The Impact of the Internet on the Radicalization and Recruitment of Terrorists

1. Introduction

1.1 Topic Selection and Focus

The researcher is an International Relations course student, from a Libyan background. After the fall of Colonel Ghadafi regime, Libya went through political instabilities and suffered from a wave of terrorist attacks orchestrated by ISIS and AL Qaeda. This has triggered the researcher's intention to conduct this study aiming to understand the role of internet in radicalizations of terrorists.

In this study, the researcher will investigate the impact of internet in radicalization of terrorists using secondary data available on databases such as the Rand Database of Worldwide Terrorism and the Global Terrorism Database as well as media reports, articles and journals.

Radicalization, which occurs in phases, is a gradual and complex process, in which individuals become motivated to carry out acts of violence against innocent groups for their own cause (Doosje et al., 2016). First, the individual starts being sensitive to a radical ideology, which is what Dienel et al. (2010) refer to as everyone having a 'terrorist' in them. Secondly, the individual becomes a member of the radical group. Lastly, the individual becomes willing to act as a member of the group and is ready to take responsibility for the group's actions, such as planning, preparing and executing an attack.

According to Klausen, Campion, Needle, Nguyen and Libretti (2015), examples of behavioural indicators that an individual is progressing in the phases of radicalization include detachment from their usual friends; they start spending more time with extremist peers.

From interviews of approximately 500 families of terrorists, it is saddening that young western women are being recruited to extremist groups at an alarming rate (Speckhard, Shajkovci, & Yayla, 2018). Some are seduced in person, while others are approached through the internet.

The world has become a global village; internet connectivity, social media and other advancements in technology have changed daily activities. Just as society and corporates have embraced the internet to facilitate their activities, so have terrorist groups. The internet gives terrorists a platform for communication, collaboration and radicalization of individuals (von Behr, Reding, Edwards & Gribbon, n.d.). Even with this knowledge, it is difficult to address the role of the internet in this process of radicalization. Despite the available policies, actions against cybercrime and research on the topic, there is still very little information on recruits' experiences and their connection with the internet during the radicalization process. Perhaps, this is the reason why several young people are getting recruited, without the knowledge of the society and relevant authorities that have access to the platforms.

1.2   Objectives

Terrorism and the ways people become radicalized are broad topics. As such, gaining in depth details of these topics are beyond the aims of this research, however this research is specifically concerned with the role of internet in the radicalization of terrorists.

To have better understandings of the process of radicalization, the researcher set the following objectives based on themes derived from theories related to stages of how an individual becomes radicalized on line.

Themes	Objectives
Everyone having a 'terrorist' in them	Assessing the scale of using the internet as platform for communication and disclosing / absorbing extreme views
Becoming a member of the radical group	Examining behavioural indicators including detachment from friends in favour of spending

	more time with extremist peers (online and offline).
Becoming ready to take responsibility for the group's actions	Examining the cases where ex-terrorists acted upon online extremists' contents

1.3   Research Questions

1. How does potential terrorists (ISIS and AL Qaeda) use internet to communicate with others?
2. How does such communication play a role in radicalizing individuals?
3. What online strategies do ISIS and AL Qaeda use to recruit people?
4. Could the internet be the only mean of recruiting individuals, get them radicalized and trigger them to act?
5. Why radicalization has become so easy for terrorists?

1.4   Scope and Limitations of the research

Having a quick search of the available literature, it seems evident that most of the available literature focuses on understanding how radicalization occurs. However, understanding why radicalization has become so easy for terrorists is becoming very essential due to the suspected role the internet plays in the radicalization process.

Consequently, the author of this study realized the importance of investigating the impact and the role of the internet in radicalizing terrorists. Since there is a limitation in gaining access to

information from those who are convicted of terrorism, the author will rely on existing literature and secondary data (published interviews) related to the research topic.

The results of this study will shed some lights on the online radicalization processes, which would assist the authorities and anti-terror agencies in understanding how radicalization occurs. As a result, they would put some measures in place to prevent terrorism before it occurs.

1.5   Chapters outline

Chapter 1: is the dissertation introduction, providing a general background and specifying the research aims and objectives.

Chapter 2: lays the theoretical foundation of the research, discussing major studies related to the research topic.

Chapter 3: the research methodology is discussed in this chapter, describing aspects such as purpose, philosophy, data collection, ethical issues, etc.

Chapter 4: results presentations and analysis of the research findings compared to the pre-set objectives.

Chapter 5: discussing conclusions, findings implications, limitations, contributions to current literature and future research suggestions.

Literature Review

2.1　Terrorism in the Past Years

Although one person may solely conduct a terrorist attack, the attacks are often conducted in groups, since it is easier to prepare and coordinate an attack as a group, and the probability of backing out at the last minute is low (Bruneau, 2016). The two terrorist groups that have been active in the past decade are ISIS and Al Qaeda. According to the Global Terrorism Database (GTD), there have been a total of 694 terrorist attacks in the US alone between 1995 and 2017. These attacks claimed a total of 3786 American lives (Miller & Jensen, 2018). The most significant attack on US soil was on September 11, 2001 (9/11), and it claimed nearly 3000 lives. The attacks decreased between 2001 and 2011, but started increasing again over the past decade. Most of these attacks have been credited to Al Qaeda and ISIS.

Broadly, terrorists are extremists who use extreme violence to instil fear in the masses. They base their attacks on political, social, racial, or religious ideologies. The FBI's priority, since September 11, 2001 (9/11), has been to protect the US against terrorism ("Terrorism," n.d.). Most acts of domestic terrorism have political agendas, such as the Las Vegas shooting in 2014, which was conducted by a couple who wanted to start a revolt against the government (Lovett, 2014). The shooting claimed 58 lives, including that of the shooter, and over 500 injuries. In recent years, most terrorist attacks have been launched to coerce the target governments to give in to certain demands and, also, instil fear into the masses. ISIS and Al-Qaeda are terrorist groups that use the Islamic religion to brainwash their recruits into joining them (Dickey, 2017). Furthermore, they use radical beliefs and ideologies to validate their actions.

The internet and social media, in general, have contributed significantly to the radicalization of terrorists over the past decade. Several messaging platforms have given terrorists the opportunity to radicalize and recruit new members, through the use of extremist ideologies (Weimann, 2014). The primary target has been younger people, since they are comfortable with messaging through social media platforms. Besides the internet, social media has enabled terrorists to carry out their

attacks, because of the quick facilitation that the platform provides. They gain easy access to their targets as the information is available for anyone to access.

The fear that terrorist attacks instil in people may have further adverse effects than the immediate trauma. For instance, it may lead to increased polarization on religious, ethnic, social, political, or racial bases (Bhatia, 2009). Both ISIS and Al-Qaeda claim to be fighting a religious war. There are innocent Muslims who now face stigma in society, especially, through the media, due to the belief that they (Muslims) are all terrorists (Millo, 2018). Similarly, there is a difference in the way the authorities address terrorist allegations, if the suspect is not Muslim. For instance, in 2014, there was overwhelming evidence against a fire bomber, who was allegedly planning an attack in Sydney and Newcastle, Australia, yet he was not charged with any terrorism-related offenses (Abdel-Fattah, 2015). There is increased conflict among different people in society, due to the animosity and fear caused by terrorist attacks. After a series of surveys, several case studies on US Muslims seeking to establish their opinions and experiences in the country come up with the conclusion that most Muslims feel alienated and discriminated based on their religion. Most of them hold negative opinions of suicide bombing and ISIS, in general (McCauley & Moskalenko, 2014). Therefore, it is vital to study terrorism, the radicalization process and potential methods of achieving de-radicalization, since it poses a significant threat to the security of citizens and society as a whole.

The Radicalization Process and the Role of the Internet

Several case studies trying to understand the psychology of terrorists have indicated that terrorists are not psychopaths. Dienel, Sharan, Rapp and Ahituv (2010) argue that there is a terrorist in everyone. Radicalization, which occurs in phases, is a gradual and complex process, in which individuals become motivated to carry out acts of violence against innocent groups for their own cause (Doosje et al., 2016). First, the individual starts being sensitive to a radical ideology, which is what Dienel et al. (2010) refer to as everyone having a 'terrorist' in them. Secondly, the individual becomes a member of the radical group. Lastly, the individual becomes

willing to act as a member of the group and is ready to take responsibility for the group's actions, such as planning, preparing and executing an attack.

Although many people would like to understand why radicalization has become so easy for terrorists, one can only understand how the radicalization occurs. Following the Al-Qaeda/Daesh inspired attacks in Ottawa in 2014, the Canadian Security Intelligence Service, alongside interested parties, such as the general public, experts and journalists, embarked on a case study to examine the radicalization process and the mobilization to terrorist activities (Canadian Security Intelligence Service, 2018). Emphasizing Dienel et al.'s point as noted earlier, the Canadian Security Intelligence Service (2018) claims that many people may support radical ideas, but they may never undertake extremist activities due to their inhumane nature. Additionally, the United States government has been at the forefront of funding research projects aimed at finding answers to the most asked questions about terrorism (Bast, 2018). For instance, the National Institute of Justice, based in Washington DC, provides community leaders with the resources they need to focus on research and evaluation of terrorism ("Research on Domestic Radicalization and Terrorism," 2018). The most important question is radicalization to terrorism.

The questions to answer in understanding the process are: common trends among the domestic cases of radicalization to terrorism; the models used; why people choose to believe in radical ideologies and act on them and; how communities respond to the process. As stated earlier, the process begins with an individual's sensitivity to radical ideologies. One of the papers prepared with the support of the National Institute of Justice affirms that where individuals exhibit their radical beliefs, the outcome of extremist acts of violence is inevitable (Smith, 2018). According to Klausen, Campion, Needle, Nguyen and Libretti (2015), examples of behavioural indicators that an individual is progressing in the phases of radicalization include detachment from their usual friends; they start spending more time with extremist peers.

Recent discoveries claim that recruits are mainly young men, although women and little girls are also being recruited. All extremist groups look for aggressiveness and ambition in recruits, which they find in young men. According to Zehorai (2018), the Islamic State (ISIS) and Al-Qaeda are among the top ten most powerful, ruthless and well-funded terrorist groups today. Terrorist

groups require significant funding to facilitate their attacks. Most of them get their funding from states and private donors, along with other illegal activities, such as ransom from kidnappings (Gordon, 2016). From interviews of approximately 500 families of terrorists, it is saddening that young western women are being recruited to extremist groups at an alarming rate (Speckhard, Shajkovci, & Yayla, 2018). Some are seduced in person, while others are approached through the internet.

Some of the young women opt to join the extremists because of the oppression they suffer, or they identify with people who have gone through oppression; consequently, they view themselves as saviours, rescuing such people from oppression. As they join the groups, these young women have visions of being heroines whose legacies live on, even if they die. Similarly, as young men join, they are promised wives and girls to enslave in this world, as sexual relationships with virgins await them in the after-life, when they are finished fighting the "Holy War," which is the main reason for the existence of suicide bombers (Thayer & Hudson, 2010). However, some of these young recruits point out that, at times, it is not always about sex; it is about the respect and dignity that manhood commands. They seek refuge from extremists because they give them hope in the face of joblessness and poverty (Bhatia & Ghanem, 2017). Most victims of terrorist activities are from developing countries (Bandyopadhyay & Younas, 2017). It hurts their economic growth.

The world has become a global village; internet connectivity, social media and other advancements in technology have changed daily activities. Just as society and corporates have embraced the internet to facilitate their activities, so have terrorist groups. The internet gives terrorists a platform for communication, collaboration and radicalization of individuals (von Behr, Reding, Edwards & Gribbon, n.d.). Even with this knowledge, it is difficult to address the role of the internet in this process of radicalization. Social media platforms have policies that control online content. Last year, Google and Facebook were in trouble for alleged leaked user information (Salinas, 2018). Such faults pose threats to national security. Despite the available policies, actions against cybercrime and research on the topic, there is still very little information on recruits' experiences and their connection with the internet during the radicalization process.

Perhaps, this is the reason why several young people are getting recruited, without the knowledge of the society and relevant authorities that have access to the platforms.

In most extreme cases, recruits had earlier ambitions of building their reputations in other careers. For example, in 2014, a suspected Jihadist identified as Abdel-Majed Abdel Bary had ambitions of being a famous rapper and lyricist (Dearden, 2014). He posted a photo of himself holding a detached head on his Twitter handle. Before this incident, Bary had a budding music career where he appeared in music videos and had his own singles played on BBC Radio (Dearden, 2014). He resurfaced in Syria, but later disappeared, and no one seems to know his whereabouts, including his family. "Lyricist Jinn," his stage name, may not have been a terrorist before this incident (Dearden, 2014). Violent extremists may have taken such an opportunity to recruit him, because of his interest in radical ideologies.

Terrorists believe that they have been wronged in some way, so they have no choice but to engage in extreme violence. Furthermore, they are all fighting "a defensive war", in which they adopt the behaviour and accessories of soldiers in a war (Hoffman, 2006). Through this war, those who would be insignificant if they had chosen to be normal activists would become the heroes of the society. They believe themselves to be God's chosen people, to shine the light of liberty on their enemies (Mishra, 2016). Through this mindset, the Islamic State tries to get fighters for the "holy war." They use several social media accounts to operate on YouTube, Facebook and Twitter (Torok, 2015). Moreover, they use videos to lure recruits and then praise them for their bravery in standing up for what they believe is right.

Most times, whenever there is a terrorist attack, extremists are quick to take credit for such attacks. They record videos acknowledging their responsibility, even if the attacks involved the deaths of their own; however, at times, they do not (Snyder, 2016). Sometimes, if they aim to instil fear, the extremists' stage ornately choreographed death ceremonies where they behead, burn, or even drown their enemies. They play on this fear to divide the world and try to dominate it (Cordesman, 2016). During the era of Osama Bin Laden, the radicals conducted interviews and ensured that their attacks claimed a significant number of lives for them to be recognized globally. Bin Laden even did one last interview before going into hiding ("Osama Bin Laden's

Last Interview," 2017). The radicals relied on the media to fuel their reputation. Nowadays, through the internet and social media, terrorists publicize their operations on their own. The terrorist groups have evolved from having a hierarchical structure, to a horizontal structure of communication (Kepel & Jardin, 2017). In this way, recruits can easily follow the rules.

How Isis and Al-Qaeda use the Internet to Radicalise and Recruit their Respective Fighters

Wilson (2017) admits that there is a direct relationship between the increasing number of views and shares of ISIS videos on Facebook, Twitter, and YouTube and the number of recruits. However, Taylor, Holbrook and Joinson (2017) claim that al-Qaeda relies on more traditional web-platforms like websites and forums. Additionally, the noted difference lies in the approach used to pass the message. Gomes and Mikhael (2018) explain that ISIS occasionally posts videos and images of symbolic crucifixion displays, public rape, and beheadings and mass executions to terrorise all opponents, including Muslims into submission. The approach, they believe, would help purify the community, and the fear created spreads quickly. Bertram (2016) contributes to the discussion by explaining that al-Qaeda favours a gentler approach, resisting from displaying brutality in the videos and messages posted on social media platforms. The group's focus is on fighting western influence, and it displays only online content that tries to persuade Muslims to join their war against the West.

Tinnes (2018) observed that both factions perceive the internet as an essential tool in their terrorist activities. He illustrates that even before the 2001 New York attack, al-Qaeda recognised the importance of exploiting the "new media" through globally broadcasting its ideology and attracting potential recruits. It relied on the internet for operations too, planning the 9/11 attack by communicating online and researching their targets through the internet. For example, in an unsigned letter sent to Taliban leader Mullah Omar, Osama bin Laden explained that the constructive use of social media covers 90% in preparing for war. Similarly, it advances this perspective through the harb electroniyya ("electronic warfare") and ghazwa ma'lumatiyya ("information operations") (Tinnes, 2018).

Open source journals and applications have also become a common form of communications strategy for both ISIS and al-Qaeda. Droogan and Peattie (2018) outline that cyber magazines such as *Inspire* have been available on the internet since 2010 and published in English to attract a sizeable Western audience. Numerous editions of *Inspire* provide detailed and lengthy guidelines on ways of planning and perfecting bomb attacks, and groups and individuals attempted attacks after downloading this material. According to Vergani and Bliuc (2018), ISIS applies the same the strategy relying on an online magazine called *Dabiq,* the name for a Syrian town on the Turkey border and the apocalyptic region where Muslims fight infidels. The quality of articles produced is remarkable, and they contain enticing messages legitimising ISIS's action against the West.

Both terrorist factions have also displayed their attempts to appeal to the younger generation. Choi, Lee and Cadigan (2018) conducted a study and noted that even before 2006, al-Qaeda had created websites meant to attract a media-saturated, video-game-addicted and computer-savvy audience. Al-Rawi (2018) supports this view by claiming that one jihadist internet platform had the video game "Quest for Bush". It was designed to allow players to fight against Americans and proceed to advanced stages such as the "Americans Hell" and "Jihad Growing Up". It also included attacking soldiers who resembled President in six levels, followed by the final mission in the desert where Jihadist songs play on the background (Al-Rawi, 2018).

Monaci (2017) supports this idea by demonstrating that ISIS has been using video game technology to recruit members, but advanced this approach to the new level. The author demonstrates that the group modified the 2012 Grand Theft Auto game to enable users to navigate as ISIS members engaged in combat. Other changes included its militants killing police officers and attacking military convoys with snipers and explosives.

3

Methodology

3.1 Introduction

The objective and purpose of the research on the role of the internet in the radicalisation of terrorists will be clarified in the methodology chapter. According to Langkos (2014), the methodology helps the author to outline the research philosophy, approach, strategy, data collection and analysis, sampling method, limitations and ethical considerations. The subject on terrorism radicalisation through the internet is best understood using the following elements of methodology. The research objectives are provided below:

3.2 Research Objectives

The following objectives are based on questions on how the communication age influences terrorism as raised in popular editorials such as the New York Times by Harrington (2018).

- To understand how AL Qaeda and ISIS extremists use the internet for communication.

- To analyse the role of the internet in the radicalisation of individuals.

- To explore the online strategies employed by Al Qaeda and ISIS to radicalise people.

- To distinguish how different terror groups (Al Qaeda and ISIS) use the internet for radicalisation purposes.

3.3 Research Philosophy

The research explanation of the radicalisation and internet communication elements of terrorism is justified by three key philosophies namely ontology, epistemology and doxology. According to Guarino, Oberle and Staab (2009), ontology is vital in showing the different properties of a phenomenon and the relation between them; in this case how radicalisation relates with internet usage to further the course of Al Qaeda and ISIS terrorist groups. Epistemology is a philosophical assumption that deals with what is known about a particular subject (De Araújo, Guimarães, and Tennis, 2017). For instance, there is definitive proof that Al Qaeda and ISIS are

a security threat and they recruit through radicalisation. However, the unknown elements of the spectre of terrorism are explained through doxology which elaborates what is believed to be true (University of Hong Kong, 2019). In the context of this study, government organisations and researchers believe that the internet is one of the channels used for the radicalisation of people, mostly youths, which qualifies the doxological philosophical assumption. The research philosophy employed by this study is in part due to the emergence of ontology as a means of knowledge engineering as opposed to just the traditional branch of metaphysics dealing with the nature of being (Poli, Healy, and Kameas, 2010). Essentially, epistemology, ontology and doxology encapsulate the impact of the internet in terrorism-based radicalisation.

3.4   Research Purpose

Given that the purpose of this study is to determine the impact of the internet in radicalisation among terror groups, the researcher employs a combination of research methods mainly pure, applied and exploratory techniques. According to Charters (2014), the pure element allows for the acquisition knowledge that can be the basis for theories to be used in the applied research. However, the exploratory element serves the purpose of the research which is to seek a deeper understanding into how Al Qaeda, ISIS and other terror groups reach recruits and convince them to join their course. Swanson (2015) corroborates the assertion in that an exploring researcher is likely to discover new information that can be a basis for new studies or solutions to the prevailing problem, in this case terrorism as a security threat. The findings of pure and exploratory research are then applied in subsequent topics in the same subject to form a new understanding of the problem or a fresh academic approach to terrorism, communication and radicalisation.

3.5   Research Approach

The primary research approach is the inductive method. According to Burney and Saleem (2008), the inductive approach seeks to develop theories of study from the existing data on a given topic. In the context of this study, the research will accumulate data from prominent sources such as the Rand Organisation and the Global Terrorism Database to understand the

extent to which the internet furthers the course of Al Qaeda, ISIS and other extremists. Soiferman (2010) agrees with Burney and Saleem (2008) in that the inductive approach is suitable for the exploratory and confirmatory research purposes discussed in the preceding section of the methodology. Unlike the inductive approach, deduction involves working with a "top down" approach to prove a theory (Creswell and Clark, 2007). Therefore, since the study aims to use secondary sources to understand the relationship between the internet and radicalisation, induction is the most suitable research approach for the subject of terrorism. There is a consensus among Creswell and Clark (2007), Soiferman (2010) and Burney and Saleem (2008) that using induction or deduction is incumbent on the type of subject and elements of topic under study.

3.6 Research Strategy

A qualitative analysis using secondary sources is the primary research strategy that will enable the exploration and confirmation of the research purpose relating to radicalisation through the internet. Whiteside, Mills, and McCalman (2012) note that a qualitative research strategy employing secondary data is vital for building a theoretical understanding for a complex social issue such as terrorism. Furthermore, given the scope of the topic of study, primary data collection is highly unreliable and only data and information from news articles, prominent global organisation and published research can assist in exploring the impact of the internet in the radicalisation of individuals into the terrorism doctrine. According to López (2017), the qualitative research strategy using secondary data requires minimal processing which makes is easy for the research to summarise and form inferences from the acquired information. Greenhoot and Dowsett (2012) agree with López (2017) when he contends that a research strategy involving secondary data is vital for answering critical developmental questions such as the difference in the use of the internet between Al Qaeda and ISIS terror groups.

3.7 Data Collection Method

The data collection mode for any research paper must fit the methodology's research objective, philosophy, purpose and strategy (University of Minnesota, 2019). The global nature of the

subject of terrorism requires the researcher to adopt a broad perspective while still narrowing down on a given element of study. Therefore, for the elements of internet usage and radicalisation in relation to terrorism, the data collection method involves an analysis of published documents and records from recognised institutions and organisations such as news agencies and global bodies respectively.

For the sake of this study, the researcher relied heavily on data collected from the Global Terrorism Database (GTD) and the RAND Database of Worldwide Terrorism Incidents (RDWTI). With a collection of more than 180000 documents on the details of terrorist attacks globally since 1970, GTD offers the researcher the requisite data to efficiently explore, determine and investigate the impact of the internet on radicalisation of individuals by Al Qaeda and ISIS (Miller, LaFree, and Dugan, 2018). Questions on demographics, region of attack, the responsible party and the mode of communication used would be vital in answering questions concerning the distinction between terror groups.

While GTD provides access to terrorist activities since 1970, RDWTI provides details of extremist events with data collection variables such as regional expertise, online language patterns, and comprehensive data on terror activities (RAND Corporation, 2019). Therefore, the first step in the data collection would involve surfing through GTD to determine the attacks and incidents worth analysis on the basis of impact, method of communication and scope of internet usage. For clarity, the researcher would use the RAND database to narrow down to specific data variables such as internet use, online data movement and all elements related to radicalisation and the use of the internet. RAND is a justified source of data given their citation of the use of internet radicalisation in terrorism and extremism as of 2013 (Behr et al., 2013).

Although the above databases are vital in providing raw data for analysis, publications from the government, global bodies and new agencies are also essential for providing context through editorials and opinions from experts. For instance, Gill et al. (2017) wrote an article on the quantifying behaviours, patterns and processes for individuals radicalised through the internet. Koehler (2015) corroborates the sentiments of Gill et al. (2017) and the two articles can be the basis for understanding the raw data from RAND and GTD databases.

Information on countering cyber-terrorism and exploitation of the internet by extremists from recognised global institution such as the Council for Foreign Relations (2015) and UNODC (2012) provide a global context of the impact of internet use by extremists. The most affected countries are also a source of secondary data since the governments publish data for public sensitisation on radicalisation and terrorism. For example, while the US Department of State (2007) wrote on terrorist motivation and behaviours in the 21st century, Bjelopera (2017) from the Congressional Research Service adopts a narrow approach of internet use by domestic terrorists in the US. Still, cases in the public domain such as that of Hosam Maher Husein Smadi who pleaded not guilty of trying to blow up a Dallas skyscraper offer more context into the subject of radicalisation of youths (Mantel, 2016).

3.8 Data Analysis

The above data is collected and analysed using tables, charts and statistical approaches. Given the search for the relationship between internet use and radicalisation as well as the impact, Excel is the main tool for the use in this study. Excel records terror attacks and incidents according to the different variables such as communication mode, region, and online data movement. From such data, it is possible to determine the strength of the relationship between modern extremism and the use of the internet. The range of relations is -1 to + 1 depicting a weak and strong correlation respectively (Laerd Statistics, 2019). Given the lack of primary data, there would be minimal statistical inferences and data analysis would depend wholly on figures and statistics from RAND and GDT coupled with information from news sites, global agencies and government publications. Arkkelin (2014) supports a researcher's approach due to its ability to offer different modes of data analysis, transformation and output.

3.9 Research Limitations

The primary limitation of the study is the possibility of overwhelming data and evidence on the impact of internet in radicalisation given the various avenues of secondary data source (Kekalih, 2005). If the researcher fails to undertake a proper analysis using secondary data, then the results are an imperfect reflection of reality. Furthermore, it is difficult to determine the validity and

quality of the data and information from the various sources with some offering contradicting figures and statistics, thus complicating analysis. The difference between the goal of the secondary sources and that of the researcher can raise bias on the part of the analyst.

3.10 Sampling Method

The sampling of secondary data on internet usage and radicalisation first considers updated electronic and written sources. According to Barrow (2009), it is recommended to have a form of random sampling to eliminate some of the publications and also starting with the most recent sources to ensure the collection and analysis of the most accurate and relatable data. A sample of records according to the variables of study such as region of attack, age of extremist and method of radicalisation are critical for sampling secondary data of a large scope such as terrorism.

3.11 Pilot Study

The study considers that the topic of terrorism is broad and the method of data collection and analysis is equally complicated, thus, the need for a pilot study. Van Teijlingen and Hundley (2002) contend that a mini-version of the full-scale research enables the researcher to examine the viability and validity of the topic of study. The researcher can examine the impact of radicalisation in a single region of the US as one of the countries mostly affected by terrorism. By analysing data from the news articles, government publications and other organisations, the viability of a broader study of Al Qaeda and ISIS radicalisation is visible.

3.12 Ethical Considerations

The two major ethical considerations are the consent for the use of secondary data and the ability to access archived information without infringement of copyright laws (Grinyer, 2009). A publication's consent for an unknown future purpose cannot be sufficiently informed or determined and the researcher may unknowingly use information without proper regulation. Furthermore, anonymisation of data and information for re-use increases the risk of misuse and also damages data quality. The rigorous codes of practice involvement access to classified

government records coupled with tight copyright laws can diminish the validity of a research outcome due to a constrained study process.

3.13 Summary

The ontological research philosophy that seeks the relationship between two elements of a broader concept is vital for understanding how extremist emanates from radicalisation of individuals through the internet. The purpose and objectives of the research are achieved through a qualitative research study that uses secondary data and an inductive approach to help understand terrorism from the existing data on radicalisation and internet usage in the 21st century. Data collection and analysis are vital aspects of the study which are the basis for a conclusion that may provide an alternative academic perspective on the subject of terrorism and extremism.

4 Results and Analysis

4.1 Introduction

The role of the internet in furthering the course of Al Qaeda and ISIS terror operations through radicalization boils down to the communication and financial interactions that can be performed online. In this chapter, the researcher evaluates data collected from various sources to develop themes for further breakdown and discussion. In this regard, the data is checked for its ability to respond to research questions, and the responses compared to the objectives set at the onset of the data collection process.

4.2 Data Analysis Process

With the research being purely inductive, the data relied upon is obtained from multiple sources, including peer reviewed journals regarding related subjects, terrorism database and government records on communication and terror. Primarily, the patterns identified from the information obtained from both government databases and organizational systems inform the interpretation of the qualitative information. From the interpretation, the statistical comparisons can be introduced as a means of associating patterns to themes identified from interpretations of the

information these sources provide. Recurring trends in the process of online transmission of radical data, communication with members of extremist groups and the motivation of terrorist attacks within encrypted networks, can be identified and themed. Data presented from the sources accessed is dependent on the primary research performed by the original compilation in each source, and is dependent on the review and credibility of the researcher. Nonetheless, being published journals and authorities on such information, the data should be largely similar to the actual conditions.

4.3   The Scale of Terror Communication Cells on the Internet

Radicalization spreading through communication cells on the internet dominated by terrorist patrons is a significant contributor to the recruitment platform for ISIS and Al Qaeda. From the Dienel et al. (2010) definition of terrorism, the political, civil, social and religious interests of extremist groups play the most critical role in recruiting new subjects into the doctrines they operate by. The following themes were identified within the Islamism group of ISIS:

Mobilizing sympathy online

Post 9/11 terrorism in the United States is very much dependent on remote communication between persons within the regional borders and external actors. From the illustration that the country's risk of terrorism has increased, the statistical inference for the persons injured, killed, or associated with terrorism can be made with the growth of sympathizers online. While the data from Wilson (2017) estimates that the number of Islamist sympathizers in the American borders may be increasing due to localized communication, radicalization remained largely undefined. Mobilizing sympathy for terrorist operators, from the data level, requires the identification of the most vulnerable individuals, their inclusion in faith-based online seminars and their initiation into extremism.
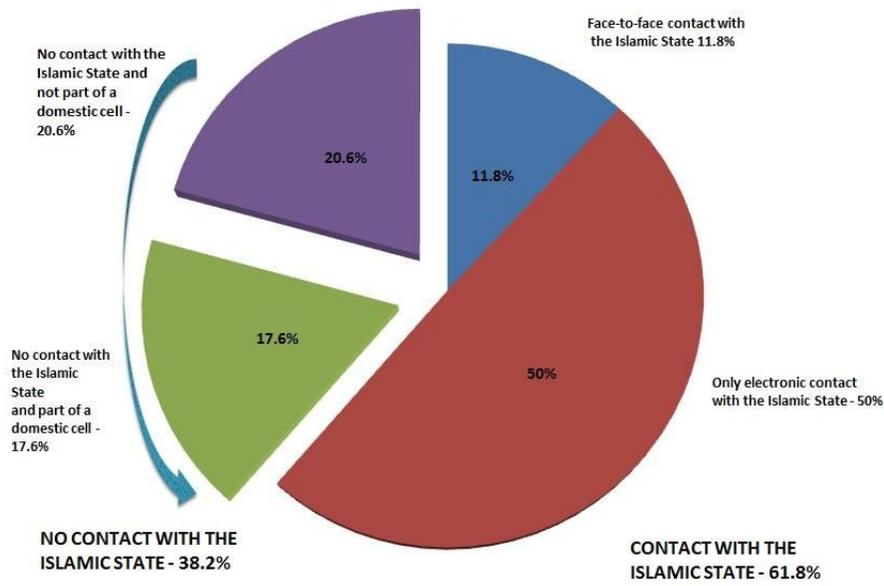
Figure 1- Contact level with radicalized members of ISIS (United Nations Office on Drugs and Crime 2012)

From *figure 1* above, it is possible to compare the contact level achieved with radicalized members of ISIS over time, including radicalization from the group by pure online engagement. Of the 61.8 % of the contact achieved with the extremist group through direct communication, 50% was achieved with electronic means. In the modern world, it is unnecessary to come into physical contact with the terrorist organization, with electronic contact offering a suitable platform for interaction. From the above illustration, it is evident that domestic terrorism has changed, with the utilization of online communication that transcends the need for complex communication, or cross-border travel. Also, the graphic represents the decreasing necessity for expanded theaters of operation for ISIS, allowing them to confine themselves to functional social media platforms for recruitment, encrypted private messaging and exchange of material, or finances.

4.3.1 How do potential terrorist (ISIS and Al Qaeda) use internet to communicate?

In as much as the communication technologies may be blamed for facilitating the underlying transition between the exchange of information regarding life's philosophy (on an ontological level) to the knowledge that is exchanged, individuals are also inclined towards such platforms. Extremist online forums are often private chat rooms that evade checks, which are

intended to prevent the misuse of loopholes in online systems. Consideration of the communication patterns for radicalized persons requires the comparison of the level of contact one may have had with a terror group, and the result this has on terrorism on a global scale. From the combination of the previously reviewed datasets (Figures 4, 6 & 7), the following comparative graph (Figure 2) can be deduced for further analysis and discussion.
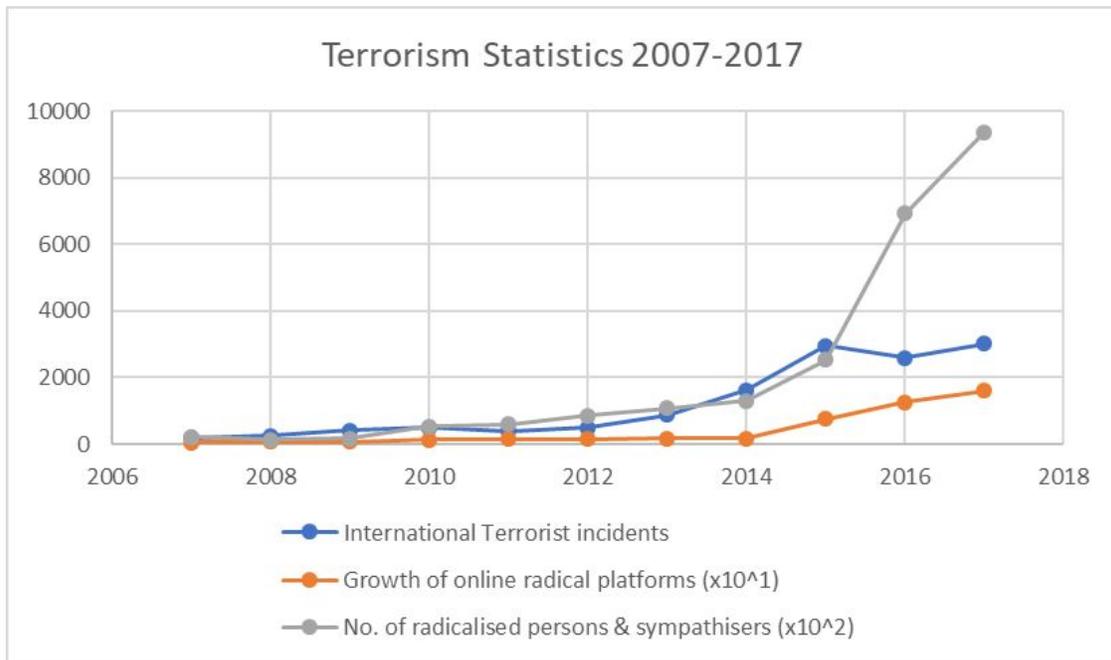

Figure 2- Compiled Terrorism Statistics (Europol, 2019, RAND Corporation, 2019 & UNODC, 2012)

Fundamentally, the comparison of the incidences of terror across the globe show significantly comparable growth to the increased usage of the internet over the last decade, to the extent of facilitating radicalization. Furthermore, the increased number of persons exposed to the terrorists' agenda has been facilitated by the explosive use of the internet, over the last five years, for the propagation of their agenda. While it is impractical to assume that this is the sole reason for the increased number of international terror incidents, it would be unwise to assume that social media, encrypted messaging and rapid communication haven't had an impact. The UK, for example, has seen the increase of ISIS brides, some as young as 15, moving into Syria through Turkey after various aspects of similar conversations were shared with them (Abdel-Fattah, 2015). Such processes of radicalization allow for these UK citizens to be converted into

sympathizers, ending up as ISIS brides serving the interests of the terror operatives in the Middle East.

Confining theaters of operation

Within the example of the Islamism groups operating in the Middle East, Choi, Lee, and Cadigan (2018) illustrate how the internet can alter the communication patterns to include identity responses to sympathizers. Based on requests, the database of the United Nations Office on Drugs and Crime (2012) provides an opportunity to identify potential theaters of operation based locally in the United States, commonly grouping sympathizers, radicalized activists and terrorists on confined theaters of opinion. Online platforms, such as social media, represent the largest aspect of this statistic (40-60%), as observed in the radicalization assessment of potential subjects. The inclusion of this activity on a variety of internet platforms allows the extremist group to alter its identity and offer knowledge that suits each individual.
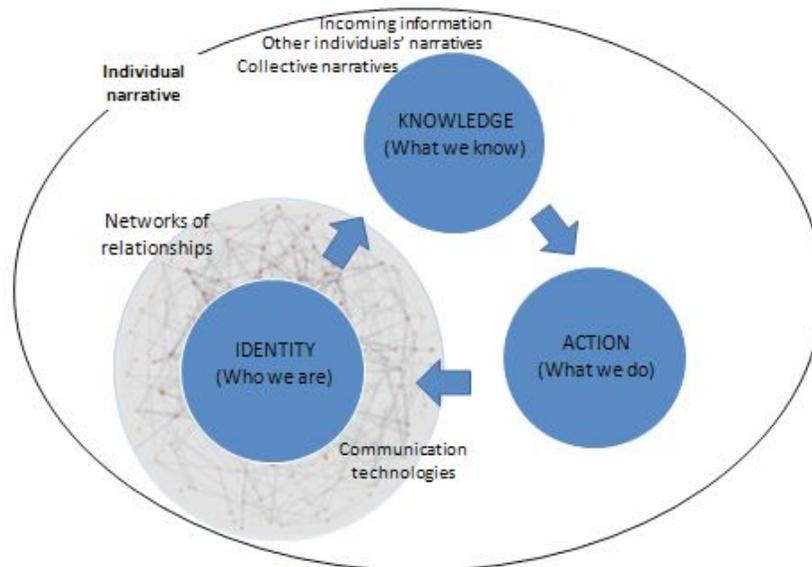
Figure 3- Process of terror communication online (Council on Foreign Relations, 2015)

The pattern of confining an individual to specific theaters of mental operation is the base definition of the alteration of knowledge, identity and actions within terrorism. From the fundamental individual narrative, the dataset by U.S. Department of State (2007) proves the

extent to which social media and other internet-based platforms influence readers. Furthermore, this is supported by the statistical records from Speckhard, A. Shajkovci Yayla (2018) regarding the existence of terror communication cells online. Access to extremism-related information on the internet is dependent on communication technology, which is intended to be optimized for everyone's consumption.

Statistically, the likelihood of a vulnerable individual coming into contact with extremist or radicalizing information has grown with the advent of social media (The Independent, 2019: BBC News, 2019). In recent happenings, the recruitment of young girls into ISIS territory has been highlighted as a plight for the improper influence of the internet. These girls are lured into serving the interests of ISIS, have travel documents arranged and facilitated through the dark web (The Independent, 2019). The following datasets showcase the extent of the risk, the validity and the extreme nature in which localized terror cells can operate. From intelligence, the online personnel who are on the watchlist for engaging sympathizers or radicalized persons online, it is possible to identify the direct role of Al Qaeda. The graphic indicates the threats from terror groups, from which individuals are identified for callous claims and placed under investigation (a watchlist).
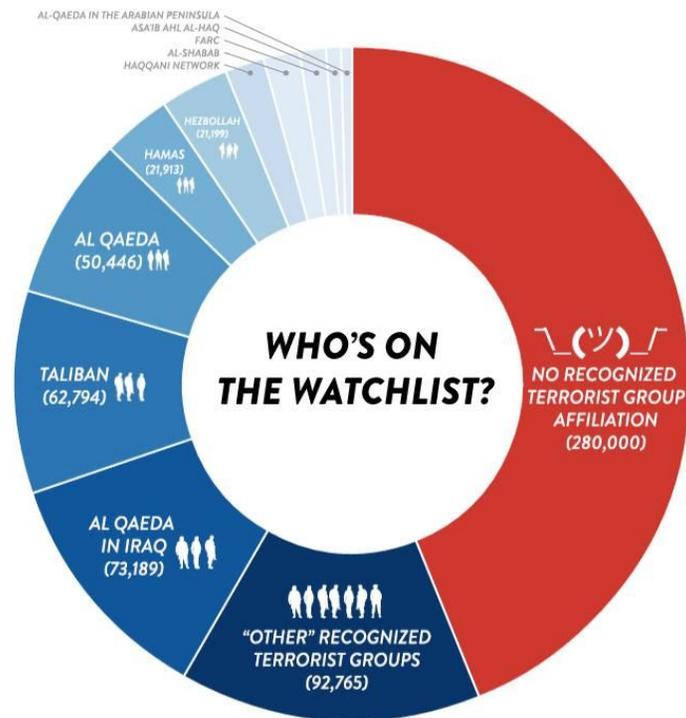
Figure 4- Persons on Online Watchlists (The Independent, 2019)

4.3.2 How do communications play a role in radicalizing individuals?

With regard to the themes and statistical patterns within which extremist communication and radicalization occurs, potential pathways of communication can be identified from secondary data. Increasingly being exposed to information suited to extreme opinions increases the possibility of the communication leading to a radicalization process, actively engaging the subjects in specific material that motivates their extreme views, thereby, growing their convictions (Bhatia, 2009). The following data illustrates the transitions that occur with regard to transitioning information exchange into recruitment and racialization opportunities for extremist groups.
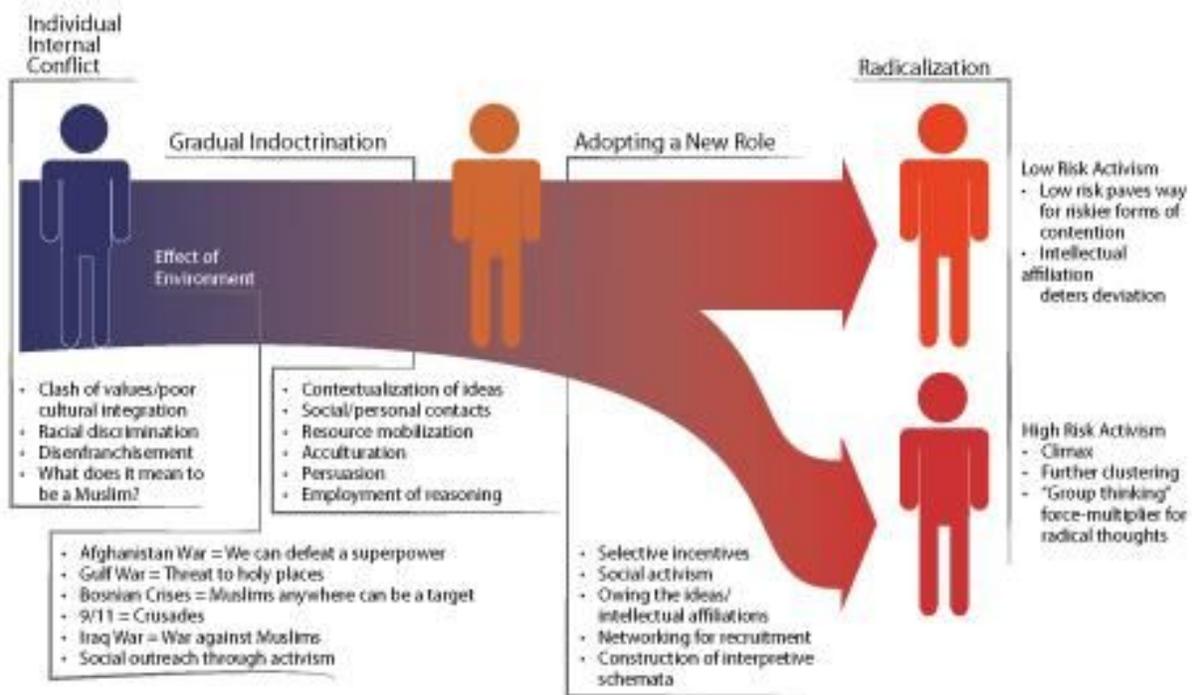
Figure 5- Individual internal conflict during radicalization (United Nations Office on Drugs and Crime 2012)

4.3.3 What online strategies do ISIS and AL Qaeda use to radicalize / recruit people?

The influence of similar domestic cells acting with the same extremist agendas reflects comparatively similar statistics. From the perspective of by Shefet (2016) regarding the spread of the message of terrorism across the internet, it is arguable that the data regarding communication structure, also, directly influences the framework defining the possible operations of the inspired factions in other regions of the world. Progressive interaction with communication cells for extremist groups online furthers the agenda that they pursue, primarily, with regard to inspiring followers and new factions (Wilson, 2017). Communication, therefore, is the basis of the formation of the structure for terror cells, both locally and on the global scene. Extremism, for instance, relies on the development of doctrines from the original concept into specific terrorist activities, or additional radicalization and recruitment.

4.3.4 Is the internet the only mean of recruiting, radicalizing and triggering individuals to act?

In the European context, the consequences of terrorists mobilizing youth and increasingly spreading the radical agenda is visible, due to the increased number of sympathisers and lone wolf attackers. It is possible to evaluate this aspect as a consequence of mobilization from the online platforms illustrated in the previous subsection, having grown over the last decade. Convincing subjects to join the cause of a terrorist operation requires radicalization online and adopting different techniques. From the RAND and EUROPOL databases reflecting the amount of cybercrime related to terrorism, one may develop an argument regarding the relevance of online radicalization.
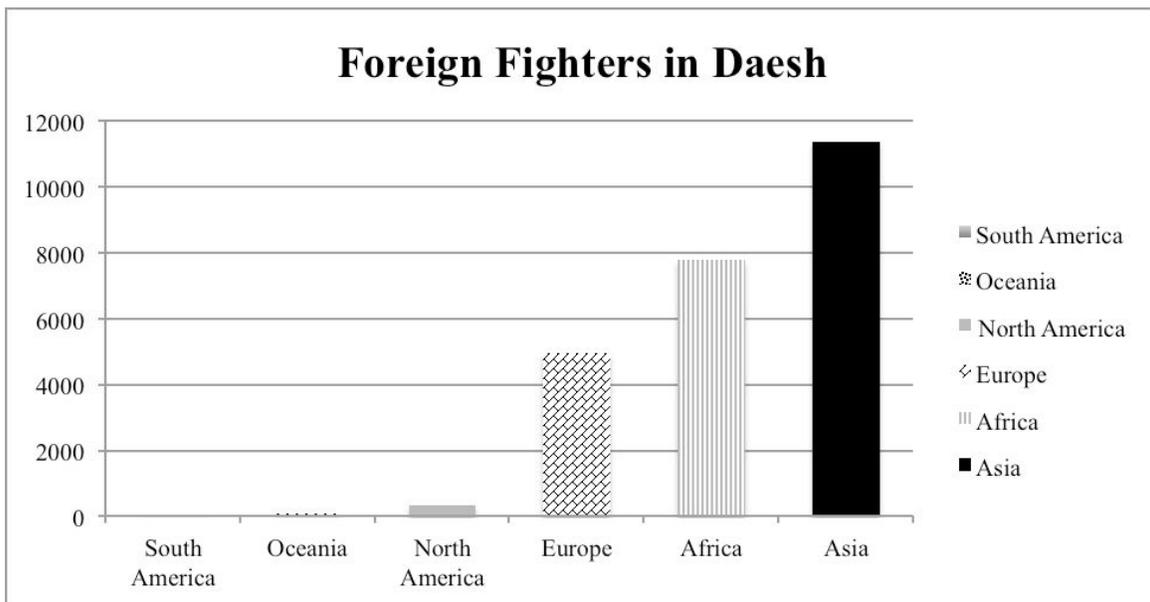

Figure 6- Foreign fighters in Al Qaeda (Daesh) (Terrorism. n.d)

In as much as the mobilization of fighters for Al Qaeda/Daesh is dependent on the completion of the radicalization process to the point of recruitment, the data can be used to understand the process. From Figure 6 comparing European to African and Asian fighters in Daesh, one can identify that the Islamist terrorism ranks highly functional with persons who are vulnerable. Primarily through the presentation of a specific level of information, training and mobilization content, an Islamist group, such as ISIS, could change an individual's political

convictions from neutrality to activism, radicalism and, finally, terrorism, reflecting the journey of communication that is of interest (Wilson, 2017). The transition in ideology follows a similar path, with the neutral persons being exposed to new opinions that rationalise radical terrorist actions. In this way, individuals are transformed into sympathisers and into justifiers who, eventually, are convinced of their obligation to the cause. Such regions are more prone to such recruitment due to the combination of factors including Islam doctrines being more accepted there, inadequate anti-terror government surveillance and the presence of physical terror groups training camps (Council on Foreign Relations, 2015). Online platforms allow for the communication with such persons to be practical and effective in bringing across the message of extremism. Within the analysis, it is arguable that persons may be influenced not only by online engagement, but by chancing across radical, extreme opinions on social media, or the internet. Within this communication pattern, it becomes likely for the individual to seek additional material that is related to the radical communiqué received earlier, which essentially reinforces underlying convictions and beliefs.

Statistically, the process taking place online may transcend the communication of exchanging messages to revolve around actual training, indoctrination and mobilization into joining the Jihadist movement (Torok, 2015). The following graph combines the context of European terrorist actors sourced from their home countries, radicalised online, recruited and sent back to carry out attacks.
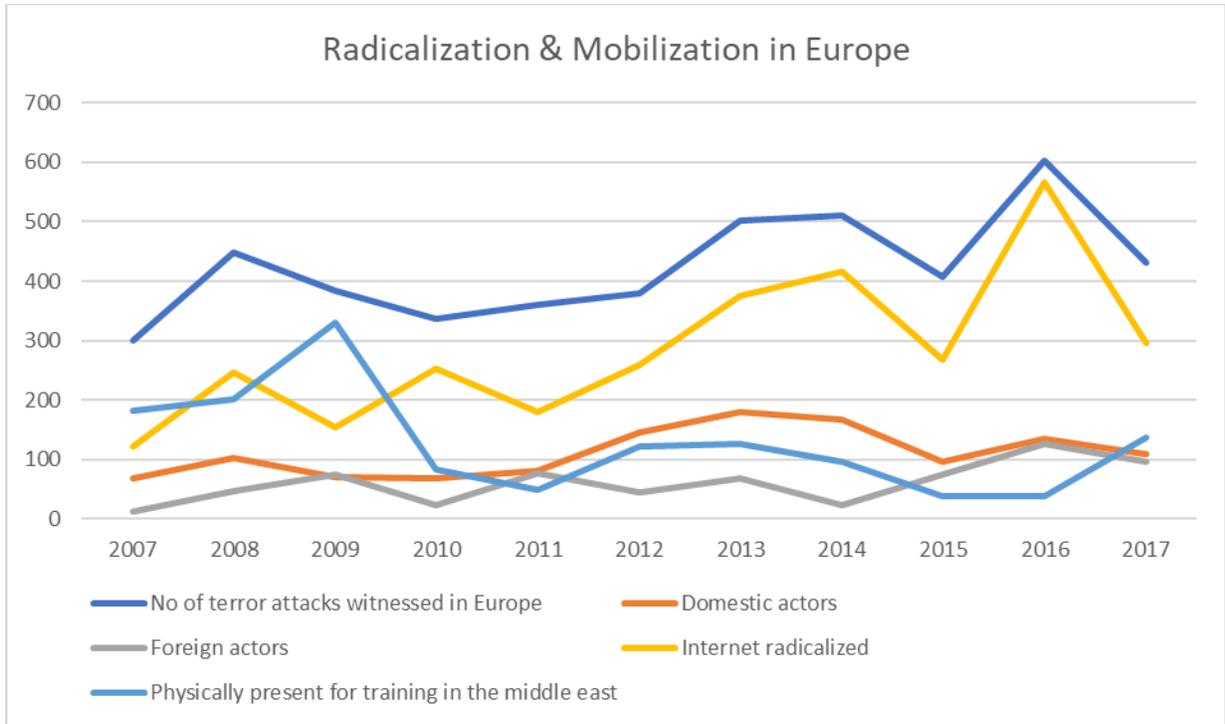
Figure 7- Radicalization & Mobilization in Europe (Europol, 2019, RAND Corporation, 2019 & UNODC, 2012)

In comparison to the indicator of the number of European fighters radicalized and mobilized by Daesh, it is arguable that these results indicate the possibility of a significant influence of domestic terrorism. Through the inspiration of 'lone wolf' actors, the evidence emerges from the increased attacks featuring radicalized men, who had not been in previous contact with the extremist cells in the Middle East (Wilson, 2017). Still, due to the increased interactive nature of the internet, sharing content, inspiring extremism and training terrorists via social media and peer-to-peer messaging has become more practical. Furthermore, the graph illustrates the reduction in the need for the physical presence of persons in radicalization camps in active fighting areas in the Middle East. Due to the possibilities presented by the internet, mobilization for domestic terrorism inspired by extremist religious beliefs is becoming more appealing for terror groups operating cells within European borders. Basically, the identification of a potential subject for recruitment, or radicalization, stems from their underlying interests, vulnerability, or pre-existing notions regarding politics, or religion (Torok, 2015).

The structure of radicalization is significantly dependent on the individuals and their level of conviction, once they are engaged on the online platform offering communication and interaction with like-minded persons. Base on the accounts of radicalised persons duped into becoming ISIS brides by The Independent (2019) and the BBC (2019), it is possible to appreciate that the online scheme is powerful enough to influence the perception of an individual. To some extent, the consumption of everyday information from other sources only serves to escalate the process, with the individuals being fully indoctrinated with the convictions of their radicalism (Council on Foreign Relations, 2015). From the communication structure, it is possible to anticipate the existence of closed-communication channels and encryptions that guarantee the online participant anonymity and confidence, as radical convictions grow. For example, with the existence of cryptocurrencies such as Bitcoin, untraceable transactions can facilitate other forms of financed terrorism domestically without detection by anti-terror monitoring systems (Wilson, 2017). Similarly, the adoption of a new role for the subject is sufficiently dependent on that person's internal conflict and pre-existing convictions regarding politics or religion. Within the dark web, the transactions, interactions and engagements of these terrorists and their proxies facilitates the existence of undetected communication and transaction systems on the internet.

For each context, the radicalization structure forms itself around the social incentives that a subject undergoing constant communication receives. Ranging from the development of interpretative schemes for normal social events, to skewed construal of political contexts, the altered communication on the platforms is shaped to resemble normal content (Wilson, 2017). However, such misconstrued information often increases the intellectual affiliation of the individual, inspiring loyalty to the cause and group thinking for the radicalized individual (The Independent, 2019). However, the technique and structure may vary to include a catalyst event, which inspires and stirs an individual from radicalization into performing acts of terrorism and violent extremism.

4.4   Discussion & Analysis

The global nature of the issue of terrorism brings into question the possibility of similar communication and radicalization framework being employed elsewhere. With the indoctrination of the individual depending on the pre-existing convictions, the recontextualization of their ideal defines the basis of their radicalism (Torok, 2015). Essentially, the functionality of the framework for the operation of online communication is underpinning the existing beliefs of individuals and bolstering their intellectual certainty. Progress regarding this aspect requires the indoctrination of the individuals, to ensure their intellectual affiliation and interpretative schema reflects the radicalizing principle (McCauley & Moskalenko, 2014). Basically, this fixates the individuals on their schemes, beliefs and thought processes, limiting the relevance of other external information that would have, otherwise, interfered with the convictions that the individuals have adopted.

Within the consideration of the impact of the internet in radicalisation, primary focus is on the activities of ISIS as the most active perpetrator group as of 2018. Their recruitment methods have been examined within an inductive approach, in which the examination of data allows the researcher to develop a new understanding of concepts and context. Fundamentally, such an examination is intended to reflect how epistemology, ontology and doxology impact internet-based radicalisation, through the identification of patterns and background data accessed during research. The skewing of such information to fit an agenda is facilitated by the combination of a specific set of content. Wilson (2017) posits that the glorification of actions by terrorists motivates the radicalized individuals to justify their need, accept the role of violent extremism and rationalize it. At this stage the structure of communication is altered (both by the individual and the online platforms engaged in) to reflect the most extreme of opinions regarding everyday events (Speckhard, Shajkovci & Yayla, 2018).

4.5   Cases of Terrorism Linked to the Internet

In 2010, the actions of a terrorist in Stockholm, Sweden, reflected the radicalization of an individual through the indoctrination, recruitment and training on online platforms. The case of the terrorist, Taimour al-Abdaly, brings into focus some of the concepts regarding the success that terrorists have had in transitioning radical individuals into lone wolf terrorists. The

individual was originally a Disk Jockey (DJ) in Great Britain, was contacted, radicalized and eventually recruited through the internet. His training on handling explosive material and preparing suicide bombs was decidedly different to the layman skills that he had originally (Waskiewicz, 2012). Arid Uka presents a similar case, where his inspiration was the extremist content posted on social video sharing forums.

From the theoretical perception presented in the literature review section, the possession of anti-western propaganda can be seen to have been advanced into radical opinions and, eventually, into terrorist activities. Similar analysis can be done for the case of Arid Uka, who became another Salafi lone wolf terrorist inspired by material he found online from ISIS and Al Qaeda, prompting him to use a weapon to shoot American soldiers, due to his anti-western beliefs that became radicalized. Parallels drawn between the two cases indicate that the individuals did not have direct contact with the terrorists, instead, interacting and exchanging material online. While the motivation was obtained from a combination of content and material supplied by the terrorists, the trigger for these individuals was their original radical perception towards persons who they eventually attacked (Waskiewicz, 2012). However, with their consumption of information from the extremists, they were radicalized continuously and were eventually triggered into carrying out lone wolf attacks.

Comparisons can be made to the 2018 Strasbourg attack, with the attack being carried out by yet another young individual, acting independently of the terrorists who had radicalized him. 29-year-old Cherif Chekatt was inspired by material that he had obtained from ISIS in digital format, to carry out a brutal, lone wolf attack on civilians. The individual had not been originally observed to be associated with terror groups, with his family being unable to explain the radicalization that had pushed the attacker to act. However, the evidence of material that he had received can be used to explain the extent to which an individual can be radicalized and pushed into performing a domestic attack (Nesser, 2018). In as much as the affiliation that this individual had did not require special training, his crude attack using a rifle and knife required conviction for him to gain the motivation to act on his extremist intent as pushed. The explanation for this is entirely based on the theoretical pathway along which the communication

with the extremist allowed the individual to become an extremist, without having to physically interact with the terrorists.

While the extremist opinions of individuals can be performed with the engagement of the radicalization process, the conspiracy of the husband and wife, Syed Farook and Tashfeen Malik presents a different situation. The couple was seen to be influenced by videos on online sharing platforms to gain inspiration, along with their access to magazines through private networks (Tsesis, 2017). Eventually, these radicalized persons were able to motivate the Boston Marathon bomber of 2013, through similar communication methods involving terrorist propaganda sourced online and radicalization pamphlets. The actions of online operators, such as these, facilitate terrorist groups like ISIS in arranging their online strategy and to continually use the internet for the recruitment and deployment of insurgent operatives, remotely, across regions in other continents. Some of these individuals have been observed to use platforms, which are regulated, such as YouTube and Facebook, to propagate anti-western material that glorify acts of terrorism and advocate for extremism. Overall, these online radicalization systems take advantage of the opportunities of anonymity and the constraint-free environment enjoyed by unregulated platforms on the internet, to speak out more vocally about their extremist views, than they would do offline.

5   Conclusion

Radicalization is a process that cannot be qualified within a limited experience and its complex and gradual nature makes its discussion intricate. From the onset of gaining sensitivity to radical ideology, to the extent of becoming a member of a group online, the procedure has been evaluated with the aim of identifying the extent to which the internet is relevant. Furthermore, the evaluation of the trends that have existed in the past with regard to intelligence, recruitment and radicalization of individuals to terrorism has shed light on the subject. In as much as the context of such radicalization cannot be associated entirely with internet-based communication, the role proven by the examination of literature and case evidence indicates a significant challenge. During the examination of context provided by the Canadian Security

Intelligence Service and the Federal Bureau of Investigations, various challenges with these forms of radicalization became apparent.

The convictions that radicalised individuals have are linked, primarily, to their extreme beliefs that are indoctrinated through channels such as the internet. From the research process and data analysis, the illustrations of the extent to which the internet can be used by terror groups, such as ISIS and Al Qaeda, prove that such convictions can be used to motivate European and even Africans into radicalization. From the provisions of the FBI and the Canadian intelligence, the consideration of the difficulty of collecting intelligence, or controlling online communication validates arguments that the internet is a growing threat. Furthermore, from the compilation of data comparing trends of terror incidents in Europe and the growth of extremism cells for radicalization, there was correlation. In as much as communicating online is difficult to regulate, the consequences are observed in growing domestic radicalization and actions of terrorists trained online. The consumption of information off the internet allows an individual to appreciate the extent to which a variety of contexts, beliefs and social systems work.

Based on the examples of the young women who opted to join extremists, it is possible to consider social pressure as a contributor and motivator for these persons. Similarly, for young men, the recruits are pushed into radicalization as a refuge from their troubles in life. However, the process of radicalization is gradual, progressively convincing these persons of their duty to act on their radicalised views, eventually recruiting them into the terror network. From the evaluation of the process of radicalization, one gets to appreciate the true impact of the internet. By gaining an appreciation of data regarding the impact of such online engagement for radicals and the eventual acceptance of extremist views, it became possible to understand the significance of the threat of terrorism that exists domestically, based on the cases of European terrorist events. While the most basic aspects of preventing the radicalisation of these European youth requires intervention using the most direct communication channels, it must also include the traditional counter-terrorism methods that aided in preventing attacks and discouraging would-be lone wolf attackers. Anti-radicalism messages on the same platforms as the radicalisation content would also influence a significant number of individuals exposed to the deleterious materials.

While one may not blame the internet for the increased terror threats on the European continent, its contribution and relevance cannot be ignored. In following recommendations for engaging intelligence, instituting counter measures and de-radicalizing people, the basis of the online influence should be considered as the definition of spreading extremism on a global level. As such, this understanding can be used for development of intelligence and counter-terrorism measures by the relevant institutions. The most significant recommendations would be towards the monitoring, analysis and checking of communication that harbours terror threats. For instance, with the identification of loopholes in internet communication that terrorists use, it is possible to gather intelligence and institute counter-measures, which may include mobile-based internet regulation and possible prevention and protection. From the recognition of the ability of terrorist factions to identify and appeal to the younger generation, it is then possible to identify the platforms, websites and forums that terrorist groups like ISIS use.

ISIS' use of publicised executions and propagation of terror as a basis of inspiration is an illustration of motivation through fear, and leads to the engagement of persons inspired by the radical actions of the terrorists. Through their means of communication, these groups have engaged young persons, delivered material online that facilitated their radicalization and, then, recruited these individuals. Private communication enabled by encrypted exchange of information, masking networks and uncensored social media, all appear to have a role in facilitating the spread of radial ideology and its acceptance among vulnerable persons. Still, there is the consideration of literature and specific instances where terrorism events were linked to communication that reflected extremist messages. These messages shared online feature violent torture, philosophical validation of radical action and an invitation to potential jihadists to join terrorist movements. From the evaluation of the success of these forms of communication in reaching out to the vulnerable, radical youth, there emerges need for the implementation of resolutions.

Based on the discussion and analysis of data defining the process, progression and consequences of radicalization of young people from various regions of the globe, it is possible to generate recommendations focused on the counter-measures. Essentially, the policies against cybercrime only cover the extent of communication and there are challenges similar to those in

counter-terrorism, due to the encryption and privatization of online forums. As such, forcing the removal of material that does not conform to law is very difficult. However, with the inclusion of more interactive policies, which force forums to restructure their communication channels to exclude and report such content, it would be more practical to implement some of the proposed measures. Furthermore, the requirement of service providers online to facilitate the reduction of deleterious content on their platforms would be of great benefit, particularly, with regard to social media. Among terror groups, it is possible to investigate and gather additional information on the role of communication in facilitating recruits and amassing financing, and using such data to design counter-measures for desensitizing radicalized individuals.

References

ABDEL-FATTAH, R. (2015, OCTOBER 9). THE STIGMATISATION OF MUSLIMS AS 'COULD-BE TERRORISTS' HAS PRODUCED A TOXIC SOCIAL ORDER. THE GUARDIAN.

AL-RAWI, A., 2018. VIDEO GAMES, TERRORISM, AND ISIS'S JIHAD 3.0. TERRORISM AND POLITICAL VIOLENCE, 30(4), PP.740-760.

ARKKELIN, D., 2014. USING SPSS TO UNDERSTAND RESEARCH AND DATA ANALYSIS. [ONLINE] VALPARAISO UNIVERSITY.

ASHOUR, O. (2009). THE DE-RADICALIZATION OF JIHADISTS: TRANSFORMING ARMED ISLAMIST MOVEMENTS. NEW YORK, NY: ROUTLEDGE.

BANDYOPADHYAY, S., & YOUNAS, J. (2017). TRADE AND TERROR: THE IMPACT OF TERRORISM ON DEVELOPING COUNTRIES. THE REGIONAL ECONOMIST, 25(4).

BARROW, 2009. STATISTICS FOR ECONOMICS, ACCOUNTING AND BUSINESS STUDIES, 5 TH EDITION. PEARSON EDUCATION LIMITED

BAST, S. (2018). COUNTERTERRORISM IN AN ERA OF MORE LIMITED RESOURCES (CSIS BRIEFS).

BBC NEWS. (2019). *WHO WILL TAKE IS FIGHTER AND HIS TEENAGE 'BRIDE'?*. [ONLINE]

BEHR, I., REDING, A., EDWARDS, C. AND GRIBBON, L., 2013. RADICALISATION IN THE DIGITAL ERA. RAND, [ONLINE]

BERTRAM, L., 2016. TERRORISM, THE INTERNET AND THE SOCIAL MEDIA ADVANTAGE: EXPLORING HOW TERRORIST ORGANIZATIONS EXPLOIT ASPECTS OF THE INTERNET, SOCIAL MEDIA AND HOW THESE SAME PLATFORMS COULD BE USED TO COUNTER-VIOLENT EXTREMISM. JOURNAL FOR DERADICALIZATION, (7), PP.225-252.

BHATIA, A. (2009). THE DISCOURSES OF TERRORISM. JOURNAL OF PRAGMATICS, 41(2), 279-289. DOI: 10.1016/J.PRAGMA.2008.05.016

BHATIA, K., & GHANEM, H. (2017). HOW DO EDUCATION AND UNEMPLOYMENT AFFECT SUPPORT FOR VIOLENT EXTREMISM?: EVIDENCE FROM EIGHT ARAB COUNTRIES. WASHINGTON, D.C: THE BROOKINGS INSTITUTION.

BJELOPERA, J., 2017. DOMESTIC TERRORISM: AN OVERVIEW. [ONLINE] CONGRESSIONAL RESEARCH SERVICE.

BRUNEAU, E. G. (2016). UNDERSTANDING THE TERRORIST MIND. CEREBRUM: THE DANA FORUM ON BRAIN SCIENCE, 2016.

BURNEY, S. AND SALEEM, H., 2008. INDUCTIVE & DEDUCTIVE RESEARCH APPROACH. [ONLINE] DEPARTMENT OF COMPUTER SCIENCE; UNIVERSITY OF KARACHI.

CANADIAN SECURITY INTELLIGENCE SERVICE. (2018). MOBILIZATION TO VIOLENCE (TERRORISM) RESEARCH: KEY FINDINGS. AUTHOR.

CHARTERS, W., 2014. PURE RESEARCH AND PRACTICAL RESEARCH. THE JOURNAL OF EDUCATIONAL RESEARCH, 12(2), PP.95-101.

CHOI, K. S., LEE, C. S. AND CADIGAN, R., 2018. SPREADING PROPAGANDA IN CYBERSPACE: COMPARING CYBER-RESOURCE USAGE OF AL-QAEDA AND ISIS. INTERNATIONAL JOURNAL OF CYBERSECURITY INTELLIGENCE & CYBERCRIME, 1(1), PP.21-39.

CORDESMAN, A. H. (2016, JULY 27). TERRORISM: THE THING WE HAVE TO FEAR THE MOST IS FEAR ITSELF.

COUNCIL ON FOREIGN RELATIONS, 2015. COUNTERING ISLAMIC STATE EXPLOITATION OF THE INTERNET. [ONLINE]

CRESWELL, J.W. AND PLANO CLARK, V.L., 2007. DESIGNING AND CONDUCTING MIXED METHODS RESEARCH. THOUSAND OAKS, CA: SAGE PUBLICATIONS.

DE ARAÚJO, P., GUIMARÃES, J. AND TENNIS, J., 2017. THE CONCEPT OF EPISTEMOLOGY IN KNOWLEDGE ORGANISATION. [ONLINE] UNIVERSITY OF WASHINGTON SEATTLE.

DEARDEN, L. (2014, SEPTEMBER 3). 'JIHADI JOHN': IDENTITY OF ISIS MILITANT WHO BEHEADED STEVEN SOTLOFF AND JAMES FOLEY REMAINS A MYSTERY. THE INDEPENDENT.

DICKEY, C. (2017). WHY TERRORIST RECRUITS SHARE THESE THREE MOTIVATIONS.

DIENEL, H., SHARAN, Y., RAPP, C., & AHITUV, N. (EDS.). (2010). TERRORISM AND THE INTERNET: THREATS, TARGET GROUPS, DERADICALISATION STRATEGIES. WASHINGTON, DC: IOS PRESS.

Doosje, B., Moghaddam, F. M., Kruglanski, A. W., de Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. Current Opinion in Psychology, 11, 79-84. doi: 10.1016/j.copsyc.2016.06.008

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

Europol. (2019). EU Terrorism Situation & Trend Report (Te-Sat).

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan, J., 2017. Terrorist use of the internet by the numbers. Criminology & Public Policy, 16(1), pp.99-117.

Gomes, A. D. T., and Mikhael, M. M., 2018. Terror or terrorism? Al-Qaeda and the Islamic State in comparative perspective. Brazilian Political Science Review, 12(1).

Gordon, J. S. (2016). The identification and exploitation of terrorist financing (Senior Honors Theses). Helms School of Government.

Greenhoot, A. and Dowsett, C., 2012. Secondary data analysis: an important tool for addressing developmental questions. Journal of Cognition and Development, 13(1), pp.2-18.

Grinyer, A., 2009. The ethics of the secondary analysis and further use of qualitative data.

Guarino, N., Oberle, D. and Staab, S., 2009. What is an ontology? Handbook on Ontologies, pp.1-17.

Harrington, W., 2018. The new radicalisation of the internet. [Online] New York Times.

Hoffman, B. (2006). Inside terrorism (2nd ed.). New York, NY: Columbia University Press.

Islamic State and the crisis in Iraq and Syria in maps. (2018, March 28). BBC News.

Ismail, N. (2018). Tackling extremism through the power of second chances.

Kekalih, A., 2005. Secondary data analysis: its uses and limitations. [Online] Henri.

Kepel, G., & Jardin, A. (2017). Terror in France: The rise of Jihad in the West. Princeton, NJ: Princeton University Press.

KLAUSEN, J., CAMPION, S., NEEDLE, N., NGUYEN, G., & LIBRETTI, R. (2015). TOWARD A BEHAVIORAL MODEL OF "HOMEGROWN" RADICALIZATION TRAJECTORIES. STUDIES IN CONFLICT & TERRORISM, 39(1), 67-83. DOI: 10.1080/1057610x.2015.1099995

KOEHLER, D. (2014). THE RADICAL ONLINE: INDIVIDUAL RADICALIZATION PROCESSES AND THE ROLE OF THE INTERNET. JOURNAL FOR DERADICALIZATION, 1, 116-134.

KOEHLER, D., 2015. THE RADICAL ONLINE: INDIVIDUAL RADICALISATION PROCESSES AND THE ROLE OF THE INTERNET1. [ONLINE] JOURNAL FOR DERADICALISTION.

LAERD STATISTICS., 2019. PEARSON PRODUCT-MOMENT CORRELATION - WHEN YOU SHOULD RUN THIS TEST, THE RANGE OF VALUES THE COEFFICIENT CAN TAKE AND HOW TO MEASURE STRENGTH OF ASSOCIATION. [ONLINE]

LANGKOS, S., 2014. RESEARCH METHODOLOGY: DATA COLLECTION METHOD AND RESEARCH TOOLS. [ONLINE] UNIVERSITY OF DERBY.

LÓPEZ, X., 2017. SECONDARY DATA. THE SAGE ENCYCLOPEDIA OF COMMUNICATION RESEARCH METHODS.

LOVETT, I. (2014). ANTIGOVERNMENT OBSESSION PRECEDED LAS VEGAS SHOOTINGS. [ONLINE] NYTIMES.COM.

MALIK, N. (2019, SEPTEMBER 20). THE FIGHT AGAINST TERRORISM ONLINE: HERE'S THE VERDICT. FORBES.

MANTEL, B., 2016. TERRORISM AND THE INTERNET. [ONLINE] CQ RESEARCHER BY CQ PRESS.

McCAULEY, C., & MOSKALENKO, S. (2014). TOWARD A PROFILE OF LONE WOLF TERRORISTS: WHAT MOVES AN INDIVIDUAL FROM RADICAL OPINION TO RADICAL ACTION. TERRORISM AND POLITICAL VIOLENCE, 26(1), 69-85.

MILLER, E., & JENSEN, M. (2018). FACT SHEET: AMERICAN DEATHS IN TERRORIST ATTACKS, 1995 - 2017. START.

MILLER, E., LaFREE, G. AND DUGAN, L., 2018. GLOBAL TERRORISM DATABASE (GTD. [ONLINE] NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM UNIVERSITY OF MARYLAND.

MILLO, L. (2018, MARCH 14). TERRORISM IN CONTEXT: THE STIGMATIZATION OF ISLAM IN FRANCE. BERKELEY POLITICAL REVIEW.

Mishra, P. (2016, October 17). The globalization of rage: Why today's extremism looks familiar. Foreign Affairs.

Monaci, S., 2017. Explaining the Islamic state's online media strategy: a transmedia approach. International Journal of Communication, 11(2017), pp.2842–2860.

Osama Bin Laden's last interview. (2017).

Pisoui, D., & Ahmed, R. (2016). Radicalisation research – Gap analysis. The European Commission.

Poli, R., Healy, M. and Kameas, A., 2010. Theory and applications of ontology. Dordrecht: Springer.

RAND Corporation., 2019. RAND Database of worldwide terrorism incidents. [Online]

Research on domestic radicalization and terrorism. (2018). The National Institute of Justice.

Richardson, C. (2011). Relative deprivation theory in terrorism: A study of higher education and unemployment as predictors of terrorism (Senior Honors Thesis). New York University.

Salinas, S. (2018, October 8). A Google bug exposed the information of up to 500,000 users. CNBC.

Shefet, D. (2016). Policy options and regulatory mechanisms for managing radicalization on the internet.

Smith, A. G. (2018). How radicalization to terrorism occurs in the United States: What research sponsored by the National Institute of Justice tells us. National Institute of Justice.

Snyder, A. (2016, October 11). Why terrorists do—and don't—take credit for attacks. The National Interest.

Soiferman, L., 2010. Compare and contrast inductive and deductive research approaches. [Online] University of Manitoba.

Speckhard, A., Shajkovci, A., & Yayla, A. S. (2018). Defected from ISIS or simply returned, and for how long? – Challenges for the West in dealing with returning foreign fighters. Homeland Security Affairs, 14(1).

SWANSON, A., 2015. EXPLORATORY RESEARCH. [ONLINE] ASHFORD UNIVERSITY.

TAYLOR, P. J., HOLBROOK, D., AND JOINSON, A., 2017. A SAME KIND OF DIFFERENT: AFFORDANCES, TERRORISM AND THE INTERNET. CRIMINOLOGY AND PUBLIC POLICY, 16(1), PP.127-133.

TERRORISM. (N.D.). FEDERAL BUREAU OF INVESTIGATIONS THAYER, B. A., & HUDSON, V. M. (2010). SEX AND THE SHAHEED: INSIGHTS FROM THE LIFE SCIENCES ON ISLAMIC SUICIDE TERRORISM. INTERNATIONAL SECURITY, 34(4), 37-62. DOI: 10.1162/ISEC.2010.34.4.37

THE INDEPENDENT. (2019). *FEMALE BRITISH ISIS RECRUITER ASKS TO RETURN TO UK SAYING 'WE JUST WANT A NORMAL LIFE'.*

TINNES, J. (ED.)., 2018. BIBLIOGRAPHY: TERRORIST TACTICS AND STRATEGIES. PERSPECTIVES ON TERRORISM, 12(5), PP.78-120.

TOROK, R. (2015). TERRORISTS USE MARKETING SKILLS TO ATTRACT NEW RECRUITS ONLINE.

U.S. DEPARTMENT OF STATE., 2007. TERRORIST MOTIVATIONS AND BEHAVIORS.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. (2012). THE USE OF THE INTERNET FOR TERRORIST PURPOSES. NEW YORK, NY.

UNIVERSITY OF HONG KONG; DEPARTMENT OF INFORMATION SYSTEMS., 2019. RESEARCH METHODOLOGY.

UNIVERSITY OF MINNESOTA, 2019. DATA COLLECTION TECHNIQUES | CYFAR.

UNODC, 2012. THE USE OF THE INTERNET FOR TERRORIST PURPOSES.

VAN TEIJLINGEN, E. AND HUNDLEY, V., 2002. THE IMPORTANCE OF PILOT STUDIES. NURSING STANDARD, 16(40), PP.33-36.

VERGANI, M. AND BLIUC, A. M., 2018. THE LANGUAGE OF NEW TERRORISM: DIFFERENCES IN PSYCHOLOGICAL DIMENSIONS OF COMMUNICATION IN DABIQ AND INSPIRE. JOURNAL OF LANGUAGE AND SOCIAL PSYCHOLOGY, 37(5), PP.523-540.

VON BEHR, I., REDING, A., EDWARDS, C., & GRIBBON, L. (N.D.). RADICALIZATION IN THE DIGITAL ERA. RAND CORPORATION

WEIMANN, G. (2014). NEW TERRORISM AND NEW MEDIA. WASHINGTON, DC. WILSON CENTER

WHITESIDE, M., MILLS, J. AND MCCALMAN, J., 2012. USING SECONDARY DATA FOR GROUNDED THEORY ANALYSIS. AUSTRALIAN SOCIAL WORK, 65(4), PP.504-516.

WILSON, L., 2017. UNDERSTANDING THE APPEAL OF ISIS. NEW ENGLAND JOURNAL OF PUBLIC POLICY, 29(1).

ZEHORAI, I. (2018, JANUARY 24). THE RICHEST TERROR ORGANIZATIONS IN THE WORLD. FORBES.