech and expression, the use of propaganda by terrorists on the Internet in order to incite acts of terrorism in considered illegal (The use of the Internet for terrorist purposes, 2012, p. 6). Although it is clear that the Internet and social media can be the very tools to provide accurate information and to ordinary individuals, the same tools can also be used to put countries in great danger (Incitement to Terrorism through the Media: UNODC organizes workshop on anti-terror law for Journalists, Security Agencies, 2021). In other words, depending on the usage, the materials on the Internet can become a tool for provocation to acts of terrorism. Therefore, it is important to highlight the difference between propaganda per se and the content intended to incite to terrorism as the latter is a particular concern to law enforcement mechanisms (The use of the Internet for terrorist purposes, 2012, p. 6). It was stated that in order to be responsible for incitement to terrorism, there must be a direct link between the propaganda and a specific act of terrorist. For instance, French law states that the dissemination of instructive materials on explosives would not be considered a violation of law unless spreading this message on the Internet specifies that the material shared in

preparing a terrorist attack, which is a highly controversial statement and situation (Zeiger & Gyte, 2020, p. 400). If investigators cannot show the proof that the subject matter is the exact one displayed in the content of alleged propaganda, that content and the creator have right to claim it's within the freedom of expression, thought, conscience and religion, belief and opinion (Vraneš, 2016). To see the role of the Internet in inciting to terrorism, the next section will review a significant case study, as it is the one and only terrorist attack that has been livestreamed during the course of events.

3.5.1 CASE STUDY: Brenton Tarrant, *the Christchurch Attack*

In only 36 minutes on March 15, 2019, Brenton Tarrant who is an Australian far-right extremist fatally shot 51 people in two mosques in Christchurch that marked the deadliest terror attack in New Zeeland's history. What was unique and worth allocating a place within the examples of terrorist propaganda, and propaganda by deed, is that he livestreamed the attack on Facebook. This was the first time that an actual terrorist attack has been filmed through livestream (Macklin, 2019, pp. 18, 20).

10-20 minutes before the first mosque attack took place, Tarrant logged on to the /pol/section of 8chan, which is an image board popular with the extreme right. As an anonymous user, Brenton posted; "Well lads, it's time to stop shitposting and

time to make a real life effort post. I will carry out and [sic] attack against the invaders, and will even livestream the attack via Facebook" (Macklin, 2019, p. 18). He then posted the link to his account; "By the time you read this I should be going live" (Macklin, 2019, p. 20). The post was indeed and farewell, and showed that he has been a frequent user of the platform. He also posted that (Evans, 2019):

> I have provided links to my writings below, please do your part spreading my message, making memes and shitposting as you usually do. If I don't survive the attack, goodbye, godbless and I will see you all in Valhalla!

The link referred to his 74-pages manifesto that he entitled *The Great Replacement* opened with an interview of himself narrating his journey from an ordinary man to a kebab removalist, which refers to a popular song with Bosnian Serb paramilitaries. In the manifesto, he set out his ideology and self-justification for carrying out the attack. One of Tarrant's strategic goals outlined in the manifesto was "to incite violence, retaliation and further divide between the European people and the invaders currently occupying European soil" (Macklin, 2019, p. 21). It is to say that his terrorist propaganda that went viral online has encouraged people to incite to terrorism, and raised the anti-Muslim sentiment online. While carrying out his attack had an anti-Muslim motivation, Tarrant also expressed his racist, xenophobic, and anti-immigration views (Macklin, 2019). He framed the rationale for the attack he executed as "defensive resistance", which he perceived as "a partisan action against an occupying force, and a preemptive measure to prevent a potential *white genocide* that is likely to be committed" by

those people Tarrant targeted (Veilleux-Lepage, Daymon, & Amarasingam, 2020, p. 1).

The current technology was the key element of Tarrant's attack in its preparation and planning. His manifesto also suggested that the Internet was responsible for the creation of his belief system, raising "you will not find the truth anywhere else" (Veilleux-Lepage, Daymon, & Amarasingam, 2020, p. 2). It has been pointed out "the central point of his attack was not just to kill Muslims, but to make a video of someone killing Muslims" (as cited in Macklin, 2019, p. 19). Filming the attack using a GoPro camera has given the footage the quality through the own eyes of the perpetrator turned the concept of "terrorism as theater to terrorism as a video game" (Macklin, 2019). Although such a "gamification of mass murder" was not new at that time, Brenton Tarrant has taken propaganda by deed into a unique level through livestreaming the atrocity on Facebook, aiming that current technology would facilitate his message being spread and incite like-minded individuals to terrorism. As a punishment to his act, since August 2020, Tarrant has been serving life in jail without parole making him the first person in New Zeeland's history to receive such a sentence (Christchurch mosque attack: Brenton Tarrant sentenced to life without parole, 2020). What is striking in this case is that terrorists do not make use of Facebook as much as they do of Twitter, and when they do, it is generally photos and videos circulating which Facebook usually takes an action removing within few days. For Christchurch mosque attack, it took more than two days for Facebook to remove all relevant content

because it was shared, commented, and used in separate posts many times. The fact that the first user reporting the attack on Facebook did so several hours later also contributed the livestream to be distributed immensely. The nature of the attack showed that extremists do not have limits utilizing the Internet to create publicity and incite to terrorism through their acts, although it was not necessarily a very sophisticated method used by Brenton Tarrant. He just used a very basic function of Facebook, posting a video and letting other users to see it. It should have been the social platform itself that needed to take an immediate action once it started livestreaming. Therefore, it is essential to prevent such things happening online and from granting terrorists with publicity without having to count on users to report it. Such social media platforms must be aware of the loopholes and have an effective team combatting it; especially it has been a considerable amount of time since the platform started running and has been used for similar purposes before.

3.6 Recruitment

The Internet has not only been used as a means to broadcast extremist content and rhetoric, and to wait for potential supporters to be impressed by those and approach terrorists. In addition, it has been seen as a way to develop network and relationships with those who are sympathized and more responsive to terrorist propaganda and content. As the Internet provides terrorist organizations with a

global reach, it also offers a global pool of potential recruits where "the recruiter and the volunteer get to meet in the message boards, run a series of confidence tests, and be accepted into the organization if they prove successful" (The use of the Internet for terrorist purposes, 2012, p. 5; Ogun, 2012, p. 207). Given the technological barriers to entry to recruitment platforms and cyberforums secured by restricted access also increases the difficulty for intelligence agencies and law enforcement mechanisms to track terrorism related activity on the Internet. Combined with this, the fact that terrorists use the Internet in an increasingly interactive and efficient way to roam online chat rooms and cyberforums ends up with a high success rate in recruiting sympathizers. Such individuals are generally the vulnerable and marginalized groups in society who are prone to be manipulated and brainwashed. Targeting this type of audience on the Internet, terrorist propaganda is designed to capitalize on an individual's sense of being excluded from the society, humiliation, injustice, and following no sense of belonging at all (Weimann, 2006, pp. 37-38). Although terrorist propaganda is tailored to consider demographic factors such as gender and age as well as socio-economic backgrounds, what is vital in their target selection process is that those must be vulnerable individuals who are open to be exploited for some deprivation-related reason in their lives.

When it comes to recruitment pattern of terrorist organizations, Marc Sageman (2016) highlights that radicalization and recruitment into terrorist organizations, which he addresses as neo-jihadist "because real jihad is declared by legitimate

authorities, not by individual perpetrators who target innocent noncombatants without sanction from any legitimate government" (p. 5), are similar to "the growth of cults, like that of gangs, (which) is based on friendship and kinship, what I call 'a bunch of guys". He also stresses "the path to political violence was a collective journey, not an individual one, even for so-called lone wolves" (p. 6). Accordingly, he proposes there are four components in the process of radicalization; "moral outrage at recent political events, a warlike ideology, personal experiences that resonated with this ideology, and mobilization through existing militant networks" (p. 11). Through this analysis, he mostly refers to the structure and functioning of Al Qaeda's early times where terrorists have not much considered recruiting individuals online as they have preferred people coming from their own social cycle such as family members and close friends. However, terrorist organizations who have long engaged in guerilla warfare such as Hamas do opt for different patterns of recruitment. Hamas targets three different audiences: current and potential supporters; international public opinion; and enemy publics. They also rely on e-mail, chatrooms, e-groups, forums, virtual message boards, and social networking sites such as YouTube, Facebook, and Twitter (Weimann & Mozes, 2010, pp. 211, 213). It has been stated that, the creation of virtual communities as such, the social bonding online, and the radicalization process are all instruments to take further steps in recruiting more members into the organization (Weimann & Mozes, 2010, p. 220).

Subsequently, the next section is dedicated to a case study illustrating a real life example of how Shannon Maureen Conley, an American citizen, has been radicalized on the Internet and almost recruited with an attempt to become a foreign fighter for ISIS at the age of 19. In terms of both accessibility and content of the case, it presents a significant example since it has been stated that her only interactions were via the Internet where terrorist propaganda she has been exposed to was powerful enough for her to get radicalized, convert to Islam, and attempt to move to Syria so as to recruited as a nurse in an ISIS training camp.

3.6.1 CASE STUDY: Shannon Maureen Conley, *Attempted Foreign Fighter*

In January 2015, a 19-year old American girl from Colorado, Shannon Maureen Conley, was imprisoned for conspiracy to provide material support to a designated foreign terrorist organization, namely ISIS (Blaker, The Islamic State's Use of Online Social Media, 2015, p. 7). In her own words, she has wanted to become an ISIS bride, and participate in its jihad in the Middle East (Martinez , Cabrera, & Weisfeldt, 2015). She also expressed that even though she was committed to the idea of jihad, she did not want to hurt anyone. In her view, it was all about defending Muslims (Zavadski, 2015).

According to the press release of the US Department of Justice, the conspiracy was accomplished, in part, when Conley met the co-conspirator, 32-years old

Yousr Mouelhi of Tunisian origin, on the Internet (Semko, 2015). During their communication, they shared their view of Islam as required participation in violent jihad. Mouelhi told Conley that he was an active member of a group fighting in Syria known as ISIS (Semko, 2015). He communicated to her that she needs to read and interpret Quran according to a set of principles, and sent her guidelines, a collection of videos and short films illustrating the objectives of ISIS and views of how they keep up with those in real life just as any propaganda message disseminated online and forwarded repeatedly. Having considering those and converted to Islam, she decided to marry him and move to Syria to join ISIS. When Conley was speaking to the FBI and describing how she came to that religious understanding, she mentioned Anwar al-Awlaki who has been referred as bin Laden of the Internet (Zeiger & Gyte, 2020, p. 380; Shannon Conley Sentencing, 2015). Being a US-born Imam in Al-Qaeda in the Arabian Peninsula (AQAP), he is seen as the first terrorist to fully exploit the potential of social networking sites to the English-speaking audience. He claimed that despite the quality of online propaganda produced, it was not reaching as wide an audience possible. Therefore, he took the responsibility of using of social networking sites to expand its area of online influence, and he created his own blog, Facebook account, and also a YouTube channel where he gets to regularly share his propaganda videos of high quality and sophisticated broadcasting as well as the online magazine Al Qaeda has been publishing, *Inspire* (Zeiger & Gyte, 2020, pp. 380-381).

In her testimony, Conley mentioned the importance of those online materials for her to have a better picture of Islam, their way of practicing it, ISIS and its organizational functioning including what her role and position would be there. She also told the FBI that she had received 13 disks from her husband-to-be. Those particularly dealt with what to do in a marriage, how to live the life, how to dress, and how one should approach religion (Shannon Conley Sentencing, 2015). In order for her to be of use, they decided Conley to join the US Army Explorers (USAE) to be trained in US military tactics and in firearms. She traveled to Texas and attended the USAE training. She also obtained first aid and nursing certification and National Rifle Association certification (Semko, 2015). She was going to become a nurse on an ISIS training camp (Colorado Woman Sentenced for Conspiracy to Provide Material Support to a Designated Foreign Terrorist Organization, 2015; Semko, 2015). All those materials she has been provided online helped her to get radicalized first, convert to Islam, and eventually almost be recruited as a member of ISIS. In a subsequent search of her home, they even found shooting targets labeled with the number of rounds fired and distances that shows that had she succeeded in her plan to get to Syria, she would likely have been brutalized, killed or sent back to the United States to commit other crimes as an experienced ISIS member (Semko, 2015). Shannon Maureen Conley being one of the first American to be imprisoned for conspiracy to support ISIS showed the whole world that terrorist groups have quite successfully developed the ability to directly attract and even recruit foreigners to commit violence or provide other

types of support on their behalf by using contemporary propaganda tools, the Internet.

Firstly, in November 2013, federal authorities were alerted to Conley's suspicious behavior outside the Faith Bible Chapel in Arvada, Colorado, where she was taking notes on numerous days (Shannon Maureen Conley). According to court documents, the FBI visited her and her family few times with the purpose of discouraging her from joining ISIS (Shannon Maureen Conley). In March 2014, Mouelhi and others arranged the purchase of a ticket for Conley to fly to Turkey in order to cross the border to Syria on 8 April 2014 (United States of America v. Shannon Conley). Conley went to Denver International Airport on 8 April 2014, and carried a list of contacts with phone numbers as well as her first aid and nursing certification, her US Army Explorers certification and her National Rifle Association certification. Before taking the flight, she was arrested at the airport by FBI agents (United States of America v. Shannon Conley).

3.7 Conclusion

In the age of tweets, selfies, instant posts and likes, the Internet and social media have drastically transformed the way people communicate (Zeiger & Gyte, 2020). It adds that people are able to exchange their ideas and worldview, communicate and interact with each other rapidly than ever, which includes reaching out to

audiences anywhere in the world. Terrorist groups and organizations have benefited these developments to spread their propaganda, radicalize individuals, and recruit new people to their organization (Zeiger & Gyte, 2020, p. 374). Accordingly, this chapter focused on terrorist propaganda on the Internet by analyzing contemporary models of terrorist propaganda, and the main focuses of the terrorist propaganda on the Internet that comes into being as radicalization, incitement to terrorism, and recruitment. Under each sub-section, a pertinent case study was examined. The case of Roshonara Choudhry showed how online terrorist propaganda material could affect individuals to a point where they commit an act of terrorism as lone actors. On the other hand, the Christchurch attack executed by Brenton Tarrant marked a unique one specifically because in only 36 minutes he managed to shot 51 people in two mosques in Christchurch while livestreaming the attack on Facebook. Such a propaganda by deed was utilized for the first time in a terror attack. Lastly, the case of Shannon Maureen Conley illustrated how a young American girl has been influenced by a ISIS fighter she met online to the extent that she got radicalized by the materials she reached online, converted to Islam, and decided to get training in US military tactics and in firearms as well as aid/nurse program so as to move to Syria and be recruited as a nurse in an ISIS camp. What those all mean is that terrorists have developed very effective and manipulative techniques to spread their propaganda online. By doing so, they aim at radicalizing and recruiting people and if this does not happen, inciting interested individuals to terrorism is just as good as these two because it helps maintaining publicity they have already achieved. When they

have been using the conventional methods to spread terrorist propaganda, the tools terrorists have employed were quite limited just as the impact it has had. It could reach to a certain group of people who had access to television, radio, and print media in the form of comics, posters, books and so on, whereas terrorists' target audience have generally been vulnerable and marginalized groups that may not necessarily have access to all of those listed. Having access to those in the years when technological advancements were not at their best has been much of a big deal than having access to the Internet and social media in today's terms. As the Internet offers a global reach as well as its capacity to distribute a wide array of contents directly and without a filter, the uncertainty over accessibility to terrorist content has been sorted out. Considering all these elements, it has been deemed necessary to bring various case studies into the discussion where terrorists have applied different techniques to radicalize and recruit individuals, and incite to terrorism through their propaganda available online. Only by shedding a light on these real-life examples, it is achievable to propose effective means to counter dissemination of online terrorism propaganda that requires an active cooperation between governments and social media companies as the case studies concluded.

CHAPTER 4: ROLE OF THE INTERNET IN THE TRAINING, PLANNING, AND EXECUTION OF ACTS OF TERRORISM

4.1 Introduction

In this chapter, the focus will be on how the Internet has been utilized with the purpose of terrorist training, planning and execution of acts of terrorism. Each purpose of the Internet use will be examined in a separate section, and each section will have a case study demonstrating how the Internet has been actually employed with such aims. Since the area of concern, because of the Internet exploitation by terrorist organizations, has been extended to transnational and international arenas, online platforms have also been extensive use for tactical, strategic, and operational measures in terrorist activities. It is, therefore, essential to bring clarity to the methods employed.

4.2 Training

In recent years, terrorist organizations have increasingly turned to the Internet as an option of reaching terrorism-training material. Newly emerging media

platforms have started to provide guidelines in the form of online manuals, audio and video clips, information, and advice. Such platforms can operate as a virtual training camp that is also used to share specific methods, techniques, or operational knowledge for committing an act of terrorism (The use of the Internet for terrorist purposes, 2012, p. 8). Given that Al Qaeda lost much of its control over infrastructure and training camps in Afghanistan, and more recently, ISIS has lost "strongholds" in Syria and Iraq, the Internet has become a primary focus as a means of terrorist training (Siqueira & Arce, 2020, pp. 1-2). The interactive nature of online media platforms helps building a sense of community among actual and potential recruits anywhere in the world, highly encouraging the creation of networks for the exchange of instructional and tactical material. People can also discuss training-related issues, exchange personal experiences, and communicate with online trainers who can explain and clarify what is problematic (Stenersen, 2008, pp. 216-217).

The types of training materials that are online vary substantially. There are pamphlets and handbooks available covering almost any topic considered necessary for training and preparation (Stenersen, 2008). The most common topics in those can be listed as conventional weapons as well as improvised weapons and explosives, guerilla warfare and field tactics, organizational security, and physical training. A major part of the instruction material seems to be derived from English open-source literature such as US Army Field Manuals and/or *explosive cookbooks* (Stenersen, 2008, p. 217). However, there are also other

manuals circulating online which have been written by experienced jihadists, senior commanders, and trainers. Manuals are often issued in larger collections called encyclopedias, and perhaps the most well-known and comprehensive one is *The Encyclopedia of Preparation* whose editor was an active member of one of the prominent jihadist forums. It had its own permanent homepage where all manuals and documents were stored in easily accessible zip-files. It included information about weapons, homemade manufacture such as improvised devices, explosives, and bomb making, guerilla warfare tactics, regular military operations, and selected English books (Stenersen, 2008, p. 218). It proved to be the largest and greatly significant to an extent that jihadist forum members who posted new training material online often asked for their own materials to be added in the Encyclopedia.

As the advent of the technology made it easy to share relatively long and high quality videos online, this has led to a significant increase in the number of jihadist movies produced and delivered every day. Although most of the videos and movies produced display propaganda purposes, there is an increasing number of instructional videos too, which bring a new dimension to the concept of virtual training camp (Stenersen, 2008). For a while, among the designated foreign terrorist organizations, the Hezbollah videos were practically the only ones on jihadist webpages that provide detailed instructions for explosives. Those were the highest quality instruction videos available online at a time. They were specifically picked up by the Internet activists, modified to serve a Sunni-

dominated audience, and then posted online on jihadist websites. Along with the instruction videos, it has been stressed that it is no longer necessary to go through the dangers and fears of travelling abroad for terrorist training, when one can simply access the military knowledge required for planning and executing an act of terrorism (Stenersen, 2008, pp. 221-222).

Below are some screen shots of tweets posted by ISIS trainers on various topics. Figure 1 illustrates Abu Mariya al-Qahtani, who is an Iraqi Islamic militant fighting in the Syria and was formerly a commander and Shura Council member in Jabhat al-Nusra (al Haj Ali, 2015), teaching on media training and development, and how to use drones effectively to collect local information. It was tweeted by the IS Academy account, before it was shut down, with the purpose of showing their operational capabilities and mainly sharing the details of their onsite training so that anyone affiliated with ISIS can access it online. In the second one, ISIS releases pictures showing a training camp for its snipers at an undisclosed location in Bayda, Libya. This tweet also used to lead to a link where one can get to watch the full video of training for its snipers as a model for ISIS inspired attacks across the world that would require the use of snipers in a terrorist attack. Lastly, in the third figure, we see a pamphlet circulated online in order to increase operational capabilities of ISIS fighting in various fronts in the Middle East such as Iraq, Syria, and Yemen with the purpose of defeating main battle tanks of the US.

[3]

Figure 3: IS Academy for Media Training and Development

[3] The Presentation of *Twitter as a Tool to Help Assess Extremism* by David Blose, Terrorism Experts Conference by COE-DAT, October 16, 2019, Ankara.

#YEMEN
#IslamicState Releases Pictures Showing A Training Camp For Its Snipers At An Undisclosed Location In Bayda. #TerrorMonitor 3/3

[4]

Figure 4: IS Training Camp for its Snipers

[4] Ibid.

[5]

Figure 5: Destruction of Abrams Tanks in 9 Months

Besides the extensive training material Jihadist terrorist organizations have provided in Twitter and other platforms, inspired individuals can also be the source of dissemination of such materials online.

[5] Ibid.

4.2.1 Case Study: Emerson Winfield Begolly

The case of a 22-year-old American citizen Emerson Winfield Begolly demonstrates how an individual involved in the Internet and, particularly, jihadist forums with the aim of expressing his radical views and providing various training materials to be an active inspiration for like-minded individuals (The use of the Internet for terrorist purposes, 2012, p. 40).

Formally known as "Asadullah Alshishani", Begolly took an active part in an internationally known jihadist forum called *the Ansar al-Mujahideen English Forum* (AMEF), and eventually became a moderator there (The use of the Internet for terrorist purposes, 2012, p. 40). As well as his affiliation with radical views, he has encouraged other members to engaging in terrorist acts in the US. His intended targets included synagogues, military facilities, train stations, police stations, bridges, water plants and cell phone towers. Over the period of nine months, Begolly has kept posting messages calling for the need for violence. A key evidence of him encouraging others to opt for violence came in a message he posted on the forum (The use of the Internet for terrorist purposes, 2012, p. 40; Pennsylvania Man Sentenced for Terrorism Solicitation and Firearms Offense, 2013):

Peaceful protests do not work. The Kuffar (non-believers) see war as solution to their problems, so we must see war as the solution to ours. No peace. But bullets, bombs and martyrdom operations.

Although it remained unknown what the source of his particular knowledge was, he posted videos with instructions for making explosive devices, and links to an online document titled as "The Explosive Course" which was around 101 page (The use of the Internet for terrorist purposes, 2012, pp. 40-41). It contained detailed instructions on setting up a laboratory with basic chemical components for the manufacture of explosives. In the document, it was noted that an anonymity software should be used before downloading the content for their own protection. Begolly came under radar when an FBI agent downloaded the same document from one of the uploaded links (The use of the Internet for terrorist purposes, 2012, pp. 40-41). He was imprisoned for his involvement in the distribution over the Internet of information relating to bomb making, use of weapons of mass destruction, and solicitation to commit bombings of places for public use, government buildings, and public transportation systems within the US (The use of the Internet for terrorist purposes, 2012, p. 41). It has been stated that this case highlights "the need for continued vigilance against homegrown extremism, the growing impact of online training platforms, and to keep a reminder that online-inspired terrorism can occur and spread from anywhere" (Pennsylvania Man Sentenced for Terrorism Solicitation and Firearms Offense, 2013).

4.3 Planning

Planning an act of terrorism typically involves remote communication among several parties as it can be conducted easily and bear less risk of being detected by the police forces. Planning an attack may require some preparatory measures such as target selection, reconnaissance, selection of entrance and exit routes, obtaining information on local peak times, and gaining knowledge on the response times and effectiveness of emergency services (Celiksoy & Ouma, 2019, p. 257). Should it be face-to-face or in any form of physical attendance, these kinds of preparatory acts would require multiple visits to target which is costly and time consuming, and most importantly highly risky to be in the radar of security forces (Celiksoy & Ouma, 2019, p. 257). However, the Internet allows terrorists to decrease such risks and costs, and organize planning and preparation of an act of terror online. For instance, in 2014, Al Qaeda's online magazine *Inspire* in its 12th issue provided a country-by-country targets list, detailed information regarding those targets, and how to carry out an attack on them especially car bomb attacks (AQAP Releases 12th Edition of Inspire Magazine, 2014). One of the earliest and foremost examples where terrorists heavily relied on the Internet in planning is the 9/11 terror attacks which prompted the *war on terror*. Federal officials discovered countless code-word and encrypted messages which have been posted in a password-protected area on the computers of arrested terrorists (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004). To secure their anonymity, Al Qaeda terrorists used the Internet in public places and sent

messages via public e-mail. Some of the 9/11 hijackers have communicated using free web-based e-mail accounts (Hoffman, 2006, pp. 197-198).

Moreover, Hamas activists in the Middle East have used chat rooms to plan operations, and operatives have exchanged e-mails to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions came in the form of maps, photographs, directions, and technical details of how to use explosives. Those were often covered by means of steganography that involves hiding messages inside graphic files (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 10). In an empirical study conducted on the cases of 223 convicted terrorists within the UK by Gill et al. (2017), strikingly 100% of those who killed others in an event had some form of online contact with a terrorist organization. 61% of these cases shows that terrorists used the Internet for various activities including radicalization and planning an attack. 32% of those prepared for their attacks by using online sources that included "bomb-making instruction videos, poison manuals, downloaded issues of Inspire magazine, surveillance advice, an assassination guidebook, torture techniques, suicide vest production, and body disposal" (Gill, et al., 2017, pp. 107-108).

To shed light on a more recent and advanced use of the Internet in the preparation and planning of acts of terrorism, the next section will examine a case study

where two individuals have domestically engaged in an act of terrorism within the UK.

4.3.1 Case Study

This section plans to demonstrate the details of a case involving two individuals who were imprisoned for engaging in preparation of an act of terrorism in the UK, and the way the Internet has been used to plan such an attack (Holbrook, 2015). If not being caught prior to their plans, they were to carry out this attack on behalf of a designated foreign terrorist organization ISIS. In other words, the perpetrators-to-be of this planned terror attack were not lone wolves, they represented group offenders. This examination is based on the analysis of Donald Holbrook (2015) as well as the additional court documents he has provided. For security-related purposes, the names of individuals were kept as anonymous in many of those documents. Therefore, I do not have any particular intention to reveal those either. In this section, they are referred as Subject A and Subject B if needed.

The prosecution concluded that both individuals have become radicalized mainly through the material that is available online on the Internet over a 10 months' period prior to their arrest. Subject B revealed that both has consumed Islamist, and Jihadist extremist ideological content downloaded mainly from the Internet

and secured through social network sites such as Facebook. A copy of Al Qaeda's online magazine Inspire, for example, was secured via a contact on Facebook, both subjects have used their Facebook profiles to share, and access links to Islamist propaganda material that includes Al Qaeda Central and Al Qaeda in Iraq (AQI) publications posted on YouTube. Two weeks before their arrest, it has been monitored that they were in an extensive search of past terrorist incidents and their perpetrators. They also searched religious concepts of *martyrdom* and *green birds*, which are supposed to carry the souls of martyrs to the heaven, which illustrates that they have been very much exposed to online terrorist propaganda pertaining to the glorification of martyrdom because of an act of terrorism (Holbrook, 2015, p. 124).

Having motivated by those, evidence shows that the subjects were planning to make a bomb to carry out an act of terrorism. A few days prior to their arrest, the 6th issue of Inspire has been acquired by subjects, with a special focus on the section "Open Source Jihad" presenting itself as a "resource manual for those who loathe tyrants; includes bomb-making techniques, security measures, guerilla tactics, weapons training and all other jihad related activities" (Holbrook, 2015, p. 125). This process detailed in the 6th issue of Inspire seemed to address the efforts of the subjects to find the correct ingredients and extract needed products in order to make the explosive component of their devise. They have tried to make use of the infamous article of the first issue of Inspire, titled "Make a bomb in the kitchen of your Mom". The article provided a systematic guide for making a

simple pipe bomb, ignited with a modified set of fairy lights and an alarm clock. Besides these technical details, the article also offered ideological justifications for urging Muslims in Europe and America to avoid travelling to areas of conflict to assemble improvised explosive device (IED), and Jews and Christians being the main targets (as cited in Holbrook, 2015, p. 125). Subject also took the advice of downloading a file-erasing program promoted in Inspire. They sought ways to secure bomb-making process in order not to leave anything to chance, and downloaded many other sources via torrent.

Despite the availability of detailed and, to a certain extent, straightforward bomb-making guidelines, the subjects could not properly turn them into practice. Their Internet searches reveal that they were working on overcoming some of the basic problems during the process (Holbrook, 2015, p. 127). Having been arrested and convicted in court, both individuals were imprisoned for planning to carry out a terrorist act and obtaining material useful in the execution of such an act (Holbrook, 2015, p. 123). What this case shows us is that the subjects used the Internet extensively in their attempt to reach operational guidelines with the aim of making an IED, finding potential targets, and ensuring operational security. Those guidelines seem to have come from different sources including non-professionals and potential supporters who post material online, and government agencies whose publications were reachable through torrents and websites (Holbrook, 2015, p. 127; Gill, et al., 2017, pp. 109-110).

4.4 Execution

Elements of training and planning categories analyzed in this chapter may be also utilized in the use of the Internet for the execution of terrorist acts. The methods of the Internet communications that are used to reach potential victims, or to coordinate the execution of an act of terrorism is a common example of the Internet use of terrorist organizations with the purpose of carrying out an attack. The use of the Internet with such a purpose may offer logistical advantages, and decrease the likelihood of perpetrators being detected (The use of the Internet for terrorist purposes, 2012, p. 11).

4.4.1 Case Study: The Westgate Attack by al-Shabaab

This section will review a case study illustrating how al-Shabaab utilized Twitter to communicate through the Westgate attack based on thorough research on the tweets posted during the attacks and the analysis of those by David Mair (2017). The attack started on September 21, 2013 when four men entered into the Westgate shopping mall in Nairobi, Kenya. Initially, it was believed that this was an armed robbery until a Twitter account linked with Somalia-based terrorist group al-Shabaab announced taking responsibility for the attack. The Westgate attack was the first incidence of a terrorist organization using Twitter to claim responsibility for an attack (as cited in Mair, 2017, p. 25). Before this incident

took place, Twitter has often been used as a tool to monitor and check the location and movements of police and military during attacks, such as Mumbai terror attack of 2008 and ISIS during the siege of Mosul (How Terrorists are Using Social Media, 2014). The Westgate attack has lasted for four days where 67 people were killed and 175 wounded (Mair, 2017). Throughout the attack, al-Shabaab's press office has created Twitter content that justified the attack, created fictional threats, sent news on hostages, and in a way taunted the police and military.

The use of Twitter by al-Shabaab for four days has served the purpose of the various elements of the use of the Internet by terrorist organizations as discussed throughout this thesis such as publicity and propaganda, recruitment and radicalization, commanding and control, which this section will examine under the category of carrying out a terror attack. Given that the attack was ongoing for four days, it required a massive flow of communication among the perpetrators and within the organization itself in the form of sending texts, asking questions, verifying the current situation sometimes via the images and videos, coordinating for the next steps, and confirming the continuity of the operation. As well as stemming from a need to stay in communication for the continuity of the attack, using Twitter with the purpose of carrying out a terror attack also reflected an example of psychological warfare. Through that, al-Shabaab has intended to target six different audiences; "the general Kenyan population, the Kenyan government, the Western world, the media, terrorist supporters, and emergency

responders" (Mair, 2017) to show their inadequacies vis-à-vis a terrorist group which can capture the control of a shopping mall and maintain its attack for four days ending up with a considerable amount of casualties. Despite Twitter's immediate efforts to suspend pertinent accounts, al-Shabaab proved how fruitless this actually is since they kept coming up with new accounts anytime Twitter suspends one of theirs which saved them time to continue live-tweeting until the platform takes further action. Moreover, in order to assure that the attack creates publicity, they have regularly posted striking images of their attack that was acknowledged that this is an important strategy for terrorist groups during the phases of planning, coordinating, and carrying out an attack (Mair, 2017, pp. 33-34). So as to prevent aforementioned publicity spreading around and operational details of four-days-lasted terror attack becoming an example or inspiration, Twitter tried to take an action as rapid as possible to remove the images as well as tweets related to command and control of attacks.

4.5 Conclusion

The tactical, strategic, and operational advantages the Internet offers to terrorist organizations have been extensively utilized by them in various ways. The Internet allows terrorists to decrease risks and costs, and organize planning and preparation of an act of terror online through remote communication among several parties as it can be conducted easily and bear less risk of being detected by

the police forces. In that event, the case of Emerson Winfield Begolly showed how an individual could use the capacity of the Internet and online terrorist forums with the material he shares aimed at providing terrorist training in order to commit an act of terrorism. In addition to that, a case where two individuals were imprisoned for preparing an act of terrorism through the assistance of the Internet in the UK was reviewed. What was discovered is that the subjects made an extensive use of the Internet to reach necessary instructions to be able to make an IED, findinf potential targets, and ensuring operational security. Lastly, the Westgate attack carried out by al-Shabaab revealed how Twitter could be employed for a duration of an attack which has lasted for four days where the perpetrators could coordinate for the sake of continuity of the attack when they also obtained a specific form of publicity as this was the first time that a terrorist organization made Twitter an essential part of their attack.

What these case studies and the revealed methods terrorists have made use of with the purposes of training, planning, and execution of an act of terrorism showed us important is that there does not seem an effective counterterrorism response from governments or international organizations working in the realm of security. For instance, if one thinks of finding information regarding terrorist training material and how to plan an act of terrorism, it is obvious that they will not just google it or look for in other search engines and unlikely that the necessary information will pop up at top of their search results. It requires a dive into Deep Web in the beginning, and then definitely visiting Dark Web which are two different things

as clarified in definitions section of the introduction chapter in this thesis. As reaching out such a content necessitates web services requiring user credentials, private information, restricted data, and a different set of protocols and software (Gross, Jr., 2020, p. 343), an attempt like this should alarm the authorities. Under French law, it has been stated "the dissemination of instructive materials on explosives would not be considered a violation of law unless the communication contained information specifying that the material was shared in furthering a terrorist purpose" (The use of the Internet for terrorist purposes, 2012, p. 6). However, if such a piece of information is already online and circulating among groups, individuals, and sympathizers what is the point of waiting to see whether or not it will be made use of in an act of terrorism? By the time, it is decided that what is available online is indeed a violation of law, damage would be already done and maybe set an example in furtherance of terrorist attack by other groups or individuals. In his report published in 2004 and focusing on how terrorism uses the Internet in the modern age, Gabriel Weimann blamed the mass media, policymakers, and even security agencies to concentrate too much on "the exaggerated threat of cyberterrorism" and, therefore, pay less attention to the daily uses of the Internet (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, p. 11). Perhaps, this was a relevant point to raise in 2004 yet given the advancement of technology since then and how deep the Deep Web indeed is, it would be fair to ask if the threat of cyberterrorism still is exaggerated enough for governments, policymakers, international organizations, and security agencies to disregard it. As a matter of fact, terrorists do not engage in

cyberattacks as much as they carry out acts of terrorism in real life. This research has not confirmed any evidence that cyberattacks are the important component of their online presence. It stems from either their deliberate choice to hold onto their modus operandi, or their lack of sophistication to conduct such attacks in cyberspace. However, this is also not to conclude that cyberterrorism is an exaggerated threat as Weimann (2004) put into words. This chapter showed that terrorists have engaged in cyberterrorism through their Deep Web and Dark Web penetration with the purpose of disseminating and finding the material of terrorist training and planning an act.

Some of the cases show that those who engage in providing online terrorist material for training, planning, and execution were arrested after they had made their point to be effectively used by others. Until they actually take an action, there is no detecting mechanism to take a preemptive measure to prevent what may occur from happening, or even if those individuals or groups are monitored it is not an effective system. Either way, the situation requires an active cooperation between governments, policymakers, security agencies, and international organizations functioning in the realm of security. Otherwise, the more time passes without effective measures started to be taken, the more terrorists will be able to provide on the Internet in terms of content and skillset.

When it comes to Turkey's performance in its fight against terrorists' use of the Internet, then there is not much information shared regarding the country's cyberterrorism policy. Indeed, Turkey has been facing terrorist threat in the real life a lot more than it has come across in cyberspace. However, this is not to say that the country has never been subject to cyber threats by terrorist groups, or has not adopted related policies and implemented legislations. For instance, in 2018 Turkish Police arrested 30 hackers in 15 different areas who were PKK members. Police also detained 23 suspects in operations in 13 provinces, charging them with membership in a terror organization and attacking public institutions' websites, and a daily newspaper. The organization's hackers named as "Cold Attack Team" took orders from the leaders in Kandil, Iraq, and Europe regarding which websites to hack, when to hack them and what kind of messages to disseminate there (Bicak & Bogdanova, 2018, p. 98). It is also known that PKK has long launched a website called *Hezen Parastina Gel* that has been available in Kurdish, Turkish, English, German, and Arabic languages. The website included a press release section, a list of terrorist leaders, a list of central commands, information on the group's activities, a link to terrorist group's online TV channel, book and article recommendations, interviews with individual terrorists, and a contact form. Turkish administration had taken an action to shut down the website and remove content, yet they attempted to create new ones. The status of website seems like it pops up at top of Google research, but the website cannot be reached as it was blocked within Turkish Internet protocol (Celiksoy & Ouma, 2019, p. 248). In the broader sense, Turkey had already evaluated cyber threats in the way that

cyberterrorism and cyber espionage were qualified as cybercrime. The latest development in that came from the Turkish Ministry of Transport and Infrastructure as an action plan targeting the period 2020-2023.

CHAPTER 5: TERRORISM FINANCING THROUGH THE INTERNET

5.1 Introduction

The last chapter of this thesis will concentrate on the use of the Internet of terrorists in order to raise funds and financing themselves. It was once stated by Colin Powell who is a former US Secretary of State that "Money is the oxygen of terrorism". Terrorism is not cheap, and it is not only the actual execution of a terrorist attack costing considerable amount of money. Significant funds and the maintenance of a sound effective terrorist organization are of vital importance in maintaining a robust and effective terrorist organization (Ashley, 2012, p. 10). It is no surprise that terrorist groups have turned to the Internet also for fundraising purposes, just as they have done so with the purposes of propaganda and training, planning, and execution as covered in previous chapters. Firstly, the four main funding streams based on typology of Michael Freeman (The Sources of Terrorist Financing: Theory and Typology, 2011) will be reviewed to have a grasp of conventional methods of terrorism financing before the Internet became the

primary actor in the 21st century. Then, the early and premature examples of online terrorism financing will be discussed in order to see their progress up to date and innovative methods they have started employing. Subsequently, the chapter will build up assessing the recent methods of terrorism financing focusing on the use of the Internet that mainly takes the form of online donations, online credit card fraud, online exploitable charities, and virtual currencies, as it is the recent trend among terrorists and, particularly, their role in ransomware attacks. Each method will come with a pertinent case study so to have a better understanding of how those systems are employed by terrorists in real-life. The last section will concentrate on a need for international cooperation and global regulation to take necessary actions in order to prevent terrorists from raising and moving funds across the world through the help of the Internet, specifically the social media platforms, virtual currencies and the latest phenomenon of fundraising; ransomware attacks.

5.2 Conventional Methods of Terrorism Financing

The range of terrorism financing sources range from state sponsorship to petty crimes such as theft. Accordingly, different sources are divided into four categories; state sponsorship, illegal activities, legal activities, and popular support (Freeman, The Sources of Terrorist Financing: Theory and Typology, 2011, pp. 461-462).

5.2.1 State Sponsorship

States can support terrorist groups and organizations by providing training, logistical support, equipment and weapons, and/or in the form of cash (as cited in Windle, 2018). It is said "state support to terrorist groups as a source of finance has significantly decreased since the end of the Cold War as both diplomatic and financial cost of sponsoring a terrorist group became too much for states to manage" (Romaniuk, The State of the Art on the Financing of Terrorism, 2014, p. 10). Moreover, state sponsorship has proved to be gradually disadvantageous for terrorist groups too because states started to control the group's activity and agenda by using its financial support. What terrorist groups have also experienced is that state support is subject to change as governments may have different interests (Freeman, The Sources of Terrorist Financing: Theory and Typology, 2011, p. 466).

5.2.2 Popular Support

One of the financial sources terrorist groups count on is the potential support of a population or specific group of voters. From the bigger perspective, charities and donations can be counted as parts of popular support. In fact, big portion of money raised out of popular support consists of charities and donations. It is

possible to document it for many Islamic terrorist groups. For instance, there was Global Relief Foundation and al-Wafa organization, which had proven links with Al Qaeda, and they raised money for the organization through donations (as cited in Freeman, 2011). Diaspora communities also play an important role supporting terrorist organizations and raise money for their cause whereas support from diaspora is based more on ethnic or religious objectives in comparison with the religiously driven ones. It has been pointed out that popular support as a source of finance can be quite advantageous for terrorist groups as it is a powerful sign that their existence gains legitimacy. However, this very same reason sometimes affects terrorists' activities and control their behaviors, as it is fair to fear that their future actions may undermine the ongoing support.

5.2.3 Legal Activities& Legitimate Investments

It has been witnessed that terrorist groups do not only carry out criminal activities, yet they often run legal businesses for a profit to be used for financing their actual agenda. For terrorist organizations, legitimate sources can pose low risk and non-suspicious encounters and it would be difficult to trace the roots. Because running a business is legal, there is not really a reason for states to get suspicious and go after it. On the other hand, opting for investing in a legitimate business may not appeal to some groups as this choice of legitimate investments for terrorist organizations very much depends on capital and their start-up skills. Although, their original aim is to finance maintenance of terrorist activities, not become a

leading business in the market, they still need adequate business skills to remain operating in competitive markets in order to make profit out of it (Freeman, The Sources of Terrorist Financing: Theory and Typology, 2011, pp. 469-470; Windle, 2018, p. 2).

5.2.4 Illegal Activities

Illegal activities range from petty theft, kidnapping and ransom, drug trafficking to carry out sophisticated cyberattacks as a way of raising fund, which reflects efforts of financing both individual acts of terrorism and larger organizations. This type of fundraising illustrates a difference to an extent that illegal activities have the characteristic of being entirely criminal whereas three other methods to raise funds are covered by side aspects. It is to raise that in this manner some commits illegal acts to be able to commit further and extensive criminal acts that makes it a crime chain that is not solely limited to acts of terrorism.

Illegal activities offer many advantages for terrorist groups as the diversity and availability suggest that it can take place anytime, anywhere. They also undermine the legitimacy of state by showing that states are not always capable of preventing those, and sometimes finding responsible ones to prevent future actions. Likewise, it may affect the legitimacy of terrorist organization itself and alienate its supporters, as they are ready to carry out anything to finance

themselves. In terms of security, it is highly risky too. Terrorist groups need to take extra cautions to stay away from policing mechanisms (Freeman, The Sources of Terrorist Financing: Theory and Typology, 2011, pp. 468-469). Conducting operations through the Internet and cyberspace is also within the type of illegal activities, as these constitute acts of cybercrime. It is to say that they are not thoroughly analyzed unless few researchers shed light on it. However, ransomware attacks carried out in cyberspace with the purpose of raising fund will be analyzed in the last section of this chapter, once the early examples of terrorism financing through the Internet and other trends that have been increasingly employed by terrorists in the recent years are analyzed.

5.3 Early Examples of Terrorism Financing through the Internet

While terrorists' use of the Internet for financing purposes has drastically increased after 9/11 terror attacks, it in fact began way before than 2001 (Jacobson, Terrorist Financing and the Internet, 2010, p. 353). In many cases, American and European governments, and the public came to a realization of such activities only after 9/11 terror attacks, which marked a breakthrough in the history of terrorism (Jacobson, Terrorist Financing and the Internet, 2010, p. 354). The most prominent example of the early use of the Internet by terrorists was Babar Ahmad who put his computer expertise in support of the jihadist cause. In 1997, Ahmad ran the website Azzam.com and a number of associated websites with the explicit purpose of financing the Taliban active in Afghanistan and the

mujahidin operating in Chechnya (Ashley, 2012, p. 17). On the websites, Ahmad solicited funds, attempted to recruit potential fighters, and even provided with detailed instructions on how individuals can get money to these conflict zones (Jacobson, Terrorist Financing and the Internet, 2010, p. 356). He wrote, "Azzam Publications has been set up to propagate the call for Jihad among the Muslims who are sitting down, ignorant of this vital duty…" (Tierney, 2018, p. 354). Thus, the purpose of Azzam Publications is specified as to incite the believers as well as fundraising for then-fighters. To persuade individuals to donate to their cause, Ahmad used an argument on his website claiming;

> first and most important thing that Muslims can do in the West is to donate money and to raise it amongst their families, friends and others…For someone who is not able to fight at his moment in time due to a valid excuse they can start by the collection and donation of funds (as cited in Ashley, 2012, p. 17).

He was very careful with what he has been doing, using aliases and boxes of post office to hide the fact that he was the one running these extremist websites. He generally used cash if necessary, and, importantly, used encrypted communications in mailing to protect data in his personal computer (Jacobson, Terrorist Financing and the Internet, 2010, p. 358). Although, Ahmad's early use of the Internet with the purpose of raising funds was unpolished in 1997, it remained as an effective terrorism financing strategy.

Furthermore, Sami al-Hussayen, who was a Saudi graduate student at Idaho State University, acted like a master for extremist websites before 9/11. Those included

the site of al-Haramain that used to be a Saudi-based NGO later designated by the US Treasury Department due to its ties to Al Qaeda (Jacobson, Terrorist Financing and the Internet, 2010, pp. 353-354). Their focus was speeches and lectures promoting violent jihad in Israel. In 2003, al-Hussayen was found guilty for also providing support to Hamas. It was found out al-Hussayen knew and intended that his expertise of IT would be used to recruit and raise funds for violent jihad in Israel and Chechnya (Jacobson, Terrorist Financing and the Internet, 2010). The material he has provided online did illustrate what was available in cyberspace even before 9/11.

5.4 Why the Internet to Raise and Move Funds?

Increasing use of the Internet by terrorist organizations and groups should not be taken by surprise given the rapid growth in the number of the Internet users worldwide. As the data displays, currently there are 4.66 billion active Internet users around the world meaning that the global Internet penetration rate is 59.5% (Johnson J. , Global digital population as of January 2021, 2021). Whereas, in 2010 it was less than the half of today's users with a number of 2.035 billion people (Johnson J. , Number of internet users worldwide from 2005 to 2019, 2021). It is to say that terrorists' use of the Internet to raise and transfer funds is also part of a new trend in the general use of technology. Moreover, there have also been shifts in how funds can be, as transferring funds electronically prove a great facilitator. Perhaps, the most obvious reason as to why terrorist

organizations and groups have increasingly turned to the Internet is the security and anonymity it assures. It is vital for terrorist organizations to stay off radar while raising larger amounts. For instance, the US and international community had restrained Al Qaeda and affiliated groups and individuals, terrorists have tried to find other options to overcome detection. In this regard, the use of the Internet and, particularly, cryptocurrencies have allowed terrorists to stay away from the radar of intelligence services and law enforcement mechanisms. Furthermore, financing through the Internet offers a global reach where terrorists have started operating in the transnational context for some time now including raising and moving funds anywhere in the world with the aim of transferring those to the conflict zones. Similarly, the Internet allows terrorists to transfer the fund as fast as possible to whoever is in need to meet operational necessities. Having explored the early instances of terrorism financing through the Internet and reasons why terrorists bother to finance themselves in such platforms, the rest of this chapter will be dedicated to the most preferred methods of raising fund online. Online donations, online credit card fraud, exploitable charities, and virtual currencies with a special focus on ransomware attacks will be analyzed followed by the recent cases.

5.5 Online Donations

Nafir al-Aqsa, which is a group, located in Israel and Palestine has been quite active in fundraising on social media sites such as Twitter and YouTube by asking

for donations online. Although the group has not explicitly associated with a designated terrorist organization, the online content they had been sharing has been enough to reveal that they support the Islamic State affiliate in Sinai Province (Tierney, 2018, p. 4). Through many different Twitter accounts that were shut down by the platform yet reopened under different names, the group shares religious messages and, the most significantly to draw attention, asks for funding by listing necessary equipment, and "the respective cost for mujahedeen fighters" in the Sinai region. In fact, their religious messages base a justification for their demand of financial support.

On March 2016, *the Nafir al-Aqsa Campaign* to "equip the mujahidin of Beit al Maqdis (Jerusalem)" posted a call for funding under the Twitter handle @Nafeer_aqsa100. It cited a hadith, which is the sayings of Islam's Prophet Muhammad, advicing "giving money to those waging jihad is as good as doing it yourself" (Shankar, 2016). What was demanded in the picture below listed from top to the bottom is translated as "Nafir al Aqsa Campaign, to equip the Mujahdin of Beit al Maqdis, equip a Mujahid, 2500 dollars, Kalashnikov, ammunition vest, military clothing, ammunition, and military boots". In addition, the message in the very bottom is put as "The Messenger of God (May God bless him and grant him peace) said "whoever equips a warrior in the way of God has himself fought, and he who supplies the needs of the family of a warrior has himself fought". This post listed a Telegram account "Nafeeraq", and mail address Nafeeraq@tutanote.de to get in touch for the campaign. Through their messages

attached to their posts on Twitter, the group has very successfully manipulated the sympathizers without a need to use long texts targeting emotions to be persuasive.

Figure 6: The Nafir al Aqsa Campaign, March 22, 2016

As also seen below, another tweet posted a day after called for sponsors for jihad, detailing the prices of some armaments such as a sniper weapon ($6,000), a grenade thrower RPG ($3,000), and PK machine gun ($5,000) (Shankar, 2016).

Figure 7: The prices of a sniper weapon, a grenade thrower RPG, and a PK machine gun

The Nafir al Aqsa campaign also solicited funds on YouTube. On April 2015, the Twitter handle @7sanaabil that belonged to a Chechen jihadist group Jaish alMuhajireen wal-Ansar based in Aleppo, Syria solicited donations for "arming medical relief sponsorship" and "sponsorship of the families of martyrs" (Shankar, 2016; Social Media Emerges as a Valuable Terrorist Fundraising Tool). For the fundraising campaign and instructions for transferring money, the group has used WhatsApp and Telegram as these two platforms provide with encrypted messaging. Another later-suspended Twitter campaign openly acknowledged that contributions would help buying weapons. The group listed the price of 8 mortal shells as "100 Kuwaiti Dinars" or "1,300 Saudi Riyal, Qatari Riyal", and the "150 Kalashnikov bullets, 50 sniper bullets" as "50 Kuwaiti Dinars" and "650 Saudi

Riyal, Qatari Riyal" (Shankar, 2016; Social Media Emerges as a Valuable Terrorist Fundraising Tool). The currencies they used as a unit illustrated where their immediate connections to raise funds are located. The tweet included Kuwaiti and Qatari WhatsApp numbers to contact to reach about making a donation (Social Media Emerges as a Valuable Terrorist Fundraising Tool).

5.6 Online Credit Card Fraud

One of the main ways that terrorist groups are using the Internet to finance themselves is resorting to criminal activity (Jacobson, Terrorist Financing and the Internet, 2010). It is fair to raise "Younis Tsouli who is a British man better known by his online code name *Irhabi 007* (translated as *Terrorist 007*) may be one of the best known virtual terrorist" (Jacobson, Terrorist Financing and the Internet, 2010, p. 355). As it has been observed by a terrorism expert, over the space of only two years he became "the undisputed king of internet terrorism" (Jacobson, Terrorist Financing and the Internet, 2010, p. 355). He did not act alone, rather was accompanied by Waseem Mughal and Tariq al-Daour.

In the beginning of his career, Tsouli used to post terrorist-related contents on various websites. Due to his IT knowledge and ambitions in that area, he attracked the attention of Al Qaeda in Iraq (AQI) and established good relations with the organization. Once he proved himself, he was given the authority to post

relevant content for AQI. At a point while he was posting related content on free websites, he did not need have big expanses. However, given the limited bandwidth of these free websites, Tsouli had to turn to sites that offer better technical capabilities, yet are costly. At this point, he started to use the Internet with an additional purpose of raising funds to finance his online terrorist activities. One of his partners, Al Daour was responsible for organizing the stolen credit card on the websites, purchasing them through various online forums such as Cardplanet (The use of the Internet for terrorist purposes, 2012, p. 38; Jacobson, Terrorist Financing and the Internet, 2010, p. 355; Ashley, 2012, p. 17). Al Daour have also been involved in further credit card fraud, the proceeds of which were not applied to the support of the websites, yet mostly utilized for their own purposes. By the time Tsouli and his partners were arrested, al-Daour had obtained 37,000 stolen credit card numbers through 32 different websites, which they used to make more than $3.5 million in charges (Jacobson, Terrorist Financing and the Internet, 2010). Tsouli laundered money through a number of online gambling sites such as absolutepoker.com and paradisepoker.com. Any winnings would be converted to cash and transferred immediately to bank accounts. As well as raising fund to maintain online terrorist presence, Tsouli has also used these credit cards to sponsor expanses of necessary equipment for the mujahidin (Jacobson, Terrorist Financing and the Internet, 2010, p. 355). The Tsouli case has drawn the attention to how the “cellular” model of global jihad complicates the war on terrorism financing, as he was an affiliate rather than a member of AQI and has operated overseas to raise funds to sponsor both his

online presence for the maintenance of terrorist content and support for the jihadi fighters. In addition, given that he has never met his partners in person, it is even more significant to note that global jihad increasingly substitutes the Internet for face-to-face communication.

5.7 Exploiting Charitable Giving

It would be fair to raise "the charitable sector has found itself at the center of terrorism financing concerns every now and then" (Keatinge & Keen, Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool, 2019). Terrorist sympathizers abuse charitable organizations in abroad to cover their raising and moving fund, personnel, military supplies, and other resources (Bensted, 2012, p. 247; NATIONAL TERRORIST FINANCING RISK ASSESSMENT, 2018). For example, for the US, there remains a terrorism financing risk for tax-exempt charitable organizations operating within, sending funds to, or affiliated with organizations in where ISIS and its affiliates, Al Qaeda and also its affiliates, and other terrorist groups are most active, such as Afghanistan, Pakistan, Somalia, Syria, and Yemen. Such a risk highlights the importance of running accountable and transparent charities and operations (NATIONAL TERRORIST FINANCING RISK ASSESSMENT, 2018, p. 24).

In March 2016, James Alexander McLintock who was the president, CEO, and chairman of the Pakistan-based Al-Rahmah Welfare Organization (RWO) was designated by the US Treasury for providing financial, material, or technologic support for Al Qaeda, Taliban, and Lashkar-e-Taiba (Keatinge & Keen, Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool, 2019, p. 191). The US Treasury assessed that RWO had solicited funding in support of supposed work with orphans that was in fact covered to support jihadi operations. This indeed was a trick, using photos of children, Afghan identity documents, and cell phone numbers for soliciting donations for RWO supported by social media activity. Of a particular note, the US Treasury asserted that (Keatinge & Keen, Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool, 2019, p. 191; United States and Saudi Arabia Designate Terrorist Fundraising and Support Networks, 2016):

> Since May 12, McLintock has provided support to the Taliban by using RWO and his other non-governmental organizations (NGOs) to receive large amounts of money from British donors who were not aware of the NGOs' Taliban ties. According to publicly available information, between April 2011 and April 2012 RWO received the equivalent of approximately $180,000 from donors in the United Kingdom. RWO has also received financial support from charities in the Persian Gulf and the United Kingdom.

Additionally, in May 2017, Treasury also designated Pakistan-based Welfare and Development Organization (WDO) for being controlled by a leader of Jamaat ud-Dawa al Quran (JDQ), which is a militant Islamist organization operating in eastern Afghanistan. WDO supposedly collected money for charity and facilitated the transfer of funds from the Gulf countries to Afghan insurgents (NATIONAL

TERRORIST FINANCING RISK ASSESSMENT, 2018, p. 25). According to the Camstoll Group, despite the designation of RWO and McLintock as of April 2016, social media accounts linked to those were still active and calling for donations (Keatinge & Keen, Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool, 2019, p. 192).

5.8 Virtual Currencies

As the latest financial developments present, the ease with which cross-border payments by virtual currencies are facilitated, the anonymity they provide and their potential to be converted into the fiat financial system make them ideal for terrorism financing. Based on Financial Action Task Force Report (2014), virtual currencies can be defined as a "digital representation of value that can be digitally traded and functions as a medium of exchange and/or a unit of account and/or a store of value, but does not have legal tender status in any jurisdiction". Such currencies can be seen as digital objects that hold economic value and are functionally similar to fiat currencies that are issued by governments, yet they are not issued in the same way but rather are created based on private agreement among users (p. 4).

Based on the expertise of Alan Brill and Lonnnie Keene (Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014) the functioning of virtual

currencies is explained in the following sentences. There are two main characteristics of virtual currencies, they can be either centralized or decentralized. Centralized virtual currencies have a central administering authority that controls the system and issues the currency. The exchange rate for a convertible virtual currency may be floating or fixed. On the other hand, decentralized virtual currencies, meaning that they are issued without a central administering authority, are crypto-based and distributed on a peer-to-peer basis. They are better known as cryptocurrencies. Those are convertible virtual currencies meaning that they have an equivalent value in real fiat currency and can be exchanged for such fiat currency. In the advanced markets, the acceptance of cryptocurrencies as a method of payment has become widespread. For instance, Bitcoin which was the first cryptocurrency to obtain international status is now an acceptable form of payment in exchange for goods and services including Amazon, eBay, Expedia, Victoria's Secret, and Subway. Bitcoin is a fast, open-source, and peer-to-peer cryptocurrency that relies on public& private key technology and a decentralized clearing system (Brill & Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014). It was introduced by Satoshi Nakatamo in 2008 (Lee & Choi, 2021, p. 364). The storing and mobilization of finance raised by terrorists is also critical in determining their ability to carry out acts of terrorism. As they need people and transactions outside of their immediate network and those are often conducted through the formal financial sector, it is beyond their control. Therefore, the convertibility of virtual currencies and the anonymity surrounding their usage make them very attractive for terrorists

(Salami, 2018, pp. 970-971). In this respect, I will subsequently review the dismantling of two terrorist financing cyber-enabled campaigns including the use of the cryptocurrencies announced by the US Justice Department. Those campaign involve the al-Qassam Brigades (Hamas' military wing), and Al Qaeda.

Al-Qassam Brigades Campaign

In the beginning of 2019, the al-Qassam Brigades which is the military wing of Hamas operating in Palestine is posted a call on its social media page for Bitcoin donations in order to fund its campaign of terror. Then, this request was moved to its official websites, alqassam.net, alqassam.ps, and qassam.ps (Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts, 2020). This specifies that Bitcoin donations were/are untraceable and would be used for violent causes. Those websites aforementioned offered video instruction on how to make anonymous donations by using unique Bitcoin addresses generated for each individual donor. However, it turned out to be that such donations were not completely anonymous. IRS, HIS, and FBI agents working together tracked and seized all 150 cryptocurrency accounts which laundered funds (Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts, 2020). With judicial authorization, law enforcement seized the infrastructure of the al-Qassam

Brigades websites and covertly operated alqassam.net. During this covert operation, it has been discovered that the website received funds from individuals providing material support to the organization, yet they donated the funds Bitcoin wallets controlled by the US. Moreover, the US Attorney's Office for the District of Columbia unsealed criminal charges for two Turkish individuals, Mehmet Akti and Hüsamettin Karataş who both acted as related money launderers as operating an unlicensed money transmitting business (Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts, 2020).

Figure 8: The al-Qassam Brigades Online Campaign for Bitcoin Donations

Al Qaeda Campaign

The second cyber-enabled terror finance campaign involves a scheme by Al Qaeda and its affiliates mostly based in Syria. These groups carried out a Bitcoin money-laundering network using Telegram and other social media platforms with the purpose of calling for cryptocurrency donations to maintain their terrorist goals. In some cases, they acted as charities although they were explicitly calling for funds for the maintenance of terrorist attacks. Some of the terrorist groups it involved follows as; Malhama Tactical which is a private military contractor from Uzbekistan that has provided training for and fought alongside several terrorist groups in Syria, Al Sadaqah that is a Syria-based organization active on social media purporting to be a charity but has been implicated in terrorism financing, and Al Ikhwa affiliated with terrorist groups like Hay'at Tahrir al-Sham (The 2021 Crypto Crime Report, 2021, p. 97). For example, one post from a charity under the name of *Reminders From Syria* asked for donations to provide terrorists with weapons in Syria (The 2021 Crypto Crime Report, 2021, p. 97). Some undercover HIS agents got in contact with the administrator of Reminder From Syria, and the administrator stated that he hopes for the destruction of the US. Accordingly, he discussed the price for funding surface-to air missiles, and warned about the possible consequences of carrying out a jihad in the US (The 2021 Crypto Crime Report, 2021, pp. 97-98). The report of the US Department of Justice highlights that today's complaint seeks forfeiture of the 155 virtual currency assets consisting mainly of Bitcoin tied to this terrorist campaign

(Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts, 2020).

Figure 9: Al Qaeda's Request for Bitcoin Donation

Although there are abundant reports and studies discovering the instances of terrorist groups' use of the cryptocurrencies with the aim of financing their activities, there is few considerations of how cryptocurrency does actually work. As the innovative techniques applied by terrorists to their financing are increasingly becoming widespread and obtaining Bitcoin started to be an

everyday concern of ordinary individuals, it is worth looking at how that system actually works.

How Does Cryptocurrency Work?

As cryptocurrencies do not exist in the form of banknotes or coins we could hold in our hands, one must have a way of storing them known as a digital "wallet" to buy, sell, or use (Brill & Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014, p. 7). It is stated that there are many organizations on the Internet that will provide a digital wallet for virtual currencies (Brill & Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014, pp. 7-8). Once a digital wallet is obtained, what needs to be done is establishing an account with one or more exchanges. As the account user, one decides how many units of virtual currency desired and how much that will cost in a real-world currency. Subsequently, one makes the payment and gets the virtual currency that then allows sending payments to anyone else with a wallet and exchanging it back to a fiat currency. Cryptocurrencies have to be generated in two major methods. For instance, it is stressed "Bitcoins are created by solving extremely difficult math problems that are made harder over time to ensure that the overall supply of Bitcoins cannot grow too fast" (Brill & Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014, p. 12).

Because Bitcoins and other cryptocurrencies are not issued by a government or central bank, the supply must come from a Bitcoin exchanger. Those exchangers accept conventional currencies and exchange them for Bitcoins based on a fluctuating exchange rate. Once obtained, it can be stored in a digital wallet associated with the user's Bitcoin address and a bank account number, which is designated by a complex combination of letters and numbers. The only necessary piece of information is the Bitcoin address and it does not reflect any identifying detail of the user. A Bitcoin transaction is recorded in a public account book called the "blockchain". It is put "for a transaction to be confirmed, it must be packed in a block that fits very strict cryptographic rules (Brill & Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, 2014, pp. 11-13, 16; GLOBAL FRAUD REPORT: Vulnerabilities on the Rise, 2016). The very characteristics of cryptocurrencies described above as well as Bitcoin services being not highly regulated make them attractive to terrorists and money launderers, and pose a great threat for law enforcement mechanisms and regulators.

5.9 Ransomware

Along a continuum with cryptocurrencies, a new form of cyber-extortion called ransomware is perplexing the world with a speculation of its connection to the acts of terrorism including the use of cryptocurrencies, namely Bitcoin (Lee & Choi, 2021). However, there is no prior empirical study that demonstrates the

causal relationship between ransomware and Bitcoin, which is to say that whatever is going to be said on this will be based on anecdotal evidence. That is mainly why using ransomware with the purpose of raising funds within the terrorism context needs to be given place especially if such a study focuses on the use of cryptocurrencies. The fact that it's understudied although there are examples of using ransomware for terrorism financing purposes from 2015, which will be reviewed in this section, makes it obvious that assessment of innovation in terrorism financing is in dire need of discovery.

Employing such a method, cybercriminals usually demand their ransom in Bitcoin (Lee & Choi, 2021) and, therefore, it has become a part of this new phenomenon other than its regular use in terrorist campaigns as covered in the previous section. Since online payment methods were not really available until the mid-2000s, cybercriminals have received random employing different payment methods such as victims transferred money via SMS text messages or by mailing prepaid cards, and later using "Moneypak, Paysafecard, and Ukash cards" (as cited in Lee & Choi, 2021, p. 364). However, the invention of Bitcoin in 2008 can be fairly seen as a game changer due to anonymity and technological ease it offers that also allow perpetrators to hide behind their ransomware attacks. There are two main forms of ransomware currently in circulation; locker-ransomware and crypto-ransomware. Locker-ransomware will lock the computer by denying access to device, while the latter prevents access into the files or data (Lee & Choi, 2021, p. 364).

In August 2015, a computer intruder, calling himself the “Albanian Hacker” left a message for the administrator of a website for an Illinois Internet retailer: “Pay two Bitcoins, or about $500 at the time, and the intruder would remove all bugs on your shop!” It is stated that such demands are typical among hackers, yet this case was more than a clandestine digital mugging. The perpetrator had ties with the Islamic State Hacking Division, which is the cyber unit of the organization, and he put together a “kill list” for the ISIS with the identities of 1,351 US government and military personnel from the 100,000 names, credit card records and social security numbers he had extracted from the host server. He has used a Dell Latitude laptop, a second MSI laptop, and computer application known as *DUBrute* that allows users to seize control of another computer remotely. It is known that the hacker operated in a gray area where criminal and terror interests blend messily to test malicious computer code, raise funds, and identify Western targets. The case of the Albanian Hacker, whose actual name is Ardit Ferizi, is also significant because his work generated one of the first kill lists detailed by the ISIS designed to generate fear and publicity by showing targets. Ferizi was sent from Malaysia and has been held by US until June 2015. He admitted providing material support to terrorists and to computer hacking (Johnson T. , 2016).

5.10 Conclusion

Terrorism financing through the Internet has become worrisome situation recent years. Thanks to advent of technology, the usefulness of social media, and, specifically, the emergence of virtual currencies has led many terrorist groups to turn to the Internet to raise and transfer funds anywhere in the world. In this regard, this very chapter has reviewed the most prominent methods of terrorism financing through the Internet. Online donations, online credit card fraud, and exploitable online charities have been examined with pertinent real-life examples. The phenomenon of virtual currencies has been aimed to dedicate a special focus, as this method is the most recent and increasing trend among terrorists to opt for with the purpose of raising and safely transferring funds worldwide.

Having gone through these aspects, it is essential to draw attention to the need for international cooperation for online terrorism financing in general targeting also social media companies, and global standardization of virtual currencies in particular. As the aim of this thesis is to show how terrorists use the Internet with the purpose of propaganda, training, planning and execution, and financing, yet when one looks at the bigger picture the primary concern is to chart out effective means to combat all these elements focused. Whichever aspects stated as a gap in terrorism financing literature have been aimed to address through various case studies. All the case studies and methods covered in this chapter also have

importance from the countering perspective. In this respect, considering the security vulnerabilities of social media platforms such as Facebook, Twitter, Telegram, and YouTube whose lack of preemptive actions to prevent online terrorist presence revealed by various case studies up to this point, as a policy recommendation it is highlighted that social media companies should comply with domestic regulations as well as international sanctions by closing down related accounts. They need to take necessary measures by strengthening their technical capabilities to cope with such a threat. However, more importantly, social media companies should have a ground of information sharing and active partnership to be in maximum cooperation with intelligence agencies, law enforcement mechanisms, and local administrations of whose jurisdiction it falls into (Keatinge & Keen, Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool, 2019, p. 197). With respect to the virtual currencies and particularly cryptocurrencies, countries started to take regulatory actions to an extent of sometimes banning the use of them completely, yet those separate actions do not add much to a global response which requires a mutual effort of foreign regulators, regional blocs if a coordinated international approach cannot be achieved in the first place, and linked international organizations such as INTERPOL and Financial Action Task Force (FATF). As long as there is lack of regulation in this and countries unsurprisingly have different interests in their financial systems, terrorism financing through virtual currencies will remain as a real threat (Salami, 2018, pp. 983-985).

CHAPTER 6: CONCLUSION

The great virtues of the Internet which are "easy access, fast flow of information, little or, sometimes, no regulation, anonymity of communication, a multimedia environment, and inexpensive development and maintenance of a web presence" (Weimann, www.terror.net: How Modern Terrorism Uses the Internet, 2004, pp. 1-3) have turned to the advantage of terrorists. Considering the fact that the development of increasingly sophisticated technologies has paved the way for terrorists to engage in, this research has focused on the question of how terrorists use the Internet. Accordingly, among the methods the Internet is utilized for terrorist purposes, this thesis has taken three main categories as its base: propaganda, training, planning and execution given as points along a trajectory, and financing. Although majority of the cases reviewed in this thesis comes from designated terrorist organizations, there have been some space and analysis dedicated to the lone-wolves and inspired individuals. Case studies have been considered the backbone of this research with a purpose to demonstrate the real life examples of terrorists' use of the Internet in order to support the descriptive analysis existing within terrorism and the Internet.

It is to say that terrorists' use of the Internet for spreading propaganda; training, planning, and execution; and financing has come as an adjunct to their other activities that have been physically carried out in real life as opposed to cyberspace that is in fact a digital nonspace (Gilmour, 2014, p. 145). It does not reduce the importance of the role the Internet has been playing in terrorism, yet in fact, terrorists have executed attacks in real life considerably more than they have done in cyberspace. Despite the fact that engaging in cyberterrorism would gain time, result in more casualties at once, and degrade states' upper hand in managing cyberwarfare; there is no sort of evidence confirming that terrorists are increasingly preferring cyberspace to real life to carry out acts of terrorism. Why this has been the case is not really known or researched so far, yet it may be a deliberate choice to maintain their modus operandi, or they may be lacking the sophistication to conduct such operations. In either case, states hold the dominance over cyberwarfare through the attacks they have carried out in cyberspace[6]. This research does not address cyberwarfare in general as it would go beyond the scope of my expertise, and require knowledge on Computer and Information Technology as well as criminology. However, there has been little overlap with cybercrime such as the use of cryptocurrencies and ransomware with the purpose of terrorism financing. In consideration with these, my research

[6] It has been identified that China, Russia, Iran, and North Korea increasingly using cyber operations to pose a threat in different ways; to steal information, to influence citizens, or to target critical infrastructure. China's actions have reflected its primary strategic goals: economic hegemony and security. Russia considers its cyber espionage capability as a key element within its broader information warfare objectives. Similarly, Iran has used cyber espionage to ensure regional power. North Korea views spying through cyberspace as a way of enabling regime survival and to disturb regional forces, especially the US and South Korea (Diotte, 2020, pp. 32-38).

stands out as a preliminary survey in the relation between cybersecurity and terrorism studies. As long as terrorists' use of the Internet for the purposes studied in this thesis brings the concept of cyberspace into the discussion, the connection between two disciplines have aimed to be established. Since the subject matter is of considerable importance due to the exploitable nature of the Internet and its tendency to evolve into a problem of cybersecurity, it is essential to map out the developments and the latest trends.

Throughout this research assessing terrorists' use of the Internet, Turkey has not been part of the discussion much. It is mainly because Turkey has been waging war against different terrorist groups on the ground both within the country and through cross-border operations such as PKK/YPG, FETO, and ISIS. It implies that Turkey has been facing terrorist threat in the real life a lot more than it has come across in cyberspace. However, this is not to say that the country has never been subject to cyber threats by terrorist groups, or has not adopted related policies and implemented legislations. For instance, in 2018 Turkish Police arrested 30 hackers that were PKK members. Police also arrested 23 suspects in operations in 13 provinces, charging them with membership in a terror organization and official Turkish websites, and a daily newspaper. The organization's hacker team named as "Cold Attack Team" took orders from the leaders in Kandil, Iraq, and Europe regarding which websites to disrupt and what kind of messages to disseminate there (Bicak & Bogdanova, 2018, p. 98). It is also known that PKK has long launched a website called *Hezen Parastina Gel*

that has been available in Kurdish, Turkish, English, German, and Arabic languages. The website included a press release section, a list of terrorist leaders, a list of central commands, information on the group's activities, a link to terrorist group's online TV channel, book and article recommendations, interviews with individual terrorists, and a contact form. Turkish administration had taken an action to shut down the website and remove content, yet they attempted to create new ones. The current status of website seems like it pops up at top of Google research, but the website cannot be reached as it was blocked within Turkish Internet protocol (Celiksoy & Ouma, 2019, p. 248). In the broader sense, Turkey had already evaluated cyber threats in the way that cyberterrorism and cyber espionage were qualified as cybercrime. It is also known that in accordance with the NATO decision of 2011, the Turkish Armed Forces established an institution in 2012 called "the General Staff Warfare and Cyber Defence Command" (Tuohy & Pernik, 2014). With its awareness of those threats, Turkey adopted an Action Plan in 2013 to develop its response capacity against cyberattacks. This Action Plan emerged as significant as it was the first time that Turkey has taken an action to stop these kinds of attacks (Tuohy & Pernik, 2014). However, since then there is little information shared regarding Turkey's cyberterrorism policy. It points out to a limitation that there are no further details on how Turkey has been performing with respect to those policies mainly due to security-related reasons. Although the specifics of the Action Plan adopted in 2013 are not available to make an analysis, it is striking that the Turkish Ministry of Transport and Infrastructure adopted a recent action plan targeting the period 2020-2023. Thus, it is fair to address that

Turkish administration has been taking decided steps to keep its cybersecurity policies up-to-date based on the latest threats from both terrorist groups and states.

6.1 Limitations

Throughout this work, one of the limitations I have come across with several times is that there is no available research on the statistics revealing the percentage of attacks showing terror attacks where the Internet has been primarily used. I also had to rely on data from 2008 and 2010 regarding terrorists' use of the Internet with the purpose of training and planning, whereas I have aimed at illustrating the most recent trends throughout my research. There is no available research confirming the current validity of the information processed in 2008 and 2010. Moreover, as the role of the Internet is focus of this thesis, I would like to have more analysis included with respect to the use of Telegram because it is and will continue to be a significant use for terrorists due to its encrypted characteristic. However, it still is under scrutiny of intelligence and security agencies, the social platform itself, and governments. Therefore, there is not as much data and research available as it is for Twitter and Facebook. Correspondingly, I would like to integrate the social media platform Instagram, as it is currently one of the leading ones with a high circulation of visuals and videos. Nevertheless, other than few news articles there is not much data displaying terrorists' use of Instagram either. In consideration of these, a future

research addressing the role of the Internet in terrorism should focus on the emerging social media platforms to be able to provide the latest trends. As a further research recommendation, one needs to monitor the up-to-date situation with regard to the cryptocurrencies, because states' stance towards them displays different patterns. In the near future, it is also likely that cryptocurrencies can be subject to a degree of regulation, thus it is in best interest of researchers in this field to keep an eye on in order to observe how terrorism financing through cryptocurrencies would potentially be affected by that.

6.2 Findings

The question of how the Internet has been utilized by terrorists and for what purposes is not asked and researched for the first time here as a part of this thesis, as one would not be surprised to find out. In the literature, there is an abundance of studies focusing on the role of the Internet in terrorism propaganda, online training and planning, and terrorism financing. However, what is lacking is that there is no comprehensive study showing the progress of these means throughout the years, or changing trends through real life examples from different terrorist movements stemming from the development of increasingly advanced technologies. Especially after 9/11 terror attacks, more scholars and researchers have started to address the convergence of the Internet and terrorism, yet those studies do not necessarily provide readers with the up-to-date information at a time they are published. The timeliness of the material provided tend not to go in

parallel with the latest developments on terrorists' end. One could fairly say that with the Internet, it is inevitable as technical developments and innovations go faster than the process of reaching necessary data without limitations and conducting a proper research on it to put forward a publication. It is reasonably accepted as a limitation of terrorism studies. What is intended to stress here is that, for instance as covered in chapter 5, the case of Ardit Ferizi who is also known as the Albanian Hacker shows that ransomware has been used in order to raise funds through bitcoin and generate one of the first kill lists for ISIS in 2015. However, this case has not been studied until 2021 within the context of terrorism financing on the Internet. Furthermore, one of the gaps in the literature is that there is no such study showing the percentage of terror attacks that have utilized the Internet. Similarly, there is also no study addressing how different terrorist organizations use the Internet, and if there are different patterns in terms of their priority to use the Internet for propaganda, training, planning, and execution, and financing purposes. Although this has been the case and I could not find any solid information on which terrorist organizations more active on the Internet, the majority of cases I have benefited came from Al Qaeda and ISIS. Many sources referred to the training and planning material of Hezbollah as the highest quality videos available at a time (early 2000s), yet no recent research has confirmed the validity of this claim. Similarly, Hamas has come under the radar with its successful recruitment techniques through online propaganda. Less documented, there appear some studies describing the modus operandi of acts of terrorism where the Internet has been utilized, but they do not specify how the process

actually works. If a case includes the use of cryptocurrencies, there must be a basic explanation on their functioning and how they are converted to fiat currency. If Deep and/or Dark Web penetration is the primary focus of a case using the Internet, we must know how one could go online and find the information he/she is looking for, or handle the barriers to reach terrorist chat forums. After all, this sort of evidence would lead policy makers, intelligence and security agencies, and governments to the most effective responses in order to combat it.

The chapter on terrorism propaganda online discovered online terrorist propaganda targeting potential or actual supporters focuses on radicalization, recruitment, and incitement to terrorism. Three case studies, each being an example for these focuses, illustrated different implications within the discussion of how terrorists use the Internet for propaganda. The case of Roshonara Choudry is important as it showed that a 20-years-old British girl who had access to higher education in one of the most prestigious universities within the UK could get radicalized on herself by terrorist material online which has been circulating for a long time without a successful attempt to remove. The online material, lectures and speeches, spread by the radical cleric Anwar al-Awlaki was so influential on Choudry that she made a plan targeting her local MP as a punishment because he voted in support of war in Iraq in 2003. Awlaki had started uploading these videos into his YouTube channel around early 2000s and Choudry took such an action in 2010, which made her the first British woman convicted of an Islamic attack. A

lot of groups, sympathizers and ordinary individuals with no such a background like Choudry could get to reach those materials and get radicalized to an extent to make plans aiming at revenge, punishment, and spite. Therefore, what matters more than studying on Awlaki's online propaganda material in the early 2000s is to restudy it in the following years in order to see what kind of impact it still creates on individuals, if there is any.

Another case of Shannon Maureen Conley displayed a direct online communication between a sympathizer and ISIS member. Until she got arrested in the airport before taking a flight to Turkey with the purpose of crossing border to Syria to join ISIS, she has watched the videos of, again, Awlaki, got a basic orientation through disks on how to live in accordance with the organization's principles once she joins in, and even got a training in US military tactics, firearms, and nursing to make use of these in ISIS camp. Conley did not attract the attention of FBI until she displayed suspicious behaviors outside of a chapel while observing and taking notes. If she has been more careful in that, maybe she would not have attracted any attention at all, and would make it to ISIS camp in Syria as she initially planned. The point is up until that, how did any one of these not come under radar of FBI and other authorities? The two have communicated for a long time on a chatting forum, exchanged extremist ideas and beliefs, arranged a training process for Conley to actually apply those in ISIS camp she was supposed to reach, and planned a transfer from the US to Turkey first, and then to Syria by car. What that shows us is that a member of designated foreign

terrorist organized has used the Internet for propaganda purposes and he was so close to succeed at recruiting the potential supporter, whereas FBI and the US government became aware of this multi-staged recruitment plan in its last step. Therefore, it proved important to bring such a case study into the discussion of recruitment through online terrorist propaganda to show very late response of the authorities despite of methods employed by terrorists being not to sophisticated or complicated.

Last and maybe the most interesting case reviewed in the propaganda chapter is the Christchurch Attack carried out by Brenton Tarrant in 2019 as an example of inciting to terrorism. In Christchurch attack, he livestreamed the whole attack on Facebook and this was the first time that an actual terrorist attack has been filmed in its duration. Facebook has been subject to a circulation of terrorist material in the form of pictures, videos, and written posts. However, a far-right extremist took it to a different level by livestreaming during the attack and marked it as a propaganda by deed in a most recent way. The first report among users came several hours after so it could not prevent the video from being shared many times and made use of in different formats by the users. Facebook had to put two-days of effort to remove all relevant content as monitoring team did not take an immediate step while it was being filmed or right after. A social media platform that has been utilized for terrorist purposes before was supposed to have effective means for combatting such a situation. The fact that Facebook did lack necessary response capacity in this case made Brenton Tarrant achieve his goal of inciting to

terrorism and raised anti-Muslim sentiment online as he stated. Under the consideration of these various case studies, the chapter on terrorist propaganda through the Internet aimed to pay attention how it has been utilized with the purposes of radicalization, recruitment, and incitement to terrorism, and reveal what need to be furthered to combat it.

In chapter 4, training, planning and execution have been studied together due to their sometimes-overlapping nature. For an act of terrorism to be carried out, they may be perceived as the necessary points along a continuum. On the media platforms performing as virtual training camps, actual and potential supporters share guidelines. Virtual training camps stand out as important mainly because bigger terrorist organizations that used to prefer onsite training. Therefore, providing online material or leading to the links on social media platforms has become an important trend for terrorist groups that do not have immediate access to guidance and instructions for their ground operations. To see some of the examples, a few tweets were posted by ISIS trainers covering media training and development how to use drones effectively to collect local information, use of snipers at an undisclosed location, and destruction of Abrams tanks. These tweets remained on Twitter for a long time and retweeted many times. For the similar situations, Twitter comes up with the excuse that whenever such content is removed and the account is shut down, more related accounts are created and it becomes a loop. If the situation after tweets posted get so unmanageable for Twitter, maybe they should have better content-checking and confirming

mechanisms before it goes posted on the platform. As the dissemination of tactical and strategic information so freely on a social platform with around 206 million of users as of 2021 (Leading countries based on number of Twitter users as of July 2021, 2021) is too risky not to take the most effective responses, it is essential to highlight the remaining dangers in terrorists' use of the Internet.

It was also found out that the Internet allows terrorists to decrease costs of time and finance, and risk of being radar in the security forces in the phase of planning and preparation of an act of terror. Accordingly, a case study where two individuals have involved in a planned domestic terrorist attack within the UK was reviewed. The case showed that the subjects of the planned attack were considering making a bomb to perform a terrorist attack, and they reached majority of necessary information through Al Qaeda's online magazine, Inspire. For this time, it has been Facebook that helped terrorists to be in communication, share material with the purpose of plan, and prepare an act of terrorism. One could say that due to the privacy-related reasons, Facebook cannot intervene in one-on-one private messaging yet it is so open to abuse for terrorist purposes along with various potential exploitations of the platform. Either way, it alludes to the fact that this case is just one example of which Facebook fell short of preventing exchange of terrorist content through the platform.

Lastly, the chapter discovered that the Internet could be utilized to plan and prepare to carry out an attack, as the use of the Internet offers logistical advantages. The Westgate Attack by al-Shabaab presented a unique case since it was the first time that a terrorist organization has utilized Twitter during an ongoing attack lasted for four days. Along with gaining publicity and potentially inciting sympathizers to terrorism through live-tweeting for four days, al-Shabaab mainly used Twitter to coordinate the continuity of the attack by sending texts, asking questions, verifying the current situation sometimes via the images and videos, coordinating for the next steps, and confirming the continuity of the operation. As it has been seen in tweets posted by ISIS trainers, Twitter had the same problem running; whenever such content was removed and the accounts were shut down, more related accounts were created. The fact that we come across with inadequacy of Twitter to find an effective solution for the removal of terrorist content permanently and preemptive measures to prevent it from occurring more than once, and it is only few cases thoroughly analyzed here, illustrates that Twitter needs to invest in its capacity building measures. In order to counter this, building a more efficiently functioning team for monitoring terrorist activity on social media platforms, not specific to Twitter, is necessary.

The last chapter of this thesis helps us to see that probably the most innovative and more sophisticated methods employed on the Internet by terrorists are seen for financing purposes. In the chapter, the most used methods of online fundraising have been analyzed such as online donations, online credit card fraud,

exploiting charitable giving. A special focus has been dedicated to the virtual currencies and the use of ransomware through them with the purpose of terrorism financing, as this has been one of the most significant findings of this thesis due to its up-to-dateness. Chapter 5 also brings cyberterrorism into the discussion more than previous chapters do, since it includes the use of Deep and Dark Web a lot more. It has been intended to attract the attention to the use of virtual currencies and ransomware mainly because such innovations in terrorism financing through the Internet will keep posing a threat due to their highly unregulated and untraceable nature for a longer time. This very recent method of terrorism financing surely requires an active cooperation of states, foreign regulators, and associated international organizations such as INTERPOL and FATF.

Overall, based on the findings throughout this thesis three main recommendations to combat terrorists' use of the Internet come into being; monitoring and shutting down the terrorist content available online, creating fake websites to attract the attention of actual and potential supporters, and developing regulatory technology solutions to shut down funding especially raised through the cryptocurrencies. First of all, in order to prevent terrorist propaganda to reach its aims of radicalization, recruitment, and inciting to terrorism, social media companies such as Twitter, Facebook, WhatsApp, Telegram, and Kik need to strengthen their monitoring teams and emergency protocols to activate if necessary. By doing so, they can take preemptive actions, or minimize the loss by responding quickly when terrorism-related content is posted online. However, that would require a

great effort to scan users' profiles to see if they display any terrorist tendency or sympathy, group and/or organization pages, event announcements, and private messaging by the platforms that provide space to hold one-on-one or multiple users-based conversation. Account holders may argue that could result in the violation of privacy, and restriction of freedom of speech and expression. Secondly, security and intelligence agencies can create fake websites to attract the attention of actual and potential supporters. In this way, they get to identify individuals involved, learn about their background and connections to the wider movements if there are any, their plans to carry out acts of terrorism, and the online content that is subject to exchange between supporters. In other words, in order to catch terrorism one needs to think like and act like terrorists would do. A possible shortcoming of such an action could be that terrorists or potential supporters probably do not immediately involve in websites and chat forums that seem like running similar content. In order to secure themselves and the wider movements they have been linked to, they might ask for security protocols and identity verification. It may take too much effort and time for agents to provide information that would seem as valid and genuine. This may be problematic especially if they conduct time-sensitive operations to reveal the identity of perpetrators or reach necessary information to prevent a planned attack from happening. Lastly, in order to shut down funding there must be a global standardization of regulatory technology solutions especially for virtual currencies. Among terrorism financing methods utilizing the Internet, the use of virtual currencies emerges as the latest trend and require a more comprehensive

response because of their cross-border and highly unregulated nature. Countries started to take regulatory actions to an extent of sometimes banning the use of them completely, yet those separate actions do not add much to a global response which requires a mutual effort of foreign regulators, regional blocs (Salami, 2018, pp. 983-985) if a coordinated international approach cannot be achieved in the first place, and linked international organizations such as INTERPOL and Financial Action Task Force (FATF). After all, what the former Secretary-General of the United Nations, Ban Ki-moon once raised compiles what has been aimed to explore throughout this thesis, "The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner." (The use of the Internet for terrorist purposes, 2012)

REFERENCES

(n.d.). Retrieved from Eye on Hezbollah: https://hezbollah.org/

Gartzke , E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41-73.

United States and Saudi Arabia Designate Terrorist Fundraising and Support Networks. (2016, March 31). Retrieved from U.S. DEPARTMENT OF THE TREASURY: https://www.treasury.gov/press-center/press-releases/Pages/jl0400.aspx

Abrahms, M. (2006). Why Terrorism Does Not Work. *International Security, 31*(2), 42–78.

al Haj Ali, A. (2015, March 09). *Abu Maria: The Nusra leader behind the split with IS in Syria?* Retrieved from Middle East Eye: https://www.middleeasteye.net/features/abu-maria-nusra-leader-behind-split-syria

Anika, E. I. (2019). *New technology for old crimes? the role of cryptocurrencies in circumventing the global anti-money laundering regime and facilitating transnational crime.* University of British Columbia. Retrieved from https://open.library.ubc.ca/collections/ubctheses/24/items/1.0379183

AQAP Releases 12th Edition of Inspire Magazine. (2014, March 18). Retrieved from MSA SECURITY: https://www.msasecurity.net/security-and-counterterrorism-blog/bid/100406/aqap-releases-12th-edition-of-inspire-magazine

Ashley, S. P. (2012). The Future of Terrorist Financing: Fighting Terrorist Financing in the Digital Age. *Penn State Journal of International Affairs, 2*(1), 9-26.

Aydinli, E. (Ed.). (2010). *Emerging Transnational (In)Security Governance.* Oxon: Routledge.

Benjamin, D., & Simon, S. (2002). *The Age of Sacred Terror.* New York: Random House.

Benson, D. C. (2014). Why the Internet Is Not Increasing Terrorism. *Security Studies, 23*(2), 293-328.

Bensted, G. (2012). Hi terrorist financing and the Internet: dot com danger. *Information & Communications Technology Law, 21*(3), 237-256.

Bicak, M. B., & Bogdanova, D. (2018). Fighting Cyber Terrorism: comparison of Turkey and Russia. *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism* (pp. 98-101). Ankara: ULAKBIM UASL.

Biswas, R. (2018). *Emerging Markets Megatrends.* Palgrave Macmillan.

Blaker, L. (2015). The Islamic State's Use of Online Social Media. *Military Cyber Affairs, 1*(1), 1-9.

Blaker, L. (2015). The Islamic State's Use of Online Social Media. *The Journala of the Military Cyber Professionals Association, 1*(1), 1-9.

Bouhana, N., Malthaner, S., Schuurman, B., Lindekilde, L., Thornton, A., & Gill, P. (2018). LONE-ACTOR TERRORISM: Radicalisation, attack planning and execution. In A. Silke (Ed.), *Routledge Handbook of Terrorism and Counterterrorism.* Routledge.

Brill, A., & Keene, L. (2014). Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review, 6*(1), 7-30.

Brill, A., & Keene, L. (2014). Cryptocurrencies: The Next Generation of Terrorist Financing? *Defence Against Terrorism Review, 6*(1), 7-30.

Bryan, D., Kelly, L., & Templer, S. (2011). The failed paradigm of ‘terrorism’. *Behavioral Sciences of Terrorism and Political Aggression, 3*(2), 80-96.

Burke, J. (2011, December 16). *Al-Shabab's tweets won't boost its cause.* Retrieved from The Guardian: https://www.theguardian.com/commentisfree/2011/dec/16/al-shabab-tweets-terrorism-twitter

Carrapico, H., Irrera, D., & Tupman, B. (2014). Transnational organised crime and terrorism: different peas, same pod? *Global Crime, 15*(3-4), 213-218.

Carrapico, H., Irrera, D., & Tupman, B. (2014). Transnational organised crime and terrorism: different peas, same pod? *Global Crime, 15*(3-4), 213-218.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism, 13*(3), 285-300.

Celiksoy, E., & Ouma, S. (2019). TERRORIST USE OF THE INTERNET. *Bilisim Hukuku Dergisi, 2*, 243-267.

Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Tweeting Propaganda, Radicalization and Recruitment: Islamic State Supporters Multi-Sided Twitter Networks. *Proceedings of the 16th Annual International Conference on Digital Government Research* (pp. 239-249). New York: Association for Computing Machinery.

Chatfield, T. A., Reddick, C. G., & Brajawidagda, U. (2015). Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks. *Proceedings of the 16th Annual International Conference on Digital Government Research: Digital Government and Wicked Problems: Climate Change, Urbanization, and Inequality* (pp. 239-249). New York: University of Wollongong.

Christchurch mosque attack: Brenton Tarrant sentenced to life without parole. (2020, August 27). Retrieved from BBC NEWS: https://www.bbc.com/news/world-asia-53919624

Christensson, P. (2015, September 17). *Internet Definition.* Retrieved April 15, 2021, from TechTerms: https://techterms.com/definition/internet

Clayton, A. N. (2018). *ARE U.S. BASED 'JIHADI' INSPIRED TERRORISTS TRANSITIONING AWAY FROM PH Y FROM PHYSICAL TRAINING CAMPS T SICAL TRAINING CAMPS TO ONLINE TRAINING O ONLINE TRAINING.* San Bernardino: California State University.

Clayton, A. N. (2018). *ARE U.S. BASED 'JIHADI' INSPIRED TERRORISTS TRANSITIONING AWAY FROM PHYSICAL TRAINING CAMPS TO ONLINE TRAINING CAMPS?* Electronic Theses, Projects, and Dissertations, California State University, San Bernardino, National Security Studies.

Cohen-Almagor, R. (2017). Jihad online: how do terrorists use the Internet. In F. C. Freire, X. R. Araujo, V. A. Martinez Fernandez, & X. L. Garcia (Eds.), *Media and Metamedia Management* (pp. 55-66). Dordrecht: Springer.

Collier, K. (2021, July 27). *FBI tracking more than 100 active ransomware groups.* Retrieved from NBC NEWS: https://www.nbcnews.com/tech/security/fbi-tracking-100-active-ransomware-groups-rcna1524

Colorado Woman Sentenced for Conspiracy to Provide Material Support to a Designated Foreign Terrorist Organization. (2015, January 23). Retrieved from The United States Department of Justice: https://www.justice.gov/opa/pr/colorado-woman-sentenced-conspiracy-provide-material-support-designated-foreign-terrorist

Conway, M. (2006). Terrorism and the Internet: New Media—New Threat. *Parliamentary Affairs, 59*(2), 283-298.

Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism, 40*(1), 77-98.

Cottee, S. (2015, March 2). *Why It's so Hard to Stop ISIS Propaganda.* Retrieved from THE ATLANTIC: https://www.theatlantic.com/international/archive/2015/03/why-its-so-hard-to-stop-isis-propaganda/386216/

Crenshaw, M. (2017). The Strategic Logic of Terrorism. In O. b. Ladin (Ed.), *Conflict After the Cold War: Arguments on Causes of War and Peace* (pp. 448-462). New York: Routledge.

Croissant, A., & Barlow, D. (2007). Following the money trail: Terrorist financing and government responses in Southeast Asia. *Studies in Conflict & Terrorism, 30*(2), 131-156.

Cronin, A. K. (2009). *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns.* Princeton; Oxford: Princeton University Press.

Cronin, A. K. (2015). ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadist Threat. *Foreign Affairs, 94*(2), 87-98.

de Mesquita, E. B., & Dickson, E. S. (2007). The Propaganda of the Deed: Terrorism, Counterterrorism, and Mobilization. *American Journal of Political Science, 51*(2), 364-381.

Deibert, R. (2018). Trajectories for Future Cybersecurity Research. In A. Gheciu, & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security* (pp. 531-547). Oxford: Oxford University Press.

Diotte, P. (2020). The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online. *Canadian Military Journal, 20*(4), 32-42.

Dodd, V. (2010, November 03). *Roshonara Choudhry: Police interview extracts.* Retrieved from The Guardian: https://www.theguardian.com/uk/2010/nov/03/roshonara-choudhry-police-interview

Droogan, J., & Peattie, S. (2018). Reading jihad: Mapping the shifting themes of Inspire magazine. *Terrorism and Political Violence, 30*(4), 684-717.

Evans, R. (2019, March 15). *Shitposting, Inspirational Terrorism, and the Christchurch Mosque Massacre.* Retrieved from Bellingcat: https://www.bellingcat.com/news/rest-of-world/2019/03/15/shitposting-inspirational-terrorism-and-the-christchurch-mosque-massacre/

(2014). *FATF REPORT: Virtual Currencies- Key Definitions and Potential AML/ CFT Risks.* Financial Action Task Force. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Fisher, A. (2015). How Jihadist Networks Maintain a Persistent Online Presence. *Perspectives on Terrorism, 9*(3), 3-20.

Fisher, A. (2015). Swarmcast How jihadist Networks Maintain a Persistent Online Presence. *Terrorism Research Initiative, 9*(3), 3-20.

Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. *Studies in Conflict & Terrorism, 34*(6), 461-475.

Freeman, M., & Ruehsen, M. (2013). Terrorism Financing Methods: An Overview. *PERSPECTIVES ON TERRORISM, 7*(4), 5-26.

Ganor, B. (2002). Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research, 3*(4), 287-304.

Ganor, B. (2008). Terrorism as a Strategy of Psychological Warfare. *Journal of Aggression, Maltreatment & Trauma, 9*(1-2), 33-43.

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences.* Cambridge: MIT Press.

Gerring, J. (2004). What Is a Case Study and What Is It Good for? *The American Political Science Review, 98*(2), 341-354.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom , M., & Horgan, J. (2017). Terrorist Use of the Internet by the Numbers; Quantifying Behaviors, Patterns, and Processes. *Crimonology & Public Policy, 16*(1), 99-117.

Gilmour, S. (2014). Policing Crime and Terrorism in Cyberspace: An Overview. *The European Review of Organised Crime, 1*(1), 143-159.

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns: Largest Ever Seizure of Terrorist Organizations' Cryptocurrency Accounts. (2020, August 13). Retrieved from THE UNITED STATES DEPARTMENT of JUSTICE: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

(2016). *GLOBAL FRAUD REPORT: Vulnerabilities on the Rise.* Kroll.

Gross, Jr., W. F. (2020). Monitoring and Tracking ISIS on the Dark Web. In J. R. Vacca (Ed.), *ONLINE TERRORIST PROPAGANDA, RECRUITMENT, and RADICALIZATION* (pp. 341-351). Boca Raton: CRC Press.

Hern, A. (2017, November 13). *'YouTube Islamist' Anwar al-Awlaki videos removed in extremism clampdown.* Retrieved from The Guardian: https://www.theguardian.com/technology/2017/nov/13/youtube-islamist-anwar-al-awlaki-videos-removed-google-extremism-clampdown

Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.

Holbrook, D. (2015). A critical analysis of the role of the Internet in the preparation and planning of acts of terrorism. *Dynamics of Aysmmetric Conflict, 8*(2), 121-133.

How Terrorists are Using Social Media. (2014, November 4). Retrieved July 20, 2021, from The Telegraph: https://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html

Incitement to Terrorism through the Media: UNODC organizes workshop on anti-terror law for Journalists, Security Agencies. (2021). Retrieved August 03, 2021, from The United Nations Office on Drugs and Crime: https://www.unodc.org/nigeria/en/incitement-to-terrorism-through-the-media_-unodc-organizes-workshop-on-anti-terror-law-for-journalists--security-agencies.html

Injac, O., & Dojcinovski, M. (2015). Contemporary Terrorism and Propaganda-Trends, Models and Dimensions. *International Scientific Journal, 15*, 79-90.

IT 102 2020 Paper. (2020). Retrieved from Course Hero: https://www.coursehero.com/file/53058015/Internetdocx/

Jacobson, M. (2010). Terrorist Financing and the Internet. *Studies in Conflict & Terrorism, 33*(4), 353-363.

Jacobson, M. (2010). Terrorist Financing and the Internet. *Studies in Conflict & Terrorism, 33*(4), 353-363.

Johnson, J. (2021, April 07). *Global digital population as of January 2021.* Retrieved from statista: https://www.statista.com/statistics/617136/digital-population-worldwide/

Johnson, J. (2021, January 27). *Number of internet users worldwide from 2005 to 2019.* Retrieved from statista: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Johnson, T. (2016, July 20). *Computer hack helped feed an Islamic State death list.* Retrieved from McClatchy DC Bureau: https://www.mcclatchydc.com/news/nation-world/national/article90782637.html

Juergensmeyer, M. (2000). *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley, Los Angeles, and London: University of California Press.

Kadir, N. K., Judhariksawan, & Maskun. (2019). Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crime. *Fiat Justisia, 13*(4), 333-344.

Keatinge, T., & Danner, K. (2018). Assessing Innovation in Terrorist Financing. *Studies in Conflict & Terrorism*, 1-18.

Keatinge, T., & Keen, F. (2019). Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool. *Studies in Conflict & Terrorism, 42*(1-2), 178-205.

Keatinge, T., & Keen, F. (2019). Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool. *Studies in Conflict & Terrorism, 42*(1-2), 178-205.

Krueger, A. B., & Maleckova, J. (2003). Education, Poverty and Terrorism: Is There a Causal Connection? *Journal of Economic Perspectives, 17*(4), 119-144.

Ladin, O. b. (2017). Speech to the American People. In R. K. Betts (Ed.), *Conflict After the Cold War: Arguments on Causes of War and Peace.* New York: Routlegde.

Leading countries based on number of Twitter users as of July 2021. (2021, July). Retrieved from statista: https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/

Lee, H., & Choi, K.-S. (2021). Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoritical Framework. *Victims & Offenders: An International Journal of Evidence-based Research, Policy, and Practice, 16*(3), 363-384.

Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). *Countering the New Terrorism.* Santa Monica: RAND.

Lieberman, A. V. (2017). Terorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law and Policy, 9*(1), 95-124.

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *The American Political Science Review, 65*(3), 682-693.

Lindsay, J. R. (2014). The Impact of China on Cybersecurity: Fiction and Friction. *International Security, 39*(3), 7-47.

Macklin, G. (2019). The Christchurch Attacks: Livestream Terror in the Viral Video Age. *CTC SENTINEL*, 18-29.

Maggioni, M. (2015). *The Islamic State: Not That Surprising, If You Know Where to Look.* Milan: Italian Institute for International Political Studies (ISPI).

Mair, D. (2017). #Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack. *Studies in Conflict & Terrorism, 40*(1), 24-43.

Martinez , M., Cabrera, A., & Weisfeldt, S. (2015, January 24). *Colorado woman gets 4 years for wanting to join ISIS.* Retrieved from CNN: https://edition.cnn.com/2015/01/23/us/colorado-woman-isis-sentencing/index.html

(2018). *NATIONAL TERRORIST FINANCING RISK ASSESSMENT.* Washington D.C.: U.S. Department of Treasury.

Ogun, M. N. (2012). Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes. *Journal of Applied Security Research, 7*(2), 203-217.

Okolie-Osemene, J., & Okoh, R. I. (2015). The Nature Terrorism Reports on Social Networks. *Journal of Culture, Politics, and Innovation, 3*(6).

Pape, R. A. (2006). *DYING TO WIN: THE STRATEGIC LOGIC OF SUICIDE TERRORISM* . New York: Random House.

Patterson, D. (2021, July 22). *The world's top ransomware gangs have created a cybercrime "cartel".* Retrieved from CBS NEWS:

https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/

Pearson, E. (2015). The Case of Roshonara Choudhry: Implications for Theory on Online Radicalization, ISIS Women, and the Gendered Jihad. *Policy & Internet, 8*(1), pp. 5-33.

Pennsylvania Man Sentenced for Terrorism Solicitation and Firearms Offense. (2013, July 16). Retrieved from THE FBI: Federal Bureau of Investigation : https://archives.fbi.gov/archives/pittsburgh/press-releases/2013/pennsylvania-man-sentenced-for-terrorism-solicitation-and-firearms-offense

Pokalova, E. (2020). Online Terrorist Propaganda: Strategic Messaging Employed by Al Qaeda and ISIS. In J. R. Vacca (Ed.), *ONLINE TERRORIST PROPAGANDA, RECRUITMENT and RADICALIZATION* (pp. 267-290). New York: CRC Press.

Raphaeli, N. (2003). FINANCING OF TERRORISM: SOURCES, METHODS, AND CHANNELS. *Terrorism and Political Violence, 15*(4), 59-82.

Rapoport, D. R. (2004). The Four Waves of Terrorism. In A. K. Cronin, & J. M. Ludes (Eds.), *Attacking Terrorism: Elements of a Grand Strategy* (pp. 46-73). Washington DC: Georgetown University Press.

Reitman, J. (2015, March 25). *The Children of ISIS.* Retrieved May 15, 2020, from Rolling Stone: https://www.rollingstone.com/culture/culture-features/the-children-of-isis-42701/

Risk assessment of lone actors. (2017). *RAN H&SC* (pp. 1-10). Mechelen: EUROPA.

Romaniuk, P. (2014). The State of the Art on the Financing of Terrorism. *The RUSI Journal, 159*(2), 6-17.

Romaniuk, P. (2014). The State of the Art on the Financing of Terrorism. *The RUSI Journal, 159*(2), 6-17.

Rudner, M. (2017). “Electronic Jihad”: The Internet as Al Qaeda’s Catalyst for Global Terror. *Studies in Conflict & Terrorism, 40*(1), 10-23.

Sageman, M. (2014). The Stagnation in Terrorism Research. *Terrorism and Political Violence, 26*(4), 565–580.

Sageman, M. (2016). *Misunderstanding Terrorism*. Philadelphia: PA: University of Pennsylvania Press.

Salami, I. (2018). Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This? *Studies in Conflict & Terrorism, 41*(12), 968-989.

Scheuer, M. (2006). *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America*. Washington, D.C.: Potomac Books, Inc.

Semko, R. (2015, January 29). *Do you know what your teenager is up to?* Retrieved from Ray Semko: https://raysemko.com/2015/01/29/do-you-know-what-your-teenager-is-up-to/

Shankar, A. (2016, April 20). *Social Media Emerges as a Valuable Terrorist Fundraising Tool.* Retrieved from Investigative Project on Terrorism: https://www.investigativeproject.org/5314/social-media-emerges-as-a-valuable-terrorist#

Shannon Conley Sentencing, 14-cr-163 (THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLORADO January 23, 2015).

Shannon Maureen Conley. (n.d.). Retrieved from Counter Extremism Project: https://www.counterextremism.com/extremists/shannon-maureen-conley

Siqueira , K., & Arce, D. (2020). Terrorist training: Onsite or via the Internet? *European Journal of Political Economy, 63*, 1-11.

Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *The International Spectator, 53*(2), 111-123.

Social Media Emerges as a Valuable Terrorist Fundraising Tool. (n.d.). Retrieved from BREITBART: https://www.breitbart.com/middle-east/2016/04/20/social-media-emerges-valuable-terrorist-fundraising-tool/

Stenersen, A. (2008). The Internet: A Virtual Training Camp? *Terrorism and Political Violence, 20*(2), 215-233.

Stern, J. (2003). *Jessica. Terror in the Name of God: Why Religious Militants Kill.* New York: NY: Harper Collins Publishers.

Sullivan, R. (2014). Live-tweeting terror: a rhetorical analysis of @HSMPress_ Twitter updates during the 2013 Nairobi hostage crisis. *Critical Studies on Terrorism, 7*(3), 422-433.

Tamer, C. (2017, September 25). *The Differences Between the Guerrilla Warfare and Terrorism.* Retrieved from ANKASAM: https://www.ankasam.org/the-differences-between-the-guerrilla-warfare-and-terrorism/?lang=en

Tarrow, S. (2010). The Strategy of Paired Comparison: Toward a Theory of Practice. *Comparative Political Studies, 43*(2), 230-259.

Terrorism Expert Conference . (2019). *Violent Changes: How Terrorism and Counter-Terrorism is Transforming* . Ankara: COE-DAT.

(2021). *The 2021 Crypto Crime Report.* Chainalysis. Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

(2012). *The use of the Internet for terrorist purposes.* New York: United Nations Office on Drugs and Crime.

Tierney, M. (2018). #TerroristFinancing: An Examination of Terrorism Financing via the Internet. *International Journal of Cyber Warfare and Terrorism, 8*(1), 1-11.

Tugwell, M. (1986). Terrorism and Propaganda: Problem and Response. *Journal of Conflict Studies, 6*(2), 5-15.

Tuohy, E., & Pernik, P. (2014, January 13). *Military Cyber Defense Structures of NATO Members: An Overview.* Retrieved from RKK ICDS: https://icds.ee/en/military-cyber-defense-structures-of-nato-members-an-overview/

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023). (2020, December 29). Retrieved from T.C. ULASTIRMA VE ALTYAPI BAKANLIGI: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/%283%29%20TUR%20NCSS%20%282020-2023%29.pdf

(2000). *United Nations transnational organized crime assessment form (stage 2).* Vienna: United Nations, office of drug control and crime prevention, center for international crime prevention.

United States of America v. Shannon Conley. (n.d.). Retrieved from International Crimes Database: http://www.internationalcrimesdatabase.org/Case/3284

Veilleux-Lepage, Y., Daymon, C., & Amarasingam, A. (2020). *The Christchurch Attack Report: Key Takeaways on Tarrant's Radicalization and Attack Planning.* The Hague: International Centre for Counter-Terrorism.

Vraneš, J. (2016). *TERRORISM IN THE DIGITAL AGE: THE USE OF INTERNET AND SOCIAL MEDIA.* University of Belgrade. Retrieved from http://media1.naukaidrustvo.org/2016/09/5-vranes.pdf

Walt, S. M. (2010, March 30). *Is the cyber threat overblown?* Retrieved May 28, 2021, from Foreign Policy: https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/

Weimann, G. (2004). *www.terror.net: How Modern Terrorism Uses the Internet.* Washington, DC: United States Institute of Peace.

Weimann, G. (2006). *Terror on the Internet: The New Arena, the New Challenges.* Washington D.C.: United States Institute of Peace Press.

Weimann, G. (2010). Terror on Facebook, Twitter, and Youtube. *The Brown Journal of World Affairs, 16*(2), 45-54.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195-206.

Weimann, G., & Mozes, T. (2010). The E-Marketing Strategy of Hamas. *Studies in Conflict & Terrorism, 33*(3), 211-225.

Whittaker, J., & Macdonald, S. (2020). Online Radicalization: Contested Terms and Conceptual Clarity. In J. R. Vacca (Ed.), *Online Terrorist Propaganda: Strategic Messaging Employed by Al Qaeda and ISIS* (pp. 33-45). New York: CRC Press.

Windle, J. (2018). Fundraising, Organised Crime and Financing Terrorism. In *The Routledge Handbook of Terrorism and Counter-Terrorism* (pp. 1-15). Abingdon: Routledge.

Wright, L. (2007). *The Looming Tower: Al-Qaeda and the Road to 9/11*. New York: NY: Random House.

Zavadski, K. (2015, January 24). *Colorado Teen Who Tried to Join ISIS Gets 4-Year Sentence.* Retrieved from Intelligencer: https://nymag.com/intelligencer/2015/01/4-year-sentence-for-teen-who-tried-to-join-isis.html

Zeiger, S., & Gyte, J. (2020). Prevention of Radicalization on Social Media and the Internet. In A. P. Schmid (Ed.), *Handbook of Terrorism Prevention and Preparedness* (pp. 374-411). ICCT Press Publication.