2022

# Developing Industry Policies to Mitigate Terrorists' Misuse of Social Media Platforms

steve stalinsky
*Walden University*

# Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Steven P. Stalinsky

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gregory Campbell, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Thela Thatch, Committee Member,
Public Policy and Administration Faculty

Dr. Michael Brewer, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Developing Industry Policies to Mitigate Terrorists' Misuse of Social Media Platforms

by

Steven P. Stalinsky

MA, Antioch University, 2003

BS, University of Pittsburgh, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2022

Abstract

Radical Islamic militant groups, particularly Al-Qaeda and the Islamic State (ISIS), have utilized social media platforms for networking, recruitment, fundraising, information gathering, training, and planning attacks. The problem was that social media platforms, particularly Facebook, Telegram, Twitter, and YouTube, were not equipped with industry policies to provide a standardized response to terrorist misuse of social media and encryption platforms. The present study was needed because the lack of a unified response system has increased corporate liability, threatened national security, and enabled terrorist growth globally. The purpose of this study was to develop industry policies based on existing corporate policies so that platforms can implement standardized responses to terrorist misuse. This study was developed within the framework of social movement theory (SMT). Two research questions addressed ways in which social media companies responded to the misuse of their platforms by terrorist groups, whether industry policies could be produced from existing platform responses to form standardized policies to the misuse of social media by terrorists. A qualitative multiple case design was used to collect, code, and analyze open-source data using NVivo. Six themes that emerged were government collaboration, new regulation, greater platform responsibility, content removal, consequences, and policy changes. Recommendations included building policies on the strengths of existing platform policies and on the groundwork of peer-reviewed literature and NGOs. Resulting policies could facilitate positive social change by providing a blueprint for newer platforms, contributing to government efforts, and disrupting terrorist misuse.

# Developing Industry Policies to Mitigate Terrorists' Misuse of Social Media Platforms

by

Steven P. Stalinsky

MA, Antioch University, 2003

BS, University of Pittsburgh, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2022

# Dedication

This document is dedicated to those who have been in the fight against terrorism, including those who have given their lives and those who work tirelessly daily without any recognition of their efforts.

Acknowledgments

I would like to thank my family for all of their support and daily inspiration.

Table of Contents

List of Tables ..... v

List of Figures ..... vii

Chapter 1: Introduction to the Study ..... 1

Background ..... 3

Problem Statement ..... 5

Purpose of the Study ..... 8

Research Questions ..... 9

Conceptual Framework ..... 9

Nature of the Study ..... 9

Definitions ..... 10

Assumptions ..... 13

Scope and Delimitations ..... 13

Limitations ..... 14

Significance ..... 15

Summary ..... 16

Chapter 2: Literature Review ..... 18

Literature Search Strategy ..... 19

Conceptual Framework ..... 20

Literature Review ..... 22

Emergence of Cyber Terrorism in the United States ..... 22

Research of Cyber Terrorism ..... 23

Social Media and Cyber Terrorism ..... 24
Rationale for the Selection of the Variables/Concepts ..... 25
Known Concepts and/or Phenomena ..... 25
Controversial Concepts and/or Phenomena ..... 27
Meaningful Approach for the Current Study ..... 33
Summary and Conclusions ..... 34
Chapter 3: Research Method ..... 36
Research Design and Rationale ..... 36
Role of the Researcher ..... 38
Methodology ..... 39
Participant Selection Logic ..... 39
Instrumentation ..... 41
Procedures for Recruitment, Participation, and Data Collection ..... 43
Data Analysis Plan ..... 44
Issues of Trustworthiness ..... 46
Ethical Procedures ..... 47
Summary ..... 49
Chapter 4: Results ..... 50
Setting ..... 50
Demographics ..... 50
Data Collection ..... 52
Open-Source Data Sources ..... 52

Organizational Software Tool ..... 53
Variations in Data Collection ..... 53
Data Analysis ..... 53
Development of Themes and Subthemes ..... 54
Evidence of Trustworthiness ..... 55
Results ..... 56
Case Study 1: Terrorist Attacks in the United Kingdom by ISIS in 2017 ..... 57
Case Study 2: Terrorist Attacks in France by ISIS in 2017 and 2018 ..... 59
Case Study 3: Terrorist Attack in the United States by ISIS in 2017 ..... 61
Case Study 4: Terrorist Attack in New Zealand by a White Supremacist in 2019 ..... 62
Statements and Terms of Conditions by Platforms in Response to the Multiple Cases ..... 66
Emerging Themes and Subthemes ..... 77
Development of Industry Policies from Emerging Themes ..... 85
Emerging Theme 1: Government Collaboration with Online Platforms ..... 85
Emerging Theme 2: "New Era" of Regulation ..... 88
Emerging Theme 3: Responsibility Lies on the Shoulders of Online Platforms ..... 88
Emerging Theme 4: Online Platforms' Ability to Remove Content ..... 89
Emerging Theme 5: Imposing Consequences on Online Platforms ..... 90

Emerging Theme 6: Social Media Platforms Respond With Policy Changes ..... 91
Summary ..... 93
Chapter 5: Discussion, Conclusions, and Recommendations ..... 94
Interpretation of the Findings ..... 95
Findings Confirming Peer-Reviewed Literature ..... 95
Findings Disconfirming Peer-Reviewed Literature ..... 96
Findings Extending the Knowledge of Peer-Reviewed Literature ..... 98
Limitations of the Study ..... 99
Recommendations ..... 100
Implications ..... 102
Conclusion ..... 104
References ..... 108

List of Tables

**Table 1** *Demographics and Characteristics of the Participant Group* ..... 51

**Table 2** *Statements by Government Leaders and Other Institutions Concerning Online Platforms in Reaction to Terrorist Attacks in the United Kingdom by ISIS in 2017* 58

**Table 3** *Statements by Social Media Platforms After Terrorist Attacks in the United Kingdom by ISIS in 2017* ..... 59

**Table 4** *Statements by International Government Leaders Concerning Online Platforms in Reaction to Terrorist Attacks in France in 2017 and 2018* ..... 60

**Table 5** *Statements by Social Media Platforms After Terrorist Attacks in France by ISIS in 2017 and 2018* ..... 61

**Table 6** *Statements by Social Media Platforms and the Government in Reaction to a Terrorist Attack in the United States by ISIS in 2017* ..... 61

**Table 7** *Statements by Government Leaders Concerning Online Platforms in Reaction to a Terrorist Attack in New Zealand by a White Supremacist in 2019* ..... 63

**Table 8** *Statements by Social Media Platforms After a Terrorist Attack in New Zealand by a White Supremacist in 2019* ..... 65

**Table 9** *Statements by Social Media Platform Officials in Response to Terrorist Misuse of Social Media Platforms* ..... 67

**Table 10** *Terms of Service Regarding Terrorist and Criminal Content for Each Platform, From Its Beginning to the Present* ..... 70

**Table 11** *Themes of Statements by Governments Concerning Online Platforms in Reaction to a Terrorist Attack on Christchurch, New Zealand* ..... 78

**Table 12** *Themes of Corporate Statements by Online Platforms After a Terrorist Attack on Christchurch, New Zealand* ..... 80

List of Figures

**Figure 1** *Word Cloud Using NVivo of the Most Frequent Terms in the Data Set* ..... 81

**Figure 2** *Coding Hierarchy Using NVivo Based on Complete Themes* ..... 83

**Figure 3** *Coding Hierarchy Using NVivo of Themes Based on Subthemes* ..... 85

# Chapter 1: Introduction to the Study

In 1999, 2 years after the first recognizable social media site was created, social media became a cultural sensation. User-generated content was shared through mechanisms and platforms in a fundamentally collaborative way, ushering in a new era of open communication for the world (A. M. Kaplan & Haenlein, 2010). By 2006, social media platforms YouTube, Facebook, and Twitter became popular (A. M. Kaplan & Haenlein, 2010), followed by Telegram in 2013. Social media was praised for its facilitation of global connectivity, social awareness, promotional capabilities, community building, and education.

However, there were unintended consequences of social media, notably the empowerment of two radical Islamic terrorist groups, Al-Qaeda and Islamic State (ISIS). As social media advanced, so did the development of Al-Qaeda and ISIS (Cohen-Almagor, 2013). These terrorist groups utilized social media platforms as an integral function of their political, religious, and ideological purposes (Cohen-Almagor, 2013), focusing their propaganda efforts on recruitment, training, planning, and fundraising (Mullins, 2015; Theohary & Rollins, 2011; Weimann, 2004). For example, an influential recruitment strategy was terrorists' exploitation of "friend of a friend" relationships on social media to build networks and make new connections (Waskiewicz, 2012).

Consequently, a generation of youths was radicalized in part by the utilization of social media by Al-Qaeda and ISIS, resulting in violence against the West (Stalinsky & Sosnow, 2014). Twelve percent of foreign ISIS members were identified as minors under 18 years old (Cook & Vale, 2019), and their various roles within terrorist organizations

included messengers, frontline fighters, spies, and suicide bombers (United Nations, 2017). Radical Islamic terrorist groups would continue to thrive online and successfully execute attacks if their access to social media remained free and easy. With the exception of North Korea, social media was accessible throughout much of the world, including in the West and throughout the Middle East.

Although there was some action and debate regarding the role and responsibilities of social media platforms in curbing terrorists' access, the lack of clarity and a unified front across the industry resulted in little impact on the misuse of social media platforms by Al-Qaeda and ISIS. The consequences of ineffective industry policies included the increasing radicalization of youths, the further development of terrorist groups, and the exposure of social media companies to financial liability in the wake of terrorist attacks (Conway, 2007; Rogan, 2006; Weimann, 2006). In the current study, I compared and built on existing social media company policies and sought to develop industry policies for standardized responses to terrorists' utilization of social media platforms, which had national and international implications. The positive social change implications included detecting and disrupting the use of the internet by terrorist groups, providing a blueprint for the responses of newer platforms, and contributing to government efforts to stop terrorism. Study findings could be used to reduce or stop the radicalization of youths who perform terrorist attacks.

This chapter includes the background of social media platforms in relation to the development of Al-Qaeda and ISIS and provides evidence of the need for a standardized industry response to the utilization of social media platforms by terrorist groups. The

purpose of the study was developed within a conceptual framework and presented in two research questions. The chapter concludes with a clarifying set of definitions, assumptions, scope, limitations, and significance.

## Background

The 20th anniversary of the World Wide Web in August 2011 received significant media attention, including reports warning that the internet could yield to darker trends. Literature supported the fact that terrorist groups were misusing the internet, including social media platforms, for the widescale spread of jihadist ideology (Conway, 2007; Rogan, 2006; Weimann, 2006). Most notable among the literature was support from the letters and statements of the leaders of radical Islamic terrorist groups such as Al-Qaeda and ISIS (MEMRI Cyber & Jihad Lab, 2011).

The misuse of social media platforms by Al-Qaeda and ISIS was also evident in online literature across accredited jihadi websites and, increasingly, social media platforms in the form of online magazines, inspirational social media posts, and encrypted messaging, all of which were designed to target young people. Left unchecked, such social media misuse was manifested in terrorist attacks like that in San Bernardino, California, in 2015 (Collins, 2017). In the San Bernardino attack, more than 36 people were killed or seriously injured in a mass shooting and an attempted bombing at the Inland Regional Center (Collins, 2017). An investigation determined that the attacker had advocated violent jihad in encrypted social media messages that were obscured from U.S. immigration officials by the use of a pseudonym and privacy settings (Perez & Ford, 2015).

Consequently, social media platforms were receiving unprecedented attention and pressure from governments to mitigate terrorist activity online, including a movement to increase their financial liability to terrorist attacks. For example, in *Crosby, et al. v. Twitter, Google, and Facebook*, family members of the victims of the infamous shooting at a nightclub in Orlando, Florida filed a federal civil complaint against Twitter, Facebook, and Google for providing material support to ISIS, including supplying social media accounts, combining ISIS posts with targeting advertising, and sharing profit from advertising revenue (Crosby et al., 2016). In 2017, the wife of a victim of a suicide bombing in Brussels, Belgium, sued Twitter for aiding and abetting ISIS (Whitehouse, 2017), and later that year, three family members of the San Bernardino attack sued Facebook, Google, and Twitter for allowing terrorist activity to take place on their platforms (Collins, 2017). Senator John McCain (R-Ariz.) said the status quo in the handling of social media misuse was "unacceptable," promising that "in the Senate Armed Services, we're going to have hearings on it, and we're going to have legislation" (Bennet & Williams, 2015, para. 6). However, the brief period of progress after each attack was typically followed by waning interest, so the tension among social media companies remained.

In an effort to respond to the pressure, social media platforms (Facebook, Twitter, and YouTube) established the Global Internet Forum to Counter Terrorism (GIFCT) in 2017 (Twitter Public Policy, 2017). The initiative intended to deter terrorist activity on their online platforms by increasing collaboration between social media platforms and governments, academia, and international organizations, thereby preventing the online

spread of radical ideology (Twitter Public Policy, 2017). However, critics of GIFCT pointed out that insufficient resources allowed terrorists to find new ways to circumvent rules (Levin, 2017). Despite attempts by social media companies to mitigate tensions with efforts like GIFCT, governments were losing patience with the inability of the industry to stay one step ahead rather than one step behind extremists (Levin, 2017).

There was evidence of the misuse of social media and some collaboration to share best practices. However, there was little literature on the actions that can be taken by social media platforms to stop the misuse (Conway, 2007; MEMRI Cyber & Jihad Lab, 2011; Rogan, 2006; Twitter Public Policy, 2017; Weimann, 2006). The current study was necessary to bridge the gap between the knowledge of the misuse of social media and the industry efforts that could implement real change.

## Problem Statement

Social media platforms, particularly Facebook, Telegram, Twitter, and YouTube, were not equipped with industry policies to provide a standardized response to the misuse of their social media and encryption platforms by terrorists. Progress generally followed a terrorist attack, as displayed in the aftermath of the 2015 terrorist attack in San Bernardino, California, when Facebook agreed to set up a special unit to find and block online propaganda by ISIS (Collins, 2017). Also, initiatives like GIFCT showed the willingness of YouTube, Facebook, and Twitter to increase cooperation and preventative measures.

However, the individual efforts of social media companies failed to sufficiently address terrorists' interest in their platforms. The failure was evident in the aftermath of

each attack. Following a brief period of progress, interest typically waned between attacks due to insufficient resources, the constant evolution of terrorists' online tactics, and a fundamental failure of social media platforms to grasp their critical role in mitigating the development of terrorist groups (Buran, 2011; Matthews, 2015). In the absence of industry policies, social media platforms responded to the misuse of social media with mixed reactions and inconsistent efforts (Buran, 2011; Matthews, 2015). The lack of a standardized response by social media platforms allowed the continued development of terrorist groups, threatened national security, and left those involved in fighting the war on terror two steps behind where they needed to be in challenging cyber jihad (Buran, 2011; Matthews, 2015).

The misuse of social media platforms by terrorists was part of the national security conversation for more than a decade. During the 2016 presidential election campaign, then-candidate Donald Trump addressed the online activities of terrorist groups several times, promising to work aggressively to disrupt their propaganda and recruiting (Washington Post, 2015).

The persistent problem of social media misuse by terrorist groups was prompting a more urgent conversation. In 2017, Nikki Floris, deputy assistant director for counterterrorism at the FBI, detailed the online activities of terrorists before the Committee on Homeland Security and Governmental Affairs (Adapting to defend the homeland against the evolving international terrorist threat, 2017). Floris said "their widespread use of technology propagates the persistent terrorist message to attack U.S. interests here and abroad . . . ISIS uses high-quality traditional media platforms as well as

widespread social media campaigns to propagate its extremist ideology" (Adapting to defend the homeland against the evolving international terrorist threat, 2017, p. 8). Many lawmakers, including Senator Ron Johnson (R-Wis.), joined Floris in raising alarm over the success of terrorist groups like ISIS in leveraging digital platforms to recruit and spread their propaganda. As the chair of the Senate Homeland Security and Governmental Affairs Committee, Johnson said during remarks at a 2017 hearing on evolving terror threats, "It is good that we by and large have taken away the physical caliphate. [But] we have in no way, shape or form denied them the cyber caliphate. That may be a more persistent, long-term threat" (Chalfant, 2017, para. 2-3).

The growing cyber threat led scholars and think tanks to study the use of social media by terrorists (Cohen-Almagor, 2013; Klausen, 2014; Vidino & Hughes, 2015; Weimann, 2014). In 2017, an American nonprofit global policy think tank, RAND Corporation, issued a report that discussed the social media strategy of ISIS (Jones et al., 2017). The report explained that social media provided a way for ISIS to communicate with current and future followers, inspiring them to carry out attacks and information operations, send money, and travel to ISIS territory (Jones et al., 2017).

Additionally, according to the RAND Corporation report, social media provided a steady flow of foreign fighters and the ability to develop networks of radicalized individuals to carry out attacks (Jones et al., 2017). However, the studies did not provide sufficient examinations of technical methods to stop the use of social media by terrorist groups. The 2017 RAND report provided only brief recommendations, including working with companies to develop flagging mechanisms, challenging terrorists online using

words for counter-messaging, and pressuring social media platforms to tighten restrictions on accounts linked to terrorist groups (Jones et al., 2017).

Although there was evidence of the misuse of social media and a growing body of literature on the actions that can be taken by social media platforms, the existing literature did not adequately address the problem of misuse (Stalinsky & Sosnow, 2014). The heavier pressure on social media platforms was not accompanied by sufficient guidance on addressing terrorists' misuse of their services, which left a gap between global expectations and industry action (Travis, 2017). At a 2017 UN Summit, British Home Secretary Amber Rudd addressed the gap in the law regarding social media: "This is an increasingly common means by which material is accessed online for criminal purposes and is a particularly prevalent means of viewing extremist material such as videos and web pages" (Travis, 2017, para. 5).

## Purpose of the Study

The purpose of this qualitative multiple case study was to develop industry policies based on existing corporate policies so that social media platforms can implement effective, standardized responses to the problem of the misuse of their services by terrorists. Using a multiple case design, this qualitative study sought to gather data on the existing responses to misuse by multiple social media companies. The study compared the existing policies of individual social media platforms, building on commonalities and precedents and confirming the applicability and transferability of responses to develop industry policies that combat the misuse of social media and

encryption services, build a blueprint for the industry that can be applied to smaller or future companies, and hinder the social development of terrorist groups.

## Research Questions

The following research questions (RQs) were addressed in this study:

RQ1: In what ways were social media companies responding to the misuse of their platforms by terrorist groups?

RQ2: Could industry policies be produced from existing platform responses to form standardized policies to the misuse of social media by terrorists?

## Conceptual Framework

This study was developed within the framework of social movement theory (SMT). SMT is based on the fundamental idea that individuals form networks. SMT involves the causes, forms, and consequences of the social mobilization of previously uninvolved individuals, providing the basis for understanding the motivation and method by which an individual enters and participates in a movement (Borum, 2011). SMT has proven to be one of the most complete frameworks used by researchers in examining terrorism, including the process of radicalization and violent extremism (Metzger, 2014). The relationship between the SMT framework and the policies of social media platforms are explained in more detail in Chapter 2.

## Nature of the Study

This study was a qualitative multiple case study. I sought to understand and inform the decision-making processes of social media platforms to mitigate the online culture of terrorist groups that depend on social media platforms for global growth (see

Pacheco-Vega, 2020). I applied a systematic review of the terms of service, policies, and precedents of social media platforms. The review addressed approaches by the world's leading standards developing organizations (SDOs) as well as organizational software for classifying and arranging content. The aim was to develop industry policies based on insights and commonalities to equip social media platforms with standardized industry responses, thereby hindering the growth of terrorist groups.

## Definitions

*Counternarrative*: Targeted campaigns to discredit the ideologies and actions of violent extremists (Tuck & Silverman, 2016).

*Cyber security*: Measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access (Department of Defense, 2019).

*Cyberspace*: A time-dependent set of interconnected information systems and the human users who interact with these systems (NATO Cooperative Cyber Defense Centre of Excellence, n.d.).

*Dark web*: Internet space that contains content intentionally concealed, which may be accessed for legitimate purposes and to conceal criminal or otherwise malicious activities (Finklea, 2017).

*Encrypt*: Convert data into a form that cannot be easily understood by unauthorized people (National Institute for Cybersecurity Careers and Studies, n.d.).

*Encryption*: A method of converting an original message of regular text into encoded text by means of an algorithm (U.S. Department of Health & Human Services, 2014).

*Hack*: The practice of modifying or altering computer software and hardware to accomplish a goal that was considered to be outside of the creator's original objective (LAWS, n.d.).

*Hacking:* Unauthorized intrusion into a computer or a network (Techopedia, n.d.).

*Industry standard*: The average by which those in a particular field govern themselves; the ordinary manner of doing things in that field that can serve to establish different things in various legal settings (HG.org Legal Resources, n.d.).

*Internet of Things*: A connection of physical objects to the internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing (Federal Trade Commission, 2015).

*Internet provider (IP)*: An entity that provides any internet communication service, including connectivity to subscribers *(*Duhaime, n.d.).

*Jihad*: An Arabic word derived from a verb that means to struggle, strive, or exert oneself. Violent extremists understand the concept of jihad as a religious call to arms (Theohary & Rollins, 2011).

*Jihadi:* Radicalized individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph (Bjeloper, 2013).

*Phishing*: A virtual trap set by cyber thieves that uses official-looking emails to lure victims to fake websites and trick them into revealing personal information (Federal Bureau of Investigation, 2009).

*Propaganda*: Spreading of ideas, information, or rumor for the purpose of helping or injuring an institution, a cause, or a person (Merriam-Webster, n.d.).

*Self-radicalization*: A phenomenon in which individuals become terrorists without joining an established radical group, although they may be influenced by its ideology and message (Citizendium, n.d.).

*Social media*: A type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes email, online social forums, blogs, video and image-sharing websites and similar facilities (Lamar University, n.d.).

*Terms of service*: Rules a person or organization must observe in order to use a service (PC Magazine, n.d.).

*Terrorism*: The unlawful use of violence or threat of unlawful violence to instill fear and coerce governments or societies (Joint Chiefs of Staff, 2014).

*Theory*: An idea or set of ideas that was intended to explain something about life or the world, especially an idea not proved to be true; general principles and ideas about a subject (Longman Dictionary of Contemporary English, 2003).

*Virus*: A computer program that spreads by infecting files or the system areas of a computer or network router's hard drive and then making copies of itself (Nieles, et al., 2017).

## Assumptions

The study was based on four primary assumptions. The first assumption was that terrorists' misuse of the internet was a national security problem, which was relevant to the study because the findings may impact the welfare of governments, civilians, and the industry. The second assumption was that much of today's terrorist activities involve the misuse of social media, which underscores the critical role of social media platforms in mitigating online activity. The third assumption was that leading social media platforms have made initial efforts to observe and address the misuse of their services by terrorists, which would be necessary for the comparative policy analysis intended in this study. The final assumption was that the chosen methodology was the best possible tool for solving the research problems.

## Scope and Delimitations

The topic of terrorism was broad and complex. For a manageable scope, the study was limited to the platform policies and industry standards of social media platforms in response to the misuse of their services by terrorist groups. For maximum impact within time constraints, the sample of social media platforms was limited to the four leading social media platforms: Facebook, Telegram, Twitter, and YouTube. The sample of terrorist groups whose activities were targeted were limited to the two largest groups: Al-Qaeda and ISIS.

Two aspects of the original scope of the project were not investigated. First, Google was included in the list of social media platforms until it was determined that YouTube was a subsidiary of Google. To avoid redundancy and to maximize impact, the

list was refined to exclude Google. Second, the original plan to approach the study using mixed methods was changed after strong discouragement from some professors and students because of the additional work and studies it would incur.

The potential transferability of this study's findings was high. The approach and resulting industry policies could serve as a blueprint for newer platforms. The policies could impact their ability to detect and disrupt terrorists' use of social media.

## Limitations

There were several limitations to this study related to the participants, methodology, and design. First, the level of use of social media and encryption services by terrorists varied among the platforms. The platforms that were utilized more by terrorists carried a greater ability to contribute data to this study than those used less extensively. Second, social media platforms varied in their willingness to carry the burden of mitigating misuse of their services; some platforms were guiltier than others for previous inaction or apathy. An insincere approach to the removal of content impacted the availability and dependability of resources and, ultimately, the success of the study.

Third, social media platforms are in an inherently fast-paced industry. As new technologies are launched and older technologies lose popularity, the continual change impacts a platform's ability and resources to proactively track and/or respond to the misuse of their services. The fast pace of the industry also constrained the timeframe of this study. This study was designed to focus on the misuses of social media and the existing policies that were formed in response to those misuses at a certain point in time.

Finally, the transferability of the study was limited to the willingness of existing platforms and new platforms to heed recommended standards.

Some of these limitations were by design; for example, the study was designed to be limited to that of the existing policies and responses of social media platforms for optimal transferability. Additionally, the reliance on social media platforms to develop industry policies remained the most direct approach for the purpose of this study. In addressing these limitations, I began by acknowledging the potential limitations of the participant group—the varying levels of utilization of services by terrorists, the willingness to take action by social media platforms, and the limited resources in tracking and reacting to terrorist activity—and provided assurance that a commitment to the study could result in alleviating all limitations. The burden of mitigation could be shared among platforms, collective action could spur greater involvement and collaboration, and the development of industry standards could assist in proactive responses in a fast-changing industry.

## Significance

The impacts of this study could have a ripple effect throughout society, including the technology industry, the business sector, governments, terrorist groups, and civilians. Within the technology industry, the potential clarity provided by the study could help social media platforms overcome limitations and advance their ability to proactively respond to the misuse of services by terrorist groups. Standardized responses could reduce the propaganda by terrorist groups, protecting the intent of social media platforms and fortifying the industry against financial liability. A standardized approach could also

serve as a model for the policy development of new platforms as well as that of the entire business community regarding terrorist activity.

These findings could also strengthen the collaboration between the technology industry and the U.S. government. The observations, data, and policies from social media platforms on terrorist use of social media and encryption technology could contribute to the efforts of the Department of Homeland Security in examining the threat to national security. Additionally, new research and literature could be transferred for use by other governments.

Most significantly, equipping social media platforms with standardized policies has the potential to help these companies detect and disrupt terrorists' propaganda efforts, which holds implications for positive social change. When terrorist groups no longer utilize social media platforms for their purposes, civilians are less exposed to terrorists' politics, religion, and ideology and are less susceptible to becoming radicalized. Broadly speaking, any reduction in online terrorist activity could mean suffering fewer terrorist attacks, protecting the welfare of youths and creating a safer world.

## Summary

Since the advent of social media in 2006, the misuse of social media platforms by terrorist groups posed a growing threat to national security (A. M. Kaplan & Haenlein, 2010). Terrorist groups such as Al-Qaeda and ISIS thrived online, empowered by the virtual capability to recruit, train, plan, and fundraise. The lack of an effective response by social media platforms was a fundamental problem that allowed continued misuse of their services, resulting in a growing liability for the technology industry, greater

likelihood of youths who became radicalized, and greater susceptibility of the United States to terrorist attacks.

Chapter 1 introduced the study in response to this problem, the purpose of which was to craft industry policies for a standardized response by social media platforms regarding the misuse of their services by terrorist groups. This chapter provided an overview of the study, which was grounded in two research questions within a conceptual framework to compare the observations and existing policies of four social media platforms (Facebook, Telegram, Twitter, and YouTube). The industry standards developed by building on commonalities, using organizational tools, and applying a process by SDOs could help bridge the gap in research literature and technical action related to terrorists' misuse of platforms. Chapter 2 includes a review of the literature in more depth. I also provide the databases, tools, and iterative process used in the search strategy as well as the conceptual framework for the study. Chapter 3 provides an overview of research methods used in this study, while Chapter 4 reports results. Finally, Chapter 5 lends a discussion, my conclusions, and recommendations for further research.

# Chapter 2: Literature Review

Industry policies addressing terrorists' utilization of social media platforms is inadequate. This problem spawned the development of terrorist groups, the radicalization of youths, and terrorist attacks on civilians. The purpose of this study was to equip social media platforms with standardized industry policies that help them mitigate the growing misuse of their services by terrorist groups.

Letters and statements by Al-Qaeda leaders Osama bin Laden and Ayman Al-Zawahiri provide evidence of this problem (MEMRI Cyber & Jihad Lab, 2011). Media misuse was also apparent in terrorist groups' online literature across accredited jihadi websites and, increasingly, social media platforms in the form of online magazines, inspirational social media posts, and encrypted messaging. Additionally, Western government officials acknowledged the problem in panel remarks, speeches, interviews, and media statements, including those of Presidents Barack Obama and Donald Trump (The White House: President Barack Obama, 2015; Washington Post, 2015), Senators John McCain and Ron Johnson (Bennet & Williams, 2015; Chalfant, 2017), Federal Bureau of Investigation officials James Comey and Nikki Floris (Adapting to defend the homeland against the evolving international terrorist threat, 2017; Sperry, 2015), and British government officials Teresa May and Amber Rudd (Perez, 2017; Travis, 2017). Studies and reports by scholars and think tanks examined and confirmed the use of social media by terrorists, including a 2017 report by the RAND Corporation that detailed the social media strategies of ISIS (Jones et al., 2017). This chapter includes the strategy for

the literature search, the conceptual framework, the literature review in relation to key variables and concepts, and concluding statements.

## Literature Search Strategy

The literature for this study was collected by conducting a comprehensive search of databases in the Walden University Library, the Middle East Media Research Institute's Jihad and Terrorism Threat Monitor project database, and the Google Scholar search engine. Using the directory search engine of the Walden University Library, I focused on terrorist groups, social media, and industry standards. Within each focus area, searches were conducted using key search terms among articles, dissertations, and journals. The iterative process was applied to a comprehensive search of the database of the Middle East Media Research Institute's Jihad and Terrorism Threat Monitor project, which provided content from terrorist social media postings and their literature. Google Scholar's search engine and the websites of the social media platforms were also useful in collecting research from news articles and websites of technology platforms and published interviews with senior leadership of the leading technology platforms as well as statements and testimony on Capitol Hill.

Key search terms that were involved in all resources included *cyber jihad*, *terrorist use of social media*, *terrorism in the U.S.*, *jihadist groups*, *terrorism research*, *terrorist threat analysis*, *developing industry standards*, and *encryption news*. Combinations of key search terms included variations of the names of each of the four most relevant social media platforms in conjunction with each of the names of the two primary terrorist groups (e.g., ISIS Facebook). More combinations included variations of

the names of the social media platforms and/or terrorist groups with each of the key search terms (e.g., ISIS cyber jihad). I aimed to limit research to the last 5 years; however, sufficient sources were not available within this time frame, so older sources were referenced, particularly those that established historical perspectives or foundational aspects of the study.

## Conceptual Framework

The conceptual framework for this study was social movement theory (SMT). SMT evolved from the theories of French psychologist Gustave Le Bon, the founder of collective action studies (Klandermans & Stekelenburg, 2009). Based on observations of social unrest and street protests in France during the 1890s, Le Bon characterized the movement of thought transformation as spontaneous and irrational (Klandermans & Stekelenburg, 2009). However, Le Bon's early theories were rejected in light of the enormous growth of articulate and calculated social movements in the 1960s involving civil rights, women, and the environment, after which new approaches were developed in the 1970s (Klandermans & Stekelenburg, 2009). By the 1990s, the concept of social movements became intertwined with the information society, globalization, communication technologies, and networks (Klandermans & Stekelenburg, 2009).

SMT is based on the fundamental idea that individuals form networks. SMT involved the causes, forms, and consequences of the social mobilization of previously uninvolved individuals, providing the basis for understanding the motivation and method by which an individual enters and participates in a movement (Borum, 2011). SMT has proven to be one of the most complete frameworks used by researchers in examining

terrorism, including the process of radicalization and violent extremism (Metzger, 2014). The framework is divided into four trends—mass behavior, resource mobilization theory, political opportunity processes, and new social movements—which allowed for analysis at the individual, national, and international levels. Moreover, SMT takes into account rational choice, organizational culture, and political communication (Samarov, 2008).

A previous study within the SMT framework of the development of a Western pro-jihad group revealed a four-component model for radicalization that related to the current study (see Wiktorowicz, 2002). The first three components included (a) cognitive opening, which describes an individual's inherent openness to new worldviews; (b) religious seeking, which describes an individual's determination that religion was a path to meaning; and (c) frame alignment, which describes an individual's understanding of a group's narrative and ethos as "making sense" (Wiktorowicz, 2002). The fourth component, socialization, was particularly relevant to the current study (see Wiktorowicz, 2002). Socialization is the process by which an individual becomes fully indoctrinated into a movement (West, 2016). Some scholars concluded that, although social media did not necessarily radicalize people, they could complement an established belief system through continued propaganda (West, 2016).

The current study was rooted in the SMT idea that the development and movement of terrorist groups follow a life cycle that can be impacted by social media platforms. The detection and disruption of online propaganda that would be possible through industry policies could hinder the development of terrorist groups. SMT confirmed the critical role of social media platforms in mitigating the development of

terrorist groups and the importance of crafting industry policies for standardized responses to misuse of services. The research questions were designed based on the theory that technical industry action can interrupt the life cycle of the development of terrorist groups.

## Literature Review

### Emergence of Cyber Terrorism in the United States

Scholars studied terrorists' use of the internet since the 1990s. Denning (1999), one of the first scholars to address terrorists' use of the internet, stated in 1998 that 12 of the 30 groups on the U.S. State Department's list of terrorist organizations had a web presence. Just 1 year later, virtually every terrorist group was online (Denning, 1999). Within 7 years, there were more than 4,300 websites serving terrorists and their supporters (Weimann, 2006), while others estimated the number to be over 5,000 (Fielding, 2008). The watershed year of 2001 was when cyber jihad emerged as an important weapon in the arsenal of terrorist groups such as Al-Qaeda (Stalinsky & Sosnow, 2014).

The forums that set the stage for cyber jihad contained statements from different groups and leadership, news and media related to jihadi fronts, and sections related to preparations, planning, and instructions for terrorist operations, including guidelines for "lone wolf" attacks, weapons training, bomb making, and espionage tips. Subsections dedicated to cyber jihad provided information and instructions on using the latest technologies and encryption software, hacking, hiding online identity, and attacking databases, banking systems, and online retailers (MEMRI Cyber & Jihad Lab, 2011).

During that period of early work, many of the groups studied were more nationalistic than religious in nature; however, as jihadi groups began utilizing the internet and creating websites proliferated, scholars shifted their attention to these extremist groups, including the roles of governments and organizations in response to the emerging threat.

**Research of Cyber Terrorism**

The early studies of online terrorism were punctuated by a few groundbreaking observations. Furnell and Warren (1999) from the University of Plymouth predicted the nefarious uses of the internet by terrorist groups, including propaganda, fundraising, information dissemination, and secure communications. By 2002, the four observable uses were detailed by Cohen, an American computer scientist best known as the inventor of computer virus defense techniques. In 2003, Bunt provided the first comprehensive analysis of the impact of the internet on Islamic culture, with sections devoted to jihadi websites identifying the concept and emergence of e-jihad, or "electronic jihad." In 2006, Rogan, a research fellow with the Norwegian Defense Research Establishment Terrorism Research Group and expert on new militant Islamism and communication strategies and technologies, developed descriptions for online jihadists, including their structure and function, and anticipated that the internet would grow in importance to jihadis.

In the wake of an era of terrorist attacks, more scientists began studying cyber jihad. Shortly after 9/11, Arquilla and Ronfeldt (2001) published a sobering follow-up to an article by RAND consultants who had introduced in a 1993 article the terms "cyber war" and "net war" and had predicted opposition movements against Western nations through computer networks. Equally sobering was the lack of research on terrorists' use

of the internet. In a publication for the U.S. Institute of Peace, Weimann (2006) noted that policymakers, journalists, and academics focused on the overrated threat posed by cyber warfare (i.e., attacks on computer networks) and neglected terrorists' use of the internet every day. Conway (2007), a professor of law and government at Dublin City University, wrote a series of articles on online jihad that concurred with Weimann, explaining that there was limited substantive social science research on this subject.

**Social Media and Cyber Terrorism**

The early studies on cyber jihad underscored the fast pace at which the technologies and cyber jihad strategies had progressed. Since then, the main terrorist website of Al-Qaeda, *Al-Hesbah*, has been shut down and replaced by others, including *Al-Shoumoukh*. The number of internet users, which was described in the Middle East by Rogan (2006) as relatively low, grew significantly. Social media platforms such as Facebook, Twitter, and YouTube served as preferred channels of choice for terrorists (Rogan, 2006).

The connection between social media and terrorist attacks prompted social media platforms to take measures to limit the misuse of their services, such as Twitter's decision in 2012 to allow the withholding of certain content (Twitter, 2012). Many of the corporate efforts were met with criticism or were proven inconclusive or effective, as censored terrorists created new accounts (Lewis, 2015). In 2017, Facebook, Twitter, and YouTube formed the GIFCT to deter terrorist activity on their online platforms (Twitter Public Policy, 2017). However, critics said the effectiveness of GIFCT was undermined

by underpaid employees, insufficient resources, and terrorists finding new ways to circumvent rules (Levin, 2017).

**Rationale for the Selection of the Variables/Concepts**

The online terrorist presence continued to grow while the lack of research and insight persisted. Scholarly literature focusing on terrorist groups using the internet, particularly social media and encryption, was emerging as a relatively new, fast-paced subject (Jones et al., 2017). Because social media did not exist a decade prior, there was a greater gap in the research on social media policy guidelines and industry standards in relation to terrorism. For this reason, the current study focused on developing industry standards for social media platforms in response to a gap in research and in support of social media platforms and their responses to the misuse of platforms by terrorist groups.

**Known Concepts and/or Phenomena**

At the time of the current study, some aspects of terrorists' use of the internet were known. Cohen-Almagor (2013) detailed that terrorist groups were using the internet for political, religious, and ideological purposes. The online activity was defined as terrorism conducted using information technology, usually against information infrastructures, that results in violence (Cohen-Almagor, 2013). Cohen-Almagor noted that cyber-terror attacks could damage a country's economy by adversely affecting dams, nuclear plants, water, and power supplies by hacking into computers that control these services. E-jihad referred to attacks on information technology perpetrated by online groups such as Al-Qaeda (Cohen-Almagor, 2013). Cohen-Almagor also noted a method

called encryption, which protects communication channels by rendering emails and messages unreadable.

Encryption of such platforms is also a shared theme in previous studies. Klausen (2014) focused on terrorists using social media platforms such as Facebook, Twitter, Instagram, and Tumblr as well as encryption apps such as KIK and WhatsApp. Klausen revealed that these platforms became an integral part of the recruitment of jihadists groups, including ISIS, because they were used to keep communications private and to direct recruits to encrypted contact points. Klausen also highlighted how Twitter emerged as the most popular social media outlet for terrorists because of its affordability and ease of use. Weimann (2014) conducted a study that focused on the transition from traditional online activity to social media use by terrorist organizations for propaganda, recruitment, and fundraising. Weimann also highlighted the increase in the sharing of encryption software by terrorists because it allowed large audiences and ease of use, providing an even lower threshold for access than forums and websites. Weimann noted that social media allows anyone to share information with others instantly. Weimann also mentioned two jihadi encryption programs, one by Al-Qaeda and one by ISIS.

Elaborating on encryption as a point of focus, the cyber security research firm Recorded Future published the first in a series of studies, “How Al-Qaeda Uses Encryption Post-Snowden,” which provided a timeline of Al-Qaeda’s development of its own encryption technology, noting the accelerated use of encryption by terrorist groups following disclosures by National Security Agency whistleblower Edward Snowden (Ahlberg, 2014). The second part of the series confirmed the post-Snowden growth in

development and usage in encryption software by Al-Qaeda. However, the research lacked information regarding ISIS and other terrorist organizations using encryption, and it also neglected to detail the exact actions of the terrorists following the Snowden disclosures (Ahlberg, 2014).

**Controversial Concepts and/or Phenomena**

The literature revealed several controversies surrounding cyber jihad, beginning with diverging thoughts on what to do with terrorist content. Some believed, as detailed in the report by Rogan (2006), that allowing jihadist content to remain online provided a large amount of information about the movement as a means to collect intelligence, create a systematic understanding of the jihadist, and prevent terrorist attacks. In preventing online jihadist content, a remarkable amount of information was lost. Further, it was argued that it was almost impossible to stop all jihadist communication; as one tool was stopped, another was utilized. On the other hand, the prevailing thought was to consider social platforms less as a place to gather intelligence and more as a battlespace. Rogan pointed out that if learning by monitoring made a real difference, the war on terror would already be won (Rogan, 2006).

Other authors elaborate on controversy surrounding this topic. Another controversial aspect in the literature was the entities cited as responsible for the rise of cyber jihad, namely the failure of the West in battling the problem. In, "How to Lose a Cyberwar," Arquilla expressed frustration that a new generation of terrorist networks were not only able to stay in touch but able to extend their reach online (Arquilla, 2009). More specifically, the article pinned the blame on U.S. leadership for its historical lack of

effective response to terrorists' use of the internet, asserting that former U.S. President Barack Obama neglected to address cyberspace when he discussed denying a safe haven for Al-Qaeda. As Arquilla (2009) pointed out, this omission was more than President's Obama's alone, as none of the key military, intelligence, and law-enforcement arms of the U.S. government did much to curtail terrorist use of the Net.

A controversial facet of this topic is determining responsibility for terrorist use of social media platforms. As such, along with the U.S. government, social media platforms were held as partly responsible for the continuing problem of cyber jihad. In 2017, *The Economist* noticed that only after major terrorist attacks did some of the most influential media outlets begin to look at a need for developing shared industry standards to deal with terrorist activities on their platforms (The Economist, 2017). Technology companies were accused of prioritizing profit ahead of their responsibility to the community and were now increasingly facing criticism by politicians and lawsuits from citizens for not taking sufficient action to remove terrorist content (The Economist, June 2017).

Another controversy presented in the literature was the prospect of social media platforms and the U.S. government in working together to deal with cyber jihad. According to a report by the U.S. House of Representatives, major factors in terrorists' ability to create online safe havens and conceal propagandist activities from law enforcement was the use of publicly-available encrypted communications tools and social media as their virtual recruitment center (Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel, 2015). The report recommended a close working relationship between the Administration and social media platforms to develop resources

that accelerate the removal of extremist content which violates their terms of service (Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel, 2015). *The Economist* (2017) concurred, arguing for transparent cooperation with lawmakers and stating that the exploitation of the free internet by jihadis indicated a need to regulate an industry that was previously unregulated, a necessity that would create new problems and responsibilities for firms.

However, the *New York Law Journal* noted the complications that could arise between social media platforms and the government. If the government forced private companies to divulge the decryption key, it could incur legal challenges based on violation of the Fifth Amendment. The compelled party would be able to make the case that divulging the password was testimonial in nature if it was determined that the very act of production of this evidence was testimonial in nature (Crusco, 2015).

**Concepts and/or Phenomena Remaining to be Studied**

One of the most pressing aspects of terrorism remaining to be studied was the development of effective responses to terrorists' misuse of the internet, particularly social media. Countries throughout the world attempted different strategies in efforts to address online terrorist content. According to La Voix du Nord (2017), for example, France made it illegal to access jihadi websites, providing the basis for the conviction of a 23-year-old man after it was discovered later that year that he had accessed massive amounts of jihadi propaganda and content online. La Voix du Nord reported that nearly 600 jihadi documents were found on the man's phone and tablet, including beheadings, killing of

babies and a crucifixion by ISIS. The man was sentenced to a year in French prison (La Voix du Nord, 2017).

In 2018, the efforts to combat terrorism focused on social media, when Europol's Internet Referral Unit (EU IRU) and members of Internet Referral Units (IRU) from Belgium, France, and United Kingdom organized the eighth joint Referral Action Day to remove terrorist and violent extremism content uploaded on Facebook and Instagram. Law enforcement units performed assessments of several hundred pieces of suspected terrorist propaganda, detected emerging patterns of terrorist abuse of the online platforms, and looked at the rise of user-generated content as opposed to official content from terrorist organizations. Facebook joined the joint action of the EU IRU and national IRUs to identity propaganda videos and publications glorifying or supporting terrorism and extremism and help remove terrorists and related posts (Eurpol, 2018). More joint actions could be organized in the future by the EU in conjunction with its online industry partners, which would contribute to the progress of both law enforcement and social media platforms in combatting cyber jihad (Eurpol, 2018). Because these collaborative industry efforts were in the early stages of development, much remained to be studied and documented in developing effective responses to terrorists.

To bridge the gap in literature related to terrorists and social media misuse, a correlating study of standards development was necessary, particularly the groundwork established by research organizations and non-governmental organizations (NGOs) for relatively new industries such as social media. For example, one of the nation's oldest physical science laboratories, the National Institute of Standards and Technology (NIST),

researched and developed best practices for industries, academia, and other federal agencies (NIST, 2009). The NIST was an important resource with state-of-the-art facilities and expertise on creating consensus-based standards in every area, from cybersecurity to mammograms (NIST, 2009).

Additionally, the System Audit Network Security Institute (SANS) was helpful in defining industry standards in the technology realm (SANS, n.d.). SANS (n.d.) defined the terms "policy," "standard," and "guideline" in referring to documents that addressed policy infrastructure and provided a definition for each term. Policy was defined as a document outlining criteria to be met in a single area, and standard was defined as a collection of system- or procedural-specific requirements to be met by everyone (SANS, n.d.). Guideline was defined as a collection of system- or procedural-specific suggestions for best practices that were not required (SANS, n.d.).

The Digital Collections and Archives (DCA) of Tufts University also offered sets of guidelines and tools for managing and developing guidelines (Tufts University, n.d.). One set of guidelines was helpful for using information stewardship, setting core principles for stewardship, and for supporting information policies for developing effective and policies (Tufts University, n.d.). Another set of guidelines provided managers with advice for developing a new policy or revising an existing policy and prescribing a formal policy development and approval process, including identifying a policy gap, gaining at least an informal consensus from key stakeholders, assembling a small working group to draft the new policy or update an existing one, and determining who needs to approve the policy (Tufts University, n.d.). In addition, Tufts University

(n.d.) provided a template for policy documents designed to help managers form well-crafted policy documents.

Another helpful organization, the Information Technology Industry Council (ITI), was a nonprofit that works with the private sector and government to promote industry standards around the world (ITI, n.d.). ITI (n.d.) sponsored the International Committee for Information Technology Standard (INCITS), an organization dedicated to creating technology standards for the next generation of innovation. It was the leading developer of global and U.S. information and communications technology standards.

Domestically, INCITS focused on creating new American National Standards as part of its mission to promote the effective use of technology through standardization (ITI, n.d.). INCITS operated through the consensus of members who work together in technical committees and groups to create standards that result in globally-accepted, highly-interoperable products (ITI, n.d.). Its procedures allowed everyone with an interest in a subject covered by a standard to participate, either as a member of the consensus body or through public comment, and to have their comments considered (ITI, n.d.). Many times, the U.S. standard that INCITS members develop became the baseline standard for the international community.

Finally, the Institute of Electrical and Electronics Engineers' Standards Association (IEEE-SA, 2017) was one of the world's leading SDOs. On the IEEE-SA website (2017), Managing Director Dr. Konstantinos Karachalios discussed how industry standards played a growing role in the lives of the average person. Karachalios explained that standards were written documents used in nearly every aspect of industry – from

transportation to green technology – to ensure maximum reliability and productivity (IEEE-SA, 2017).

According to Karachalios, there were two types of standards, *de facto* and consensus-based (IEEE-SA, 2017). *De facto* standards were widely accepted by an industry without a ruling on them by any organization. The IEEE-SA (2017) made the final ruling on whether a standard should be accepted as consensus-based. These standards made it easier and cheaper for platforms to access technology and provide manufacturers access to new markets.

**Meaningful Approach for the Current Study**

A meaningful approach for this study – including the selection of research questions – was based on the synthesis of the two bodies of literature on terrorists' use of social media and standards development. To diffuse potential controversies in working with social media platforms, I sought to build on the strengths of existing corporate policies. To create standards in a relatively new industry, the study drew from ITI's (n.d.) attributes of the standardization process for industries, which encouraged innovators and product developers to speak to each other in a common language, resulting in an open, voluntary, consensus-based process applied to products around the world. According to ITI (n.d.), a result of this attribute was the improvement of the use and appeal of products and the selection of the best standards by innovators and product developers as they revised their choices based on technology and market conditions.

Based on this literature, this study sought to bring together developers across social media platforms to emulate the open, consensus-based process proven successful

in other industries. The approach of this study was also directly shaped by advice on standards development found in Tuft University's (n.d.) DCA, including identifying the purpose and scope of the policy, making a policy statement using the core content of the policy, identifying entities who review the policy, identifying an executive sponsor, identifying policy managers, identifying responsible offices who reserve the right to revise the policy, identifying how the policy was to be disseminated, and listing relevant policies. The research questions reflected this methodical process of developing standards.

## Summary and Conclusions

Three major themes emerged from the body of literature: the alarming misuse of social media by terrorists, the persistent lack of an effective response to that threat, and the development of terrorist groups. What was known was the consequential relationship of these factors: a lack of an effective response by social media platforms enabled the continued wide-spread growth of terrorism, compounding the risk of terrorist attacks. Although there were initial efforts to mitigate the problem, insufficient literature existed on effective industry standards in response to the misuse of social media.

Therefore, in addition to reviewing literature on terrorists' use of social media, it was necessary to perform a correlating literature review on the development of industry standards. This study sought to apply the methodical processes established by standards development organizations to the relatively new social media industry to fill the gap in the literature on terrorists' misuse of social media. Chapter 3 explores in detail the

methodology of the study, including participant selection, instrumentation, and issues of trustworthiness.

# Chapter 3: Research Method

The purpose of this qualitative study was to develop industry policies based on existing social media platform policies so that social media platforms could mitigate the misuse of their services by terrorists. Mitigation of misuse could hinder the development of terrorist groups. This chapter includes the design and rationale of the study, the role of the researcher, the issues of trustworthiness, and the methodology that was applied, including participant selection, instrumentation, procedures, and data analysis.

## Research Design and Rationale

The questions that guided this study were as follows:

RQ1: In what ways were social media companies responding to the misuse of their platforms by terrorist groups?

RQ2: Could industry policies be produced from existing platform responses to form standardized policies to the misuse of social media by terrorists?

I compared the existing policies of individual social media platforms, building on commonalities and precedents to develop industry policies that combatted and disrupted the spread of radical ideology by terrorists to a younger generation. A qualitative method was selected because this approach allows researchers to study a problem that did not receive proper attention and to apply existing or new theories to form solutions (Patton & Cochran, 2002). A multiple case design was applied to this study for two reasons: (a) The resource-intensive approach focused on data gathered from the documents rather than participants' perceptions, including vast amounts of published data from congressional testimonies, press releases, interviews, existing policies, and precedents of individual

social media platforms; and (b) ethnography allowed a less restrictive, nontraditional study of online relationships and interactions.

Other research designs were considered but not selected, including quantitative, phenomenological, and mixed methods. A quantitative approach was not applied because I was not seeking to collect numerical data or examine relationships among variables. A phenomenological design was deemed not as useful as a multiple case design because phenomenology is more dependent on interviews and prioritizes lived experiences and perceptions over resource-intensive data (Chan et al., 2013).

The prospect of combining quantitative and qualitative data, known as mixed methods, garnered initial interest but was eventually dismissed in favor of a multiple case qualitative approach for three reasons. First, some faculty and peers strongly discouraged this design because of the additional complexity that would be added to the research. This seemingly easy design belied a complex approach to inquiry that could be problematic. As Creswell and Plano Clark (2017) stated, mixed-methods research is more than data collection and analysis; it requires the simultaneous application of approaches for a stronger study. Second, mixed methods is unfamiliar to many audiences (Creswell, 2013). Using an unfamiliar approach would require additional background information, including the evolution and definition of the research design (Creswell, 2013). Third, and finally, mixed methods is more time-consuming because it involves analysis of textual and numeric data and the familiarity of the researcher with quantitative and qualitative methods (Creswell, 2013). For these three reasons, a mixed methods design was not applied.

## Role of the Researcher

As an observer-participant, I and my research goals were known and recognized by the four participating social media platforms. I served as the main instrument in the data collection but had no contact with the participants. I collected and analyzed data through the use of secondary sources such as literature, corporate materials, and software tools. Throughout this qualitative study, I aimed to maintain a neutral role but acknowledged the dynamics that could impact a study, including power relationships, researcher biases, and other ethical issues.

In looking at professional relationships, I was prepared to meet with officials from the selected social media platforms about the problem prior to the study. I was prepared to introduce myself as working for an organization that facilitates collaborative work with technology companies to support the development of solutions in dealing with jihadis and terrorists online. This preliminary conversation would have established a positive rapport and allowed for a discussion of the need for industry standards. There were no power differentials or personal relationships complicating the study due to the sufficiency of secondary sources.

My predispositions and biases could be barriers to credible qualitative findings (Patton & Cochran, 2002). As an expert in the field of terrorism, I was shaped by more than a decade of study on terrorists' use of the internet and encryption technology. I formed a point of view on the responsibility of technology companies within the broad war on terrorism and whether their actions were helpful or harmful in combating the development of terrorist groups.

However, over time, my opinions evolved and became balanced as I examined the issue more closely. I countered bias by maintaining a high level of self-awareness, recognizing that neutrality was the best route to effective results, and prioritizing the potential for industry action over personal predispositions. Additionally, the technique of bracketing was employed throughout the study to control researcher bias by deliberately putting aside limiting beliefs and knowledge (Chan et al., 2013). One bracketing strategy was the use of a reflexive diary to identify any interest or value that could influence the study (Chan et al., 2013). Another bracketing strategy was the planning of data collection and analysis, allowing commonalities to emerge among existing platform policies to guide industry policies rather than imposing policies on the industry (Chan et al., 2013).

## Methodology

This section explores four aspects of the methodology of the study: participant selection, instrumentation, procedures, and data analysis.

### Participant Selection Logic

The population for this study comprised four leading social media platforms. The sampling strategy originated in an explanation by Patton and Cochran (2002) that a researcher involved in qualitative research must first decide the appropriate unit of analysis to study, from people to larger entities. In the current study, the most relevant unit of analysis was identified as larger entities in the form of social media platforms. Among social media platforms, the criteria for participant selection were based on critical case sampling and industry leadership, both of which ensured the likelihood that participants would be able to provide the insight and information needed for this study

(Creswell, 2013). Compared to other social media platforms, industry leaders had more resources, had been operating for a longer period of time, and were more at risk of misuse due to their popularity, all of which established them as meeting the criteria of critical cases.

The number of participants was an important consideration. Creswell (2013) explained that, although the number of subjects in qualitative research ranges from one to 325, the recommended range was three to 10 subjects. The number of participants is also guided by the principle of data saturation in qualitative studies, in which the attainment of meaningful data is the primary influencer of sample size (Mason, 2010).

Working within Creswell's (2013) recommended range, I identified five social media platforms as critical cases and industry leaders: Facebook, Twitter, YouTube, Google, and Telegram. Because Google was determined to be the parent company of YouTube, Google was eliminated to avoid repetitive findings and to attain the most industry-specific data. I deemed the four remaining social media platforms as sufficient to achieve data saturation, concluding that a fifth platform would add more data but not necessarily meaning. This study focused on four leading social media platforms as a practical way to balance the ability to gather broad perspectives across the industry with the ability to collect extensive details on the policies of each platform. The four participants were as follows: Facebook, Telegram, Twitter, and YouTube. The study did not involve active engagement with participants. Sufficient data from secondary sources eliminated the need for recruitment of social media platform representatives for this study.

## Instrumentation

For the most transferable and nonthreatening study, I aimed to collect information using open-source data and an organizational software tool. Open-source data included the vast amounts of published information within each participant's platform website, which included community standards, privacy policy, terms of services, user agreements, rules and policies, press releases, congressional testimonies, interviews with leadership, and other literature. The legally binding nature of each platform's terms of services was particularly helpful in crafting protective industry standards.

The data were classified and arranged in NVivo, a software program developed by QSR International that used in qualitative and mixed-methods research for the coding and analysis of unstructured data (NVivo, n.d.). Analysis was conducted in NVivo to determine whether industry standards could be developed from the existing data from each platform. A process by the world's leading SDOs was applied during analysis to develop industry standards (see American National Standards Institute, n.d.). Although open-source data were the primary source for the study, any gaps or discrepancies in data sources could have indicated a need to contact officials from one or more of the social media platforms. This scenario did not manifest, so a phone questionnaire was not designed for use with a senior staff leader as an alternate method for data collection.

### *Open-Source Data Sources*

Data were collected from the online corporate websites of the participants. Because the websites were created by the social media platforms, these data sources were the most appropriate and valid data sources for this study. The websites of the

participants were intended for developers, stakeholders, researchers, advertisers, and users.

The release dates and user groups varied slightly among the participants. Created in 2004, the Facebook platform was originally intended for college students; later, users over 13 years old were accessing the application (Facebook, n.d.). The following year, the YouTube platform targeted broader groups of people with common interests, intents, and demographics (YouTube, n.d.).

Twitter was released in 2006 for users who were at least 13 years old; the primary user group was U.S. adults between 18 and 29 years old (Twitter, n.d.). Telegram, which was created in 2013, was intended for an even broader audience (Telegram, n.d.). There was no age minimum, and the information from Telegram (n.d.) was available for anyone who wanted fast, private messaging and calls. Because of its encryption services, Telegram's user base increased when one of the other leading social media platforms was embroiled in a privacy scandal (Dailey, 2021).

All of the websites showed updates as recently as 2019 or 2020. Although there were variations among the user groups, all of the participants' websites addressed the context- and culture-specific issues of social media misuse data, including identifying and reporting safety threats and violence. No modifications to the data were needed prior to the current study because any insufficiencies found in the data served as findings. All collected data contributed to the larger aim of creating industry standards.

### *Organizational Software Tool*

Data were classified and analyzed using NVivo (n.d.), a software tool developed by Australian qualitative research software developer QSR International. Initially released in 1997, NVivo was intended for qualitative and mixed-methods deep data analysis by academic, government, and professional researchers around the world. NVivo's functions include storage, organization, categorization, analysis, visualization, and transcription. No modifications were needed in the current study because the tool accommodated a wide range of research methods, data formats, applications, and languages, making it suitable for the context- and culture-specific issues of social media misuse and policy development (see NVivo, n.d.).

## Procedures for Recruitment, Participation, and Data Collection

I collected data from the websites of the participants to answer the two research questions, making the recruitment and interviewing of participants unnecessary. However, in the case interviewing was needed, data were recorded in NVivo (n.d.) and classified by participant, research question, and categories of misuse of social media by terrorists. The duration of the data collection was the time necessary to download the online documents, with the understanding that the policies of each participant were best practices to date that were developed over time since the inception of each social media platform. Any discrepant data would be an indication of the areas in which the industry needed standardized responses. Because the secondary open-source data provided sufficient information, and because the four participants included in this study were

critical cases and industry leaders, any discrepancies in data would indicate industry policy gaps and facilitate follow-up industry recommendations.

**Data Analysis Plan**

After collecting data from the websites of the participants, I reviewed the data in light of the first research question:

RQ1: In what ways were social media companies responding to the misuse of their platforms by terrorist groups?

Within each website, the data sources reviewed were as follows:

- The Twitter website (n.d.) provided the Twitter User Agreement, effective January 1, 2020. The User Agreement was relevant to the current study because it contained the platform's rules and policies on content, privacy rights, usage of services, accounts, disclaimers, and limitations of liability. Also relevant to this study was Twitter's Hackone Program for security researchers, which provided response standards and application programming interface documentation.
- The Facebook website contained several materials that were pertinent for the current study, including "Writing Facebook's Rule Book," a video created on April 10, 2019, to explain how Facebook policies were shaped and enforced (Facebook, 2019). Also provided were Product Policy Forum Minutes, which documented policy discussions among a variety of subject matter experts such as safety and cybersecurity policy teams, counterterrorism specialists, community operations employees, product managers, public policy leads, and

representatives from legal, communications, and diversity teams. Product Policy Forum Minutes were posted online every 2 weeks, dating back to November 15, 2018 (Facebook, 2018). The Facebook website also contained Terms of Service and Community Standards that addressed violence and criminal behavior, safety, and objectionable content, all of which was last revised July 31, 2019.

- The YouTube website outlined the Terms of Services, which was last updated on December 10, 2019. The site also provided a Policies and Safety section, containing Community Guidelines on harmful or dangerous content, hateful content, violent or graphic content, and threats. It also contained systems in place for Reporting and Reinforcement, including a "strikes" system.
- Since August 2013, the Telegram website provided information in its "FAQs" page.

Where a piece of data connected to one of the research questions, the information was entered and classified in a software tool, NVivo. Together, the data underwent analysis to fulfill the second research question:

RQ2: Could industry policies be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists?

To answer this research question, the data was classified according to participant, method of misuse of social media by terrorists, purpose of misuse in the development of terrorist groups, current terms of service and policies employed by participants in response to the misuse, and any precedents established by participants in response to

other misuses. I sought commonalities among the data categories and across participants. Where commonalities and connections were found, standards were formed. Any discrepant cases were considered helpful in identifying gaps in industry policies and forming follow-up industry recommendations.

## Issues of Trustworthiness

Patton and Cochran (2002) described credibility in research as a combination of precision and attention. The credibility and internal validity of the study was established by downloading data directly from the websites of the participants, ensuring that the industry standards resulting from the study resonated with the participants for practical implementation. Another method of establishing credibility was saturation. As previously discussed, selecting critical cases and industry leaders as participants ensured data saturation without inefficiency and redundancy. Finally, internal validity was established using triangulation. By aligning multiple perspectives and responses to the misuse of social media across the industry, best practices were corroborated, and I was provided a more comprehensive understanding of the phenomenon (Salkind, 2010).

Also important was transferability, or external validity. In this study, my methodology established the greatest opportunity for generalization. Participant selection from among industry leaders, data collection primarily from open-source data, the use of software tools, and the application of a standardization process by SDOs allowed for the transferability of this study to other social media platforms and to other industry sectors.

Dependability was established in two ways. The triangulation of the data was helpful for verifying findings as consistent and repeatable. Additionally, an audit trail

provided a transparent description of the research steps in this study. The trail included downloaded documents, raw data, data analysis, notes, literature, industry policies, and other recommendations. The audit trail also served to establish confirmability of the data, process, results, and rationale of the researcher.

Intercoder reliability – the process of analysis of written materials by a single researcher – was established in two ways. I used the software tool, NVivo, and a standardization process by SDOs. Both methods ensured consistent, methodical analysis of the data.

## Ethical Procedures

Because the information in this study was collected primarily from secondary, open-data sources, there was no concern for ethical issues or the need for safeguards related to the treatment of the participants or data. Therefore, there was no need for agreements and permissions. It was not necessary to take measures to ensure the ethical treatment of human participants, corporate identities, and corporate data, including my past measure in completing the National Institutes of Health (NIH) Office of Extramural Research Certification web-based training course, "Protecting Human Research Participants," in March 2013.

An ethical consideration was my professional connections. In this study, I was involved with an organization whose work included analyzing social and cultural trends and supporting the U.S. government and used as an academic source by many universities. In my decades-long work on the topic, I met with officials from many social media platforms, including the platforms selected as participants; any conflict of interest

or power differential was mitigated by the approach to data collection. I also acknowledged the potential limitations of the participant group – the varying levels of utilization of platforms by terrorists, willingness to take action by social media platforms, and the limited resources in tracking and reacting to terrorist activity – all of which were mitigated by the nature of the data collection. It was not necessary for me to explain the purpose of the study and the beneficial economic, social, and legal implications for social media platforms.

Regarding the ethical treatment of data, I did not interact with human participants, which assured fair, lawful, and useful collective development of industry standards. No data was used to disparage the reputation of the participants. Any data that was deemed disparaging by the me or participants would serve only to provide me with a comprehensive understanding of the industry. However, it was not necessary to take such measures, including classifying me in NVivo as anonymous.

Another ethical consideration was the use of the terms “terrorists” and “terrorist groups” in the study. In objectively identifying “terrorists” and “terrorist groups,” some people claimed that certain individuals or groups were not terrorists. It could be argued that one man’s freedom fighter was another man’s terrorist. For the purpose of this study, “terrorists” and “terrorist groups” were defined as those officially designated as such by the United States. Further, the study focused on the misuse of social media by two critical groups: Al-Qaeda and ISIS.

## Summary

Chapter 3 examined the methodology of this qualitative research, beginning with the design and rationale of the multiple case study and my role as the researcher. The methodology included the selection of participants based on critical cases in the social media industry and instrumentation of data based on open-source data and a qualitative research software tool, NVivo. Data analysis was conducted according to the four driving research questions, remaining mindful of issues of trustworthiness and ethics. Chapter 4 describes the actual implementation of the study, including setting, demographics, data collection, analysis, evidence of trustworthiness, and results.

# Chapter 4: Results

The purpose of the study was to develop industry policies based on existing platform policies so that social media platforms could respond to the misuse of their services by terrorists. The following research questions guided the study:

RQ1: What were the existing responses to terrorists' misuse of social media platforms?

RQ2: Could industry policies be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists?

This chapter addresses the setting, demographics, and data collection and analysis, and evidence of trustworthiness. The results of the study are organized by research question and presented in tables as appropriate.

## Setting

The interpretation of the results was not known to be influenced by organizational or personal conditions at the time of the study. The open-source approach of the study involved collection of secondary data from social media platforms related to the focus of this study. Although the nature of the social media industry is changing, I found sufficient data for analysis of similarities and differences among existing platform policies.

## Demographics

There were four social media platforms in the participant group: Facebook, Twitter, YouTube, and Telegram. These platforms differed in their social media services but shared similarities as key industry leaders. Table 1 shows the differences and similarities between the four leading social media platforms.

**Table 1**

*Demographics and Characteristics of the Participant Group*

| Social media platform | Date est. | Annual revenue | Number of users | Date of first recorded instance of terrorist use |
|---|---|---|---|---|
| YouTube/ Google | Google: 1998<br><br>YouTube: 2005 | Google: $181.69 billion<br><br>YouTube: $19.77 billion | Google: Nearly 4 billion<br><br>YouTube: 2.29 billion | May 31, 2007: Islamist websites posted a five-minute video of abducted BBC journalist Alan Johnston, produced by the Palestinian organization Jaysh Al-Islam (MEMRI Jihad & Terrorism Threat Monitor, 2007). |
| Twitter | 2006 | $3.72 billion | 206 million | According to media articles, around 2008 (Economic Times, 2008).<br><br>February 17, 2011: Taliban Commander's Interview Revealing The Details Of Their Print Magazines And International Media Operations, Says: 'We Are Also Active On Facebook And Twitter Where We Publish The News Every Day.' "We are also active on Facebook and Twitter where we publish the news every day and reach thousands of people" (Weimann, 2010). |
| Facebook | 2004 | $85.97 billion | 2.89 billion | Around 2008: Al-Qaeda documented using FB Aug. 21, 2008 (Weimann, 2010).<br><br>December 2, 2008: Islamist Websites Launch Online Campaign for General Strike in Egypt. One forum member indicated the following websites, which he said are visited by millions of Egyptians, as venues for the campaign: www.masrawy.com, www.yallakora.com, forum.amrkhaled.net, and www.facebook.com (MEMRI Jihad & Terrorism Threat Monitor, 2008). |
| Telegram | 2013 | Telegram does not generate revenue. | 200 million | Around 2015: Paris attacks (Tan, 2017).<br><br>March 13, 2014: Syria-Based Saudi Sheikh Launches Second Campaign To Purchase Ammunition For Jihadi Groups Fighting In Syria.<br>One tweet from March 8, 2014, recommended that anyone wishing to contact the campaign organizers use the encrypted Telegram messaging app, rather than the well-known WhatsApp which, it said, provided no privacy to its users (MEMRI Jihad & Terrorism Threat Monitor, 2014). |

## Data Collection

The most appropriate, valid, and updated instruments were identified for this study. Data were collected from each of the four social media platforms selected for the participant group: Facebook, Telegram, Twitter, and YouTube. Data collection occurred virtually using three published data collection instruments: open-source data sources, Microsoft Word, and an organizational software tool. From open-source data sources, the data were organized in Microsoft Word and analyzed in NVivo using arrangement, coding, subcode settings, analyses, and visualization.

### Open-Source Data Sources

Data were collected virtually from government websites, media articles, and the online corporate websites of the four participants, which were identified as the most appropriate, valid, and updated instruments for this study: Facebook, Twitter, Telegram, and YouTube. The websites supplied information for developers, stakeholders, researchers, advertisers, and users that addressed the context- and culture-specific issues of social media misuse data, including identifying and reporting safety threats and violence. Website information was downloaded and/or recorded from community standards, privacy policy, terms of services, user agreements, rules and policies, press releases, congressional testimonies, interviews with leadership, and/or other literature. The process of data collection for this study was conducted from January 2017 to April 2019.

### Organizational Software Tool

Data were recorded using NVivo (n.d.), a software tool for qualitative and mixed-methods deep data analysis by academic, government, and professional researchers. NVivo enabled the recording and storage of data, including the transcription of video and audio recordings as needed. NVivo also enabled the classification and organization of data by participant, context of misuse of social media, and international response.

### Variations in Data Collection

There were no variations or unusual circumstances encountered in the data collection plan outlined in Chapter 3.

## Data Analysis

The qualitative data were collected in textual form using Microsoft Word for analysis. The gathered data were analyzed through NVivo 12 because it provides clear systems for examining data (Cohen, 2017). Coding was applied to develop parent codes and child codes for further analyses. All of the specified codes were organized and assessed by the triggers.

I applied hierarchy charting that accounted for item codes, word frequency, word hierarchy, matrix coding, and thematic visualization. The results are presented in tables and figures later in this chapter. Themes emerged from the analysis, including inferences on which areas to focus industry policies. My bias in the interpretation of these results was minimized with evidence-based documentation.

## Development of Themes and Subthemes

I analyzed four case studies: New Zealand attack (2019), United Kingdom attack (2017), France attack (2017), and United States attack (2017). These cases were analyzed by statements and social media responses on Facebook, Twitter, and YouTube. I developed six major themes to answer RQ2 (Can industry policies can be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists?). The major themes were government collaboration with online platforms, a new era of regulation, online platforms taking greater responsibility, online platforms' ability to remove content, imposing consequences on online platforms, and platform policies and policy changes. The following subthemes were generated to analyze code-based queries.

1. Government collaboration with online platforms included legislation, rule of law, resolutions, legal instruments, and human rights.
2. New era of regulation included investigations, gathering, and preservation.
3. Online platforms taking greater responsibility included use of internet, misuse of internet, cybercrime, digital evidence, training, awareness, framework, and challenges.
4. Online platforms' ability to remove content included illegal content law, stricter rules applicability, moderating online content, moderating disinformation, moderating terror content, freedom of speech issues, and specific measures.

5. Imposing consequences on online platforms included effect of online media, mainstream media, open-source forum, lack of check and balance, and trends and campaign.
6. Platform policies and policy changes included community standard violations, more resources, nationalism, separatism, privacy issues, data protection issues, incitement for anarchy, violence, hate speech, fake news, misinformation, and cybercrime.

Codes were used to analyze the data. I adopted in-depth content analysis techniques to uncover to what extent industry policies can be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists. There were no discrepant cases.

## Evidence of Trustworthiness

Trustworthiness of the study was evident in four aspects: credibility, transferability, dependability, and confirmability. The first aspect of trustworthiness (credibility or internal validity) was established by downloading directly from the four participants' websites, ensuring that the resulting standards resonated with the industry for practical implementation. Another method of establishing credibility was data saturation, which involved the selection of critical cases and industry leaders as participants (Facebook, Telegram, Twitter, and YouTube). Finally, internal validity was established by using triangulation, which involved aligning multiple perspectives and responses to the misuse of social media, corroborating best practices, and providing a

more comprehensive understanding of needs and policies across the industry (see Salkind, 2010).

The second aspect of trustworthiness (transferability or external validity) was established by the methodology. A participant group of key industry leaders, data collection from open-source data, the use of NVivo, and the application of a standardization process by SDOs allowed for the highest possible transferability of this study. As a result, policies could be transferred to other social media platforms and to other industry sectors.

The third aspect of trustworthiness (dependability) was established using triangulation of the data, which verified findings as consistent and repeatable. Additionally, an audit trail provided a transparent description of the research steps in this study. The trail included downloaded documents, raw data, data analysis, notes, literature, industry policies, and other recommendations. The audit trail also served to establish the fourth aspect of trustworthiness (confirmability).

## Results

The multiple case study was guided by two research questions:

RQ1: What were the existing responses to terrorists' misuse of social media platforms?

RQ2: Could industry policies be developed from existing responses to terrorists' misuse of social media platforms?

In this section, the RQs are addressed by the results of four case studies, including emerging themes and subthemes.

**Case Study 1: Terrorist Attacks in the United Kingdom by ISIS in 2017**

Tables 2 and 3 show responses to terrorists' misuse of social media platforms after a series of three terrorist attacks in the United Kingdom in 2017. The first attack occurred in Westminster, where a man named Khalid Masood drove a car directly into a crowd on March 22, 2017. Four pedestrians were killed, and dozens were injured. The second attack was in Manchester, where Salman Abedi detonated a suicide bomb at a concert on May 20, 2017, killing 22 people and injuring more than 200.

The third attack occurred on June 3, 2017, on the London Bridge, where extremists drove a van into pedestrians on the bridge. Three extremists (Rachid Redouane, Khuram Butt, and Youssef Zaghba) stepped out and stabbed eight people to death in Borough market. Table 2 includes responses after the attack by leaders from two governments as well as one educational institution. Table 3 includes corporate statements by three major social media platforms.

**Table 2**

*Statements by Government Leaders and Other Institutions Concerning Online Platforms in Reaction to Terrorist Attacks in the United Kingdom by ISIS in 2017*

| Organization | Representative | Statement |
|---|---|---|
| U.K. National Crime Agency | Emily Dreyfuss | "Don't share pictures or video of the #manchesterexplosion on social media. Please show respect to victims and their families…" (Dreyfuss, 2017). |
| U.K. Government | Prime Minister Theresa May | "exploring the possibility of creating a new legal liability for tech companies if they fail to remove content," including "penalties such as fines for companies that fail to take action" (U.K. Government, 2017). |
| U.K. Government | Prime Minister Theresa May | "cannot allow this ideology the safe space it needs to breed. Yet that is precisely what the internet and the big companies that provide internet-based services provide" (Stone, 2017). |
| U.S. Government | Senator Al Franken | "We cannot let the internet be a safe haven for terrorist propaganda…we have to be able to take down those kinds of sites" (Murphy, 2017). |
| U.S. Government | Rep. Ro Khanna (Dem. CA) | "While I am certain more work to address this issue must be done, technology companies are being responsive and helping lead the effort to combat online sources that threaten our mutual goals for peace and prosperity…" (The Hill, 2017). |
| U.K. Government | Prime Minister Theresa May | "Just as these big companies need to step up, so we also need cross-industry responses because smaller platforms can quickly become home to criminals and terrorists. We have seen that happen with Telegram. And we need to see more co-operation from smaller platforms like this" (Stewart & Elgot, 2018). |
| U.K. Government | Home Secretary Amber Rudd | "We need [social media companies] to take a more proactive and leading role in tackling the terrorist abuse of their platforms." Rudd continued, "We need to make sure that organizations like WhatsApp, and there are plenty of others like that, don't provide a secret place for terrorists to communicate with each other... we need to make sure that our intelligence services have the ability to get into situations like encrypted WhatsApp" (Hern, 2018). |
| U.K. Government | MI5's Intelligence and Security Committee | "But the ISC reserved some of its strongest criticism for technology groups over their handling of online extremist content and communications, urging the government to lobby marketing executives to pull advertising from the big online platforms unless they did more to remove extremist content online" (Financial Times, 2018). |
| Cardiff University | None | "MPs have called for stronger enforcement on technology and social media companies. They also found that current electoral law is 'not fit for purpose' and that Facebook 'intentionally and knowingly violated both data privacy and anti-competition laws'" (Cardiff University, 2019). |

**Table 3**

*Statements by Social Media Platforms After Terrorist Attacks in the United Kingdom by ISIS in 2017*

| Organization | Representative | Statement |
|---|---|---|
| WhatsApp | Official statement | "We are horrified at the attack carried out in London and are cooperating with law enforcement as they continue their investigations" (Guynn, 2017). |
| Twitter | Head of U.K. Policy Nick Pickles | "Terrorist content has no place on Twitter. We continue to expand the use of technology as part of a systematic approach to removing this type of content. We will never stop working to stay one step ahead and will continue to engage with our partners across industry, government, civil society and academia" (Price, 2017). |
| Google | General Counsel Kent Walker | "Terrorism is an attack on open societies, and addressing the threat posed by violence and hate is a critical challenge for us all. Google and YouTube are committed to being part of the solution. We are working with government, law enforcement and civil society groups to tackle the problem of violent extremism online. There should be no place for terrorist content on our services" (Walker, 2017). |

**Case Study 2: Terrorist Attacks in France by ISIS in 2017 and 2018**

Tables 2 and 3 showed responses to terrorists' misuse of social media platforms after terrorist attacks in France. The first attack occurred on August 9, 2017, when radical Algerian Islamist Hamou Benlatrèche rammed his car into a group of soldiers as they left their barracks in the Levallois-Perret commune. Six soldiers were injured, three seriously.

The second attack occurred on October 1, 2017, when a knife-wielding Islamist stabbed two young women to death at the Saint-Charles train station in Marseille before running away shouting, "Allahu akbar!" On March 23, 2018, two Islamist attacks

occurred in the towns of Carcossonne and Trebes by a 25-year-old Moroccan named Redouane Lakdim. Ladkim killed four people and injured 15. Victims were occupants of a car and a grocery store and included Lieutenant Colonel Arnaud Beltrame, who had voluntarily swapped places with a hostage. Table 4 focused on responses after the attack by leaders from two governments. Table 5 focused on corporate statements by two major social media platforms.

**Table 4**

*Statements by International Government Leaders Concerning Online Platforms in Reaction to Terrorist Attacks in France in 2017 and 2018*

| Organization | Representative | Statement |
|---|---|---|
| French Government | President Emmanuel Macron | "'no longer acceptable' that companies say they have a contractual obligation to their users to protect their communications... 'Democratic states must have access to content exchanged between terrorists on social media and instant messaging'…" (Lomas, 2017). |
| French and U.K. Governments | President Macron and Prime Minister May | "exploring the possibility of creating a new legal liability for tech companies if they fail to remove content," including "penalties such as fines for companies that fail to take action" (U.K. Government, 2017). |
| French and U.K. Governments | President Macron and Prime Minister May | "to stop the spread of extremist material that is warping young minds... and abide by their social responsibility to step up their efforts to remove harmful content" (BBC, 2017). |
| U.K. Government | Metropolitan Police Assistant Commissioner Mark Rowley | "We need communications and internet-based companies to show more responsibility... more assertive at calling out extremists and radicalizers among us…" (The Times, 2017). |

**Table 5**

*Statements by Social Media Platforms After Terrorist Attacks in France by ISIS in 2017 and 2018*

| Organization | Statement |
|---|---|
| Twitter | "Twitter says it has suspended 360,000 user accounts in the past 18 months for threatening or promoting acts of terrorism... Twitter said in a statement that it condemns the use of its services to promote terrorism. 'This type of behavior, or any violent threat, is not permitted on our service…'" (CBS News, 2017). |
| Facebook | "Facebook has zero tolerance for terrorism... It condemns terrorist actions, prohibits terrorist content on Facebook, and swiftly removes any reported terrorist content" (L.A. Times, 2017). |

**Case Study 3: Terrorist Attack in the United States by ISIS in 2017**

On October 31, 2017, a terrorist plowed a truck into cyclists and runners along a bike path in Lower Manhattan, New York City. The attack killed eight people and injured 11. Table 6 showed responses to terrorists' misuse of social media platforms after the terrorist attack.

**Table 6**

*Statements by Social Media Platforms and the Government in Reaction to a Terrorist Attack in the United States by ISIS in 2017*

| Organization | Representative | Statement |
|---|---|---|
| Twitter | Official statement | "While we've made good progress, we recognize there's more to do" (Rutenberg, 2017). |
| U.S. Government | New York Governor Andrew Cuomo | "Internet companies should re-examine their policies regarding how best to respond when users visit extremist sites on the web . . . urge Internet companies to reassess their approach to extremist content" (Nicas, 2017). |

**Case Study 4: Terrorist Attack in New Zealand by a White Supremacist in 2019**

On March 15, 2019, 28-year-old Brenton Tarrant attacked two mosques, killing 50 and wounding 50 others in a shooting. Tarrant faced 50 murder charges and 39 attempted murder charges. Tarrant live-streamed the shooting at the first mosque, Al Noor Mosque, on Facebook Live. The live-stream video was first reported 29 minutes after the stream began and 12 minutes after it ended, being viewed over 4,000 times before Facebook took it down. The video was also spread on Twitter and YouTube (Van Boom & Keane, 2019).

Tables 7 and 8 (below) showed responses to terrorists' misuse of social media platforms after the 2019 terrorist attack in Christchurch, New Zealand. Table 7 focused on responses by government leaders after the attack, including the statements of 17 leaders across five governments. Table 8 focused on corporate statements by three major social media platforms.

## Table 7

*Statements by Government Leaders Concerning Online Platforms in Reaction to a Terrorist Attack in New Zealand by a White Supremacist in 2019*

| Organization | Official | Statement |
|---|---|---|
| Australian Government | Prime Minister Scott Morrison | Stated that he wants the social media platforms to come to the table as "responsible corporate citizens." |
| | | "We want the same rules to apply in the online social media world that exist in the physical world. Building and making it safe means you can't let a terrorist atrocity be filmed and up and posted and streamed and be online for 69 minutes – 69 minutes – that's not acceptable, that has to change." |
| | | "They can get an ad to you in half a second; they should be able to pull down this sort of terrorist material and other types of very dangerous material in the same sort of time frame" (Barbaschow, 2019). |
| New Zealand Government | Prime Minister Jacinda Ardern | Said tech companies have "a lot of work" to do to curb the proliferation of content that incites hate and violence. |
| | | Stated she would ask Facebook officials how the Christchurch attacks were able to be live-streamed, as the company revealed it removed 1.5 million videos of the shootings in 24 hours. |
| | | "This is an issue that goes well beyond New Zealand but that doesn't mean we can't play an active role in seeing it resolved. This is an issue I will look to be discussing directly with Facebook" (Digital Team, 2019). |
| U.S. Government | Rep. Bennie Thompson | Wrote letters to the heads of major tech companies on March 19, requesting a briefing on March 27 about their response to Tarrant's live stream and subsequent re-uploads that went viral. |
| | | The letter was sent to Facebook CEO Mark Zuckerberg, YouTube CEO Susan Wojcicki, Twitter CEO Jack Dorsey, and Microsoft CEO Satya Nadella. |
| | | The letter urged the companies to prioritize the removal of the terrorist content and to brief the committee on their response and plans to prevent something similar from happening in the future (Birnbaum, 2019). |
| | Senator Mark Warner | "I want technology to stay. I want the social media platforms to stay. But I do think the days of the Wild Wild West where anything goes, people just aren't going to allow it" (Bartz, 2019). |
| | Speaker Nancy Pelosi | Specifically stated that Section 230 of the Communications Decency Act, which essentially grants immunity to tech companies from content users publish on their platforms: "is a gift to them (tech companies) and I don't think that they are treating it with the respect that they should, and so I think that that could be a question mark and in jeopardy" (Birnbaum, 2019). |
| | | "When we come to 230, you really get their attention. But I do think that for the privilege of 230, there has to be a bigger sense of responsibility on it. And it is not out of the question that that could be removed" (Birnbaum, 2019). |
| | Letter by four Democratic Representatives | "During a briefing to the Committee on March 27, 2019, your representatives conveyed your companies' commitment to combating foreign and domestic terrorist content and other violent or hateful material on your platforms," says the letter, which is addressed to the companies' CEOs. "While we appreciated their strong words, we expect to see these verbal commitments backed up with financial resources, personnel, and technological investments" (Swan, 2019). |
| | | "As you all know, a budget is a statement of values. We believe that the level of resources your companies allocate to containing and combating online terrorist content is a reflection of the seriousness with which you are approaching this issue" (Swan, 2019). |

| Organization | Official | Statement |
|---|---|---|
| U.K. Government | Rep. Max Rose | "We've seen in graphic detail the extent that terrorist organizations and extremists have used social media to amplify their reach and message in recent years. While social media companies tell us they're taking this seriously, I want to see the numbers to back that up—and won't stop until we get answers" (U.K. Government, 2019). |
| | Theresa May Spokeswoman | "Facebook, Twitter, YouTube and other providers have taken action to remove the video and other propaganda related to the attack. The government has been clear that all companies need to act more quickly to remove terrorist content. There should be no safe spaces for terrorists to promote and share their extreme views and radicalise others" (U.K. Government, 2019). |
| | UK Security Minister Ben Wallace | "Later today, the Home Secretary and I will be speaking to police counter-terrorism leaders and security services to discuss what further measures we can take to protect our mosques and our communities from any threat here in the United Kingdom" (U.K. Government, 2019). |
| | British Home Secretary Sajid Javid | "You really need to do more @YouTube @Google @facebook @Twitter to stop violent extremism being promoted on your platforms. Take some ownership. Enough is enough" (Spangler, 2019). |
| | Theresa May | "For too long these companies have not done enough to protect users, especially children and young people, from harmful content. That is not good enough, and it is time to do things differently. Online companies must start taking responsibility for their platforms, and help restore public trust in this technology" (Yahoo Finance, 2019).<br><br>Warned tech companies they had "not done enough" to protect users and that her government intended to put "a legal duty of care" on the firms "to keep people safe" (Yahoo Finance, 2019). |
| | Digital Secretary Jeremy Wright | "The era of self-regulation for online companies is over," and that "those that fail to do this will face tough action" (Yahoo Finance, 2019). |
| European Union Government | UK Government | "We are consulting on powers to issue substantial fines, block access to sites and potentially to impose liability on individual members of senior management" (Yahoo Finance, 2019). |
| | European Commission Vice President Andrus Ansip | "Companies are now assessing 89 percent of flagged content within 24 hours, and promptly act to remove it when necessary. This is more than twice as much when compared to 2016" (EU, 2019). |
| | European Commission for Justice Vera Jourova | "We have no signs that such content has decreased on social media platforms. But we do have signs that the Code of Conduct is a tool which can contribute to the robust response to the challenge" (EU, 2019). |

**Table 8**

*Statements by Social Media Platforms After a Terrorist Attack in New Zealand by a White Supremacist in 2019*

| Online platform | Official | Statement |
|---|---|---|
| Facebook | CEO Mark Zuckerberg | "Lawmakers often tell me we have too much power over speech, and frankly I agree. I've come to believe that we shouldn't make so many important decisions about speech on our own. So we're creating an independent body so people can appeal our decisions. We're also working with governments, including French officials, on ensuring the effectiveness of content review systems . . . "True data portability should look more like the way people use our platform to sign into an app than the existing ways you can download an archive of your information. But this requires clear rules about who's responsible for protecting information when it moves between services" (Forbes, 2019).<br>They banned "praise, support and representation of white nationalism and separatism" (Forbes, 2019). |
| | COO Sheryl Sandberg | Facebook was exploring restrictions about who can go on Live video based on factors like prior Community Standard violations. Facebook was also putting more resources towards systems that can identify violent content even if edited (Forbes, 2019). |
| | Director of Policy, Australia and New Zealand, Mia Garlick | "Police alerted us to a video on Facebook shortly after the livestream commenced and we quickly removed both the shooter's Facebook and Instagram accounts and the video. We're also removing any praise or support for the crime and the shooter or shooters as soon as we're aware. We will continue working directly with New Zealand police as their response and investigation continues" (Feiner, 2019). |
| Twitter | Spokesperson | "We are deeply saddened by the shootings in Christchurch today. Twitter has rigorous processes and a dedicated team in place for managing exigent and emergency situations such as this. We also cooperate with law enforcement to facilitate their investigations as required" (Feiner, 2019). |
| YouTube | Official statement | "Hate speech has no place on YouTube. We've invested heavily in teams and technology dedicated to removing hateful comments and videos and we take action on them when flagged by our users" (Rodrigo, 2019). |

**Statements and Terms of Conditions by Platforms in Response to the Multiple Cases**

Tables 9 and 10 (below) presented responses to terrorist misuse by the four social media platforms across cases. Table 9 shows the statements made by officials of social media companies after terrorist misuse of platforms. Table 10 shows the terms of service for each platform after terrorist misuse.

**Table 9**

*Statements by Social Media Platform Officials in Response to Terrorist Misuse of Social Media Platforms*

| Platform | Statement |
|---|---|
| YouTube/Google | June 21, 2017: "There should be no place for terrorist content on our services," wrote Kent Walker, Google's general council, while acknowledging Google, and the industry as a whole, needs to accelerate efforts to address it. "While we and others have worked for years to identify and remove content that violates our policies, the uncomfortable truth is that we, as an industry, must acknowledge that more needs to be done. Now" (Marvin, 2017).<br><br>June 18, 2017: "First, we are increasing our use of technology to help identify extremist and terrorism-related videos."<br>"Second, because technology alone is not a silver bullet, we will greatly increase the number of independent experts in YouTube's Trusted Flagger programme."<br><br>"Third, we will be taking a tougher stance on videos that do not clearly violate our policies — for example, videos that contain inflammatory religious or supremacist content."<br><br>"Finally, YouTube will expand its role in counter-radicalisation efforts. Building on our successful Creators for Change programme promoting YouTube voices against hate and radicalisation, we are working with Jigsaw to implement the "Redirect Method" more broadly across Europe" (Walker, 2017).<br><br>May 15, 2018: "The eight companies signing agreed to take specific measures to prevent uploading and sharing of "terrorist and violent extremist content." They also agreed to cooperate more with each other and governments, improve transparency around community standards and terms of service, and do more to enforce their own rules" (O'Brien, 2019).<br><br>September 20, 2017: "At the same time, we're elevating the voices that are most credible in speaking out against terrorism, hate, and violence. YouTube's Creators for Change program highlights online stars taking a stand against xenophobia and extremism" (Walker, 2017).<br><br>"Google and YouTube are committed to being part of the solution. We are working with government, law enforcement and civil society groups to tackle the problem of violent extremism online. There should be no place for terrorist content on our services" (Financial Times, n.d.).<br><br>January 7, 2018: Google's YouTube, meanwhile, said it continued to use what it called the "Redirect Method," developed by Google's Jigsaw research group, to send anti-terror messages to people likely to seek out extremist content through what was essentially targeted advertising (Shinal, 2018). |

| Platform | Statement |
|---|---|
| Twitter | February 5, 2016: "We have increased the size of the teams that review reports, reducing our response time significantly. We also look into other accounts similar to those reported and leverage proprietary spam-fighting tools to surface other potentially violating accounts for review by our agents. We have already seen results, including an increase in account suspensions and this type of activity shifting off of Twitter" (Twitter, 2016).<br><br>June 26, 2017: "Today, Facebook, Twitter and YouTube are announcing the formation of the Global Internet Forum to Counter Terrorism, which will help us continue to make our hosted consumer services hostile to terrorists and violent extremists" (Twitter, 2017).<br><br>September 4, 2018: "Twitter is approaching these challenges with a simple question: How do we earn more trust from the people using our service? We know the way to earn more trust around how we make decisions on our platform is to be as transparent as possible" (Kang & Frenkel, 2018).<br><br>June 10, 2019: "I think that there is content on Twitter and every [social media] platform that contributes to radicalization, no doubt. I also think we have a lot of mechanisms and policies in place that we enforce very effectively that combat this." – Vijaya Gadde, Head of Legal, Policy, and Trust (Ghaffary, 2019). |
| Facebook | June 15, 2017: "In a series of blog posts by senior figures and an interview with the BBC, Facebook says it wants to be more open about the work it is doing. The company told the BBC it was using artificial intelligence to spot images, videos and text related to terrorism as well as clusters of fake accounts" (Corera, 2017).<br><br>June 15, 2017: "Image matching: When someone tries to upload a terrorist photo or video, our systems look for whether the image matches a known terrorism photo or video. Language understanding: We have also recently started to experiment with using AI to understand text that might be advocating for terrorism. Removing terrorist clusters: We know from studies of terrorists that they tend to radicalize and operate in clusters. Recidivism: We've also gotten much faster at detecting new fake accounts created by repeat offenders. Cross-platform collaboration: Because we don't want terrorists to have a place anywhere in the family of Facebook apps, we have begun work on systems to enable us to take action against terrorist accounts across all our platforms, including WhatsApp and Instagram" (Facebook, 2017).<br><br>July 31, 2017: "And so when there are message services like WhatsApp that are encrypted, the message itself is encrypted but the metadata is not, meaning that you send me a message, we don't know what that message says, but we know you contacted me."<br><br>"If people move off those encrypted services to go to encrypted services in countries that won't share the metadata, the government actually has less information, not more" (Shaban, 2017).<br><br>March 29, 2019: "Sandberg, Facebook's chief operating officer, said the company is 'exploring' placing restrictions on who can live stream video on Facebook, but did not announce any actual policy changes."<br><br>January 17, 2018: "We believe that a key part of combating extremism is preventing recruitment by disrupting the underlying ideologies that drive people to commit acts of violence. That's why we support a variety of counter speech efforts," said Monika Bickert, Facebook's head of global policy management. Facebook is also working with universities, nongovernmental organizations and community groups around the world "to empower positive and moderate voices," Bickert said (Shinal, 2018). |

| Platform | Statement |
|---|---|
| Telegram | November 19, 2015: "I think that privacy, ultimately, and our right for privacy is more important than our fear of bad things happening, like terrorism. . . Ultimately, ISIS will find a way to communicate with its cells, and if any means doesn't feel secure to them, they'll [find something else]. We shouldn't feel guilty about it. We're still doing the right thing, protecting our users' privacy" (Kaplan, 2015).<br><br>November 16, 2019: "We support free speech and peaceful protest, but terrorist propaganda has no place on our platform. The success of our ongoing anti-ISIS efforts proves that you don't have to sacrifice privacy for security. You can – and should – enjoy both" (Durov, 2019).<br><br>March 13, 2016: "In our 100 million users, probably this illegal activity we're discussing are only a fraction of a fraction of a fraction of the potential usage. And still we're trying to, you know, prevent it… this is the world of technology and it's impossible to stop them at this point. ISIS could come up with their own messaging solution within a month or so, if they wanted to…" (Stahl, 2016).<br><br>August 30, 2018: "We previously had no real privacy policy and had to come up with one this summer to comply with. We haven't shared any terrorists' data with authorities yet, but our theoretical ability to do so is another measure we've taken to discourage terrorists from abusing our platform" (First Post, 2018). |

## Table 10

*Terms of Service Regarding Terrorist and Criminal Content for Each Platform, From Its Beginning to the Present*

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| YouTube/Google | May 17, 2021 to Present: "Hate speech is not allowed on YouTube. YouTube removes content promoting violence or hatred against individuals or groups based on any of the following attributes: Age, Caste, Disability, Ethnicity, Gender Identity and Expression, Nationality, Race, Immigration Status, Religion, Sex/Gender, Sexual Orientation, Victims of a major violent event and their kin, Veteran Status" (YouTube, 2019).<br><br>"YouTube doesn't allow content that encourages dangerous or illegal activities that risk serious physical harm or death" (YouTube, 2019). Including but not limited to:<br><br>"Violent Events: Promoting or glorifying violent tragedies, such as school shootings;<br><br>Instructions to kill or harm: Showing viewers how to perform activities meant to kill or maim others. For example, giving instructions to build a bomb meant to injure or kill others" (YouTube, 2019).<br><br>"Content intended to praise, promote, or aid violent criminal organizations is not allowed on YouTube. These organizations are not allowed to use YouTube for any purpose, including recruitment" (YouTube, 2019). Including:<br><br>"Content produced by violent criminal or terrorist organizations;<br><br>Content praising or memorializing prominent terrorist or criminal figures in order to encourage others to carry out acts of violence;<br><br>Content praising or justifying violent acts carried out by violent criminal or terrorist organizations;<br><br>Content aimed at recruiting new members to violent criminal or terrorist organizations;<br><br>Content depicting hostages or posted with the intent to solicit, threaten, or intimidate on behalf of a violent criminal or terrorist organization;<br><br>Content that depicts the insignia, logos, or symbols of violent criminal or terrorist organizations in order to praise or promote them" (YouTube, 2019).<br><br>December 27, 2018: Generally, the same terms of service as outlined in 2016 onward with the addition of:<br><br>"Violent or graphic content: It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or gratuitous. If posting graphic content in a news or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence" (YouTube, 2017).<br><br>"Harassment and cyberbully: It's not ok to post abusive videos and comments on YouTube. If harassment crosses the line into a malicious attack, it can be reported and may be removed. In other cases, users may be mildly annoying or petty and should be ignored" (YouTube, 2017).<br><br>October 15, 2016: "Community Guidelines":<br><br>"YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation (YouTube, 2017)." |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| YouTube/Google | "Our products are platforms for free expression. But we don't support content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these core characteristics. This can be a delicate balancing act, but if the primary purpose is to attack a protected group, the content crosses the line" (YouTube, 2017).<br><br>"Don't post videos that encourage others to do things that might cause them to get badly hurt, especially kids. Videos showing such harmful or dangerous acts may get age-restricted or removed depending on their severity" (YouTube, 2017).<br><br>"Things like predatory behavior, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information, and inciting others to commit violent acts or to violate the Terms of Use are taken very seriously. Anyone caught doing these things may be permanently banned from YouTube" (YouTube, 2017).<br><br>January 6, 2016: YouTube's "Community Guidelines" stated: "Violent or graphic content: It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or disrespectful... Don't encourage others to commit specific acts of violence" (Stalinsky et al., 2016).<br><br>December 13, 2014: Generally, the same terms of service as outlined in 2006 onward with the addition of: "Our products are platforms for free expression. But we don't support content that promotes or condones violence against individuals or groups based on race or ethnic origin, religion, disability, gender, age, nationality, veteran status, or sexual orientation/gender identity, or whose primary purpose is inciting hatred on the basis of these core characteristics. This can be a delicate balancing act, but if the primary purpose is to attack a protected group, the content crosses the line" (YouTube, 2017).<br><br>April 9, 2013: Sarah Hunter, a Google representative, said that Google "in no way condone[s] the use of YouTube for terrorist content, and to that end we have very, very strict community guidelines on YouTube that go way beyond the law… it is not allowed on YouTube to post content that is inciting violence; it is not allowed to post content that is hate speech. When a user flags to us that there is content up on there that is breaking those guidelines, we review that content and we take it down, and these flags get reviewed within an hour" (Stalinksy & Zweig, 2013).<br><br>June 13, 2011: Generally, the same terms of service as outlined in 2006 onward with the addition of:<br><br>"Things like predatory behavior, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information, and inciting others to commit violent acts or to violate the Terms of Use are taken very seriously. Anyone caught doing these things may be permanently banned from YouTube" (YouTube, 2017).<br><br>August 2, 2010: Generally, the same terms of service as outlined in 2006 onward with the addition of "Community Guideline Tips:" Included but was not limited to:<br><br>"'Hate speech' refers to content that promotes hatred against members of a protected group. For instance, racist or sexist content may be considered hate speech. Sometimes there is a fine line between what is and what is not considered hate speech. For instance, it is generally okay to criticize a nation, but not okay to make insulting generalizations about people of a particular nationality" (YouTube, 2017).<br><br>"Dangerous Illegal Acts: While it might not seem fair to say you can't show something because of what viewers theoretically might do in response, we draw the line at content that's intended to incite violence or encourage dangerous, illegal activities that have an inherent risk of serious physical harm or death. This means not posting videos on things like instructional bomb making, ninja assassin training, sniper attacks, videos that train terrorists, or tips on illegal street racing. Any depictions like these should be educational or documentary and shouldn't be designed to help or encourage others to imitate them" (YouTube, 2017). |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| YouTube/Google | July 1, 2010: YouTube's terms of service stated that videos "…inciting others to commit violent acts…" can be flagged and that to do so viewers should follow these steps: Go to YouTube's home page, www.YouTube.com; using the "flag" button beneath the video player, flag the objectionable video (you must be a YouTube member to flag a video); once you have "flagged" the video, a drop-down menu will allow you to select the "reason" you flagged it; click "submit" (Stalinsky, 2010).<br><br>December 14, 2007: "YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation" (YouTube, 2017).<br><br>"Don't post videos showing bad stuff like animal abuse, drug abuse, or bomb making" (YouTube, 2017).<br><br>"Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it (YouTube, 2017)."<br><br>"YouTube is not a shock site. Don't post gross-out videos of accidents, dead bodies and similar things" (YouTube, 2017).<br><br>"We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech, which is content intended to attack or demean a particular gender, sexual orientation, race, religion, ethnic origin, veteran status, color, age, disability or nationality" (YouTube, 2017).<br><br>"There is zero tolerance for predatory behavior, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube" (YouTube, 2017).<br><br>October 24, 2006: "YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation" (YouTube, 2017).<br><br>"Don't post videos showing dangerous or illegal acts, like animal abuse or bomb making" (YouTube, 2017).<br><br>"Real violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it" (YouTube, 2017).<br><br>"YouTube is not a shock site. Don't post gross-out videos of accidents, dead bodies and stuff like that. This includes war footage if it's intended to shock or disgust" (YouTube, 2017).<br><br>"We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech which contains slurs or the malicious use of stereotypes intended to attack or demean a particular gender, sexual orientation, race, religion, or nationality" (YouTube, 2017).<br><br>"There is zero tolerance for predatory behavior, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube" (YouTube, 2017). |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| Twitter | August 19, 2021, to Present: "We reserve the right to remove Content that violates the User Agreement, including for example, copyright or trademark violations or other intellectual property misappropriation, impersonation, unlawful conduct, or harassment" (Twitter, 2021). Including but not limited to:<br><br>"Violence: You may not threaten violence against an individual or a group of people. We also prohibit the glorification of violence;<br><br>Terrorism/violent extremism: You may not threaten or promote terrorism or violent extremism"<br><br>Abuse/harassment: You may not engage in the targeted harassment of someone, or incite other people to do so. This includes wishing or hoping that someone experiences physical harm" (Twitter, 2021).<br><br>"Hateful conduct: You may not promote violence against, threaten, or harass other people on the basis of race, ethnicity, national origin, caste, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease" (Help Center, 2022).<br><br>December 28, 2017: Generally, the same terms of service as outlined in 2016 onward with the addition of:<br><br>"Violence: You may not make specific threats of violence or wish for the serious physical harm, death, or disease of an individual or group of people. This includes, but is not limited to, threatening or promoting terrorism. You also may not affiliate with organizations that — whether by their own statements or activity both on and off the platform — use or promote violence against civilians to further their causes;<br><br>Abuse: You may not engage in the targeted harassment of someone, or incite other people to do so. We consider abusive behavior an attempt to harass, intimidate, or silence someone else's voice;<br><br>Hateful conduct: You may not promote violence against, threaten, or harass other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease;<br><br>Hateful imagery and display names: You may not use hateful images or symbols in your profile image or profile header. You also may not use your username, display name, or profile bio to engage in abusive behavior, such as targeted harassment or expressing hate towards a person, group, or protected category" (Help Center, 2017).<br><br>December 7, 2016: Addition of "Abusive Behavior" in Twitter Rules:<br><br>"Any accounts and related accounts engaging in the activities specified below may be temporarily locked and/or subject to permanent suspension" (Help Center, 2010)."Violent threats (direct or indirect): You may not make threats of violence or promote violence, including threatening or promoting terrorism" (Help Center, 2010).<br><br>"Harassment: You may not incite or engage in the targeted abuse or harassment of others. Some of the factors that we may consider when evaluating abusive behavior include:<br><br>If a primary purpose of the reported account is to harass or send abusive messages to others;<br><br>If the reported behavior is one-sided or includes threats;<br><br>If the reported account is inciting others to harass another account;<br><br>If the reported account is sending harassing messages to an account from multiple accounts" (Help Center, 2010). "Hateful conduct: You may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease. We also do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories" (Help Center, 2010). |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| Twitter | January 6, 2016: Twitter's "Rules" stated: "Violent threats (direct or indirect): Users may not make threats of violence or promote violence, including threatening or promoting terrorism. Users also may not make threats or promote violence against a person or group on the basis of race, ethnicity, national origin, religion, sexual orientation, gender, gender identity, age, or disability" (Stalinsky et al., 2016).<br><br>August 1, 2014: Any "person barred from receiving services under the laws of the U.S." may not hold a Twitter account. (Memri, 2014)<br><br>December 30, 2013: Generally, the same terms of service as outlined in 2010 onward with the addition of:<br><br>"Targeted Abuse: You may not engage in targeted abuse or harassment. Some of the factors that we take into account when determining what conduct is considered to be targeted abuse or harassment are:<br><br>If you are sending messages to a user from multiple accounts;<br><br>If the sole purpose of your account is to send abusive messages to others;<br><br>If the reported behavior is one-sided or includes threats" (Twitter, 2010).<br><br>December 29, 2011: According to Twitter's Terms of Service, account holders could use the Services only if "you [the user] can form a binding contract with Twitter and are not a person barred from receiving services under the laws of the United States or other applicable jurisdiction" (Stalinsky, 2011). Its "Restrictions on Content" stated "We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services and to terminate users or reclaim usernames... We also reserve the right to... enforce the Terms, including investigation of potential violations hereof." Twitter also provided readers with the option to report violations. Twitter's Terms of Service did not ban designated terrorist groups, which were increasingly active on it, but focused instead on trademark violations, breaches of privacy, child pornography, copyright issues, harassment and violent threats, impersonation, and "name squatting." (Stalinsky, 2011)<br><br>November 2, 2010: "Violence and Threats: You may not publish or post direct, specific threats of violence against others" (Twitter, 2010).<br><br>"You may not use our service for any unlawful purposes or for promotion of illegal activities. International users agree to comply with all local laws regarding online conduct and acceptable content" (Twitter, 2010).<br><br>"Your account may be suspended for Terms of Service violations if any of the above is true" (Twitter, 2010). |
| Facebook | Present: "You may not use Facebook to do or share anything:"<br><br>"That violates these Terms, our Community Standards, and other terms and policies that apply to your use of Facebook."<br><br>"Threats that could lead to death (and other forms of high-severity violence) targeting people or places" (Meta, 2022).<br><br>"We expect that people will respect the dignity of others and not harass or degrade others" (Meta, 2022).<br><br>"We remove Praise, Substantive Support, and Representation of various Dangerous Organizations" (Meta, 2022).<br><br>"Do not post content that harms people, animals, property, voter interference" (Meta, 2022).<br><br>"That is unlawful, misleading, discriminatory, or fraudulent" (Meta, 2022).<br>"That infringes or violates someone else's rights, including their intellectual property rights" (Facebook, 2022). |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| Facebook | "That infringes or violates someone else's rights, including their intellectual property rights" (Facebook, 2022).<br><br>December 31, 2019: "Combat harmful conduct and protect and support our community: People will only build community on Facebook if they feel safe. We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, removing or restricting access to certain features, disabling an account, or contacting law enforcement. We share data with other Facebook Companies when we detect misuse or harmful conduct by someone using one of our Products" (Facebook, 2022).<br><br>December 2, 2013: Generally, the same terms of service as outlined in 2006 onward with the revision of:<br><br>"You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence" (Facebook, 2022).<br><br>January 1, 2013: "Safety is Facebook's top priority. We remove content and may escalate to law enforcement when we perceive a genuine risk of physical harm, or a direct threat to public safety. You may not credibly threaten others, or organize acts of real-world violence. Organizations with a record of terrorist or violent criminal activity are not allowed to maintain a presence on our site. We also prohibit promoting, planning or celebrating any of your actions if they have, or could, result in financial harm to others, including theft and vandalism" (Facebook, 2011).<br><br>"Facebook does not permit hate speech, but distinguishes between serious and humorous speech. While we encourage you to challenge ideas, institutions, events, and practices, we do not permit individuals or groups to attack others based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or medical condition" (Facebook, 2011).<br><br>December 31, 2012: "You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law" (Facebook, 2022).<br><br>December 31, 2009: Generally, the same terms of service as outlined in 2006 onward with a restructure of the guidelines and the addition of:<br><br>"You will not bully, intimidate, or harass any user;<br><br>You will not post content that is hateful, threatening, pornographic, or that contains nudity or graphic or gratuitous violence;<br><br>You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory. Etc.;<br><br>You will not facilitate or encourage any violations of this Statement" (Facebook, 2005).<br><br>December 30, 2006: Generally, the same terms of service as outlined in 2005 onward with the addition of:<br><br>"You agree not to… upload, post, transmit, share, store or otherwise make available content that would constitute, encourage or provide instructions for a criminal offense, violate the rights of any party, or that would otherwise create liability or violate any local, state, national or international law" (Facebook, 2005).<br><br>December 30, 2005: "You agree not to use the Web site to:"<br><br>"Upload, post, email, transmit or otherwise make available any content that we deem to be harmful, threatening, abusive, harassing, vulgar, obscene, hateful, or racially, ethnically or otherwise objectionable;<br><br>Intimidate or harass another" (Facebook, 2005). |

| Platform | Terms of service regarding terrorist/criminal content |
|---|---|
| Telegram | Present: Telegram's terms of service in 2021 was identical to its terms of service in 2018 (Telegram, 2022). |

May 19, 2018: “By signing up for Telegram, you agree not to:

Use our service to send spam or scam users.

Promote violence on publically viewable Telegram channels, bots, etc.

Post illegal pornographic content on publically viewable Telegram channels, bots, etc.” (Telegram, 2018).

**Emerging Themes and Subthemes**

From the aggregation of the data, six themes emerged among existing responses to terrorist misuse. Tables 11 and 12 showed the themes that emerged in the responses by government leaders and online platforms, respectively. In Table 11, the data highlighted the desire of numerous international governments for social media platforms to be better prepared to control content on their platforms and respond to active shooter situations. Government leaders urged change in six general ways: government collaboration with online platforms, a "new era" of regulation, the responsibility that lies on the shoulders of online platforms, the ability of online platforms to remove content, the imposition of consequences on online platforms, and company policies and policy changes.

**Table 11**

*Themes of Statements by Governments Concerning Online Platforms in Reaction to a Terrorist Attack on Christchurch, New Zealand*

| Theme | Australia | New Zealand | United States | United Kingdom | European Union |
|---|---|---|---|---|---|
| Government Collaboration with Online Platforms | ✓ | ✓ | ✓ | | |
| "New Era" of Regulation | | | ✓ | ✓ | |
| Online Platforms Must Take Greater Responsibility | | ✓ | ✓ | ✓ | |
| Online Platforms' Ability to Remove Content | ✓ | ✓ | | ✓ | ✓ |
| Imposing Consequences on Online Platforms | | | | ✓ | ✓ |
| Platform Policies And Policy Changes | | | ✓ | | |

*Note*. From MEMRI. (2019). *New Zealand Attack On Social Media – Companies Pressed For Statements.* (Internal Report). Reprinted with permission.

In Table 12 (below), the data emphasized social media platforms' desire to improve their policing methods and abilities to survey the content on their platforms. Two themes emerged from this data: government collaboration with online platforms and platform policies and policy changes. Following Table 12 were summaries of the emerging themes.

**Table 12**

*Themes of Corporate Statements by Online Platforms After a Terrorist Attack on Christchurch, New Zealand*

| Theme | Facebook | Twitter | YouTube |
|---|---|---|---|
| Government Collaboration with Online Platforms | ✓ | | |
| "New Era" of Regulation | | | |
| Online Platforms Taking Greater Responsibility | | | |
| Online Platforms' Ability to Remove Content | | | |
| Imposing Consequences on Online Platforms | | | |
| Platform Policies and Policy Changes | ✓ | ✓ | ✓ |

*Note*. From MEMRI. (2019). *New Zealand Attack On Social Media – Companies Pressed For Statements.* (Internal Report). Reprinted with permission.

Further data analysis and visualizations supported the findings. In Figure 1 below, a word cloud was generated to display most the frequent terms that were repeated and stressed throughout the collected data. The most dominant sub-themes that appeared were as follows: online, policies, data, issues, incitement, protection, instrument, human, and rules.

**Figure 1**

*Word Cloud Using NVivo of the Most Frequent Terms in the Data Set*


The visualization of complete coding hierarchy was presented in Figure 2, which depicted the content coverage of major and sub-themes. The top theme with the most coverage was “Platform Policies and Policy Changes.” Two themes that also covered more area in relation to industry policies and social media platforms were “Online

Platforms Must Take Greater Responsibility" and "Online Platforms' Ability to Remove Content." The theme with the least coverage was "government collaboration with online platforms."

**Figure 2**

*Coding Hierarchy Using NVivo Based on Complete Themes*

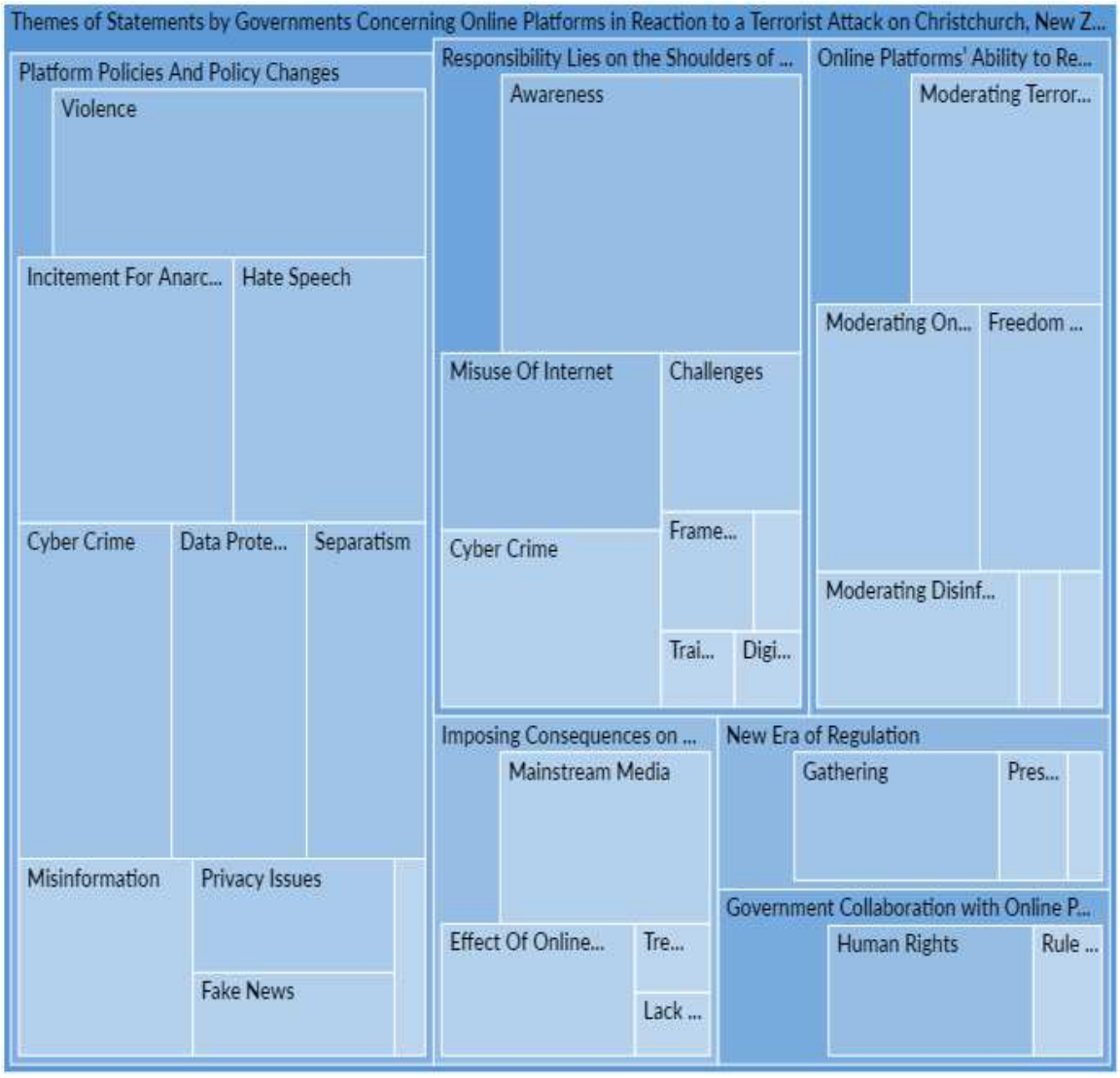
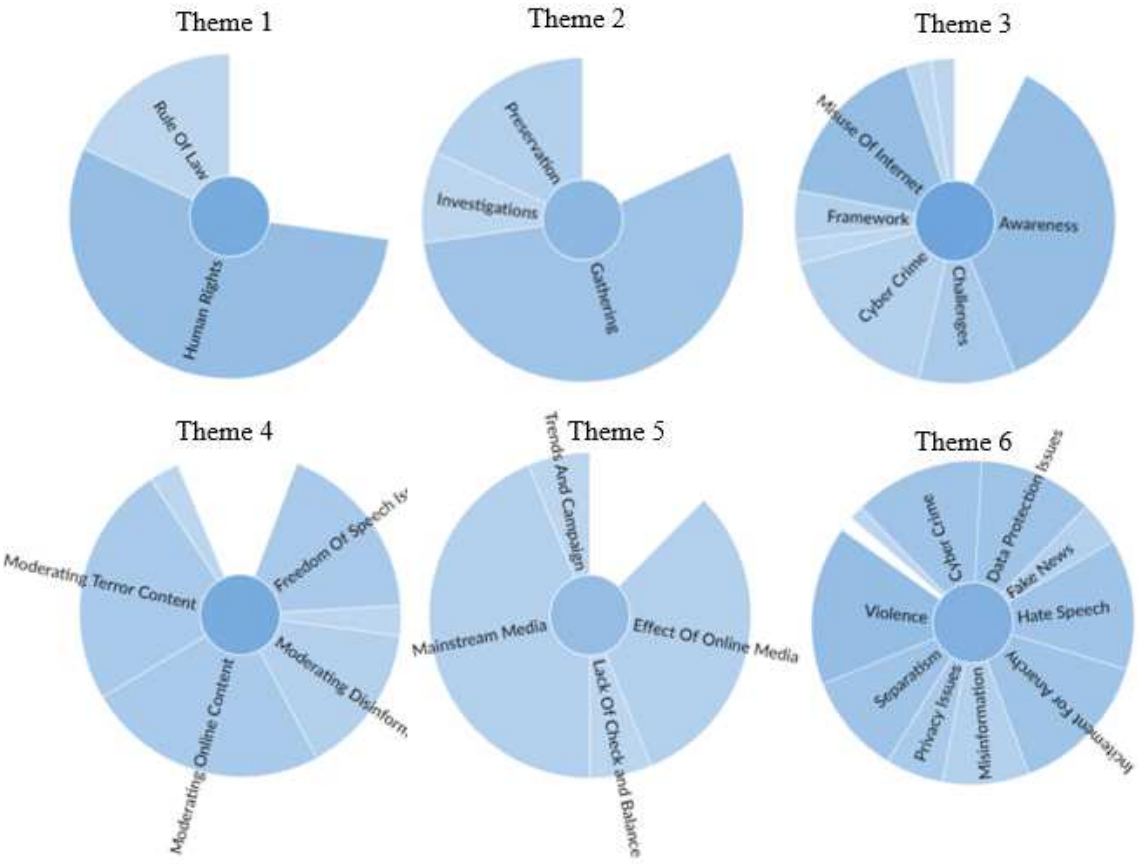


Figure 3 demonstrated the coverage of content of sub-themes under the major themes. A coding hierarchy was performed to explore the extent to sub-themes composed the six themes: (1) government collaboration with online platforms, (2) a "new era" of regulation, (3) online platforms taking greater responsibility, (4) online platforms' ability to remove content, (5) imposing consequences on online platforms, and (6) platform policies and policy changes. Theme 6, "Platform Policies and Policy Changes," was found to comprise more sub-themes than the other themes. Theme 6 was spread more broadly among content than other themes. It also included more of the major sub-themes. Theme 1, "Government Collaboration with Online Platforms," covered the least area.

**Figure 3**

*Coding Hierarchy Using NVivo of Themes Based on Subthemes*




## Development of Industry Policies from Emerging Themes

### Emerging Theme 1: Government Collaboration with Online Platforms

The data showed that government officials want to collaborate with and hold accountable social media platforms in solving the problem of terrorist misuse of social media. For example, on May 15, 2019, two months after the attack in Christchurch in which a gunman killed 51 worshippers at mosques, New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron led a group of world leaders, tech companies, and organizations to adopt the Christchurch Call to Action to Eliminate

Terrorist and Violent Extremist Content Online (Arden, 2019). The same day, Amazon, Facebook, Google, and Twitter issued a joint statement regarding the call, stating that it "expands on the Global Internet Forum to Counter Terrorism (GIFCT), and builds on our other initiatives with government and civil society to prevent the dissemination of terrorist and violent extremist content" (Microsoft, 2019, para. 3)

On February 18, 2020, New Zealand launched its Countering Terrorism and Violent Extremism Strategy, with an expanded version released June 15, 2021 (Department of the Prime Minister and Cabinet, 2020). On May 15, 2019, New Zealand Prime Minister, Jacinda Ardern, and French President, Emmanuel Macron brought together leaders from other countries and the tech sector to adopt the Christchurch Call, a commitment by Governments and tech companies to eliminate terrorist and violent extremist content online (Christchurch Call, n.d.). On May 7, 2021, the White House announced that it was joining the call. As of May 2021, the call was supported by more than 50 countries and international organizations, including UNESCO and the Council of Europe, as well as 10 major tech companies (Microsoft, 2019). Australian Prime Minister Scott Morrison expressed his desire for social media platforms to come to the table as "responsible corporate citizens" (Barbaschow, 2019, para. 11). New Zealand Prime Minister Jacinda Ardern said she would talk directly with Facebook officials about how the Christchurch attacks were able to be live-streamed (Digital Team, 2019).

Additionally, Rep. Bennie G. Thompson, Chairman of the House Homeland Security Committee, wrote letters to the heads of major tech companies on March 19, requesting regarding a briefing on March 27, 2019, about their response to Tarrant's live

stream and subsequent re-uploads that went viral. The letter was sent to Facebook CEO Mark Zuckerberg, YouTube CEO Susan Wojcicki, Twitter CEO Jack Dorsey, and Microsoft CEO Satya Nadella. The letter urged the platforms to prioritize the removal of the terrorist content and to brief the committee on their response and plans to prevent something similar from happening in the future (Birnbaum, 2019).

The data also showed that social media platforms were responsive to the comments and calls to action by lawmakers and government officials. Facebook CEO Mark Zuckerberg broadly explained,

> Lawmakers often tell me we have too much power over speech, and frankly I agree. I've come to believe that we shouldn't make so many important decisions about speech on our own. So we're creating an independent body so people can appeal our decisions. We're also working with governments, including French officials, on ensuring the effectiveness of content review systems. (Chowdhry, 2019, para. 3)

In response to comments specific to the New Zealand attack, Mia Garlick of Facebook's New Zealand office said,

> Police alerted us to a video on Facebook shortly after the livestream commenced and we quickly removed both the shooter's Facebook and Instagram accounts and the video. We're also removing any praise or support for the crime and the shooter or shooters as soon as we're aware. We will continue working directly with New Zealand police as their response and investigation continues. (Feiner, 2019, para. 7)

**Emerging Theme 2: "New Era" of Regulation**

The data showed that lawmakers were increasing pressure on social media platforms through regulatory measures to protect citizens from the misuse of social media (Yahoo Finance, 2019). Speaker Nancy Pelosi voiced support for a "new era" of regulation of tech companies (Birnbaum, 2019). On April 9, 2019, US Senator Mark Warner teamed with Senator Deb Fischer to introduce a bill to block major online technology firms from deceiving people to give personal data to platforms. On April 11, 2019, Warner said he was eyeing additional bills focused on limiting hate speech.

Warner noted the real implications that result from this type of hate speech, citing the shootings in Christchurch and Pittsburgh. "I want technology to stay. I want the social media platforms to stay. But I do think the days of the Wild Wild West where anything goes, people just aren't going to allow it" (Bartz, 2019, para. 12).

**Emerging Theme 3: Responsibility Lies on the Shoulders of Online Platforms**

The data showed that government officials were looking to social media platforms to bear the responsibility of solving the problem of terrorist attacks related to misuse of social media. Following the New Zealand attack, British Prime Minister Theresa May stated:

> For too long these companies have not done enough to protect users, especially children and young people, from harmful content. That is not good enough, and it is time to do things differently. Online companies must start taking responsibility for their platforms, and help restore public trust in this technology. (Yahoo Finance, 2019, para. 7)

British Home Secretary Sajid Javid tweeted: "You really need to do more @YouTube @Google @facebook @Twitter to stop violent extremism being promoted on your platforms. Take some ownership. Enough is enough" (Spangler, 2019, para. 10). In addition, New Zealand Prime Minister Jacinda Ardern said tech companies had "a lot of work" to do to curb the proliferation of content that incites hate and violence (Digital Team, 2019, para. 14).

**Emerging Theme 4: Online Platforms' Ability to Remove Content**

The ability of social media platforms to remove terrorist content was a frequent topic of discussion in response to misuse of social media. On March 26, 2019, the Australian government met with social media platforms that had a presence in Australia, and Australian Prime Minister Scott Morrison said:

> We want the same rules to apply in the online social media world that exist in the physical world. Building and making it safe means you can't let a terrorist atrocity be filmed and up and posted and streamed and be online for 69 minutes – 69 minutes – that's not acceptable, that has to change. They can get an ad to you in half a second; they should be able to pull down this sort of terrorist material and other types of very dangerous material in the same sort of time frame. (Barbaschow, 2019, para. 14)

Following the New Zealand attack, on March 15, 2019, Theresa May's spokeswoman stated,

> Facebook, Twitter, YouTube and other providers have taken action to remove the video and other propaganda related to the attack. The government has been clear

> that all platforms need to act more quickly to remove terrorist content. There should be no safe spaces for terrorists to promote and share their extreme views and radicalise others. (U.K. Government, 2019)

On April 1, 2019, EU officials praised the progress made by social media platforms since 2016. Andrus Ansip, European Commission Vice President stated: "Companies are now assessing 89 percent of flagged content within 24 hours, and promptly act to remove it when necessary. This is more than twice as much when compared to 2016" (D.W., 2019, para 2). On the same day as the attacks, UK Security Minister Ben Wallace said: "Later today, the Home Secretary and I will be speaking to police counter-terrorism leaders and security services to discuss what further measures we can take to protect our mosques and our communities from any threat here in the United Kingdom" (Parveen & Dodd, 2019).

**Emerging Theme 5: Imposing Consequences on Online Platforms**

While platforms made a lot of progress in the removal of content, the data showed that governments expect more progress to be made by social media platforms. The UK government stated: "We are consulting on powers to issue substantial fines, block access to sites and potentially to impose liability on individual members of senior management" (Yahoo Finance, 2019, para. 11). Theresa May warned tech companies they had "not done enough" to protect users and that her government intended to put "a legal duty of care" on the firms "to keep people safe" (Yahoo Finance, 2019, para. 4). Further, European Commission for Justice Vera Jourova said: "We have no signs that such content has decreased on social media platforms. But we do have signs that the Code of

Conduct is a tool which can contribute to robust response to the challenge" (D.W., 2019 para. 4).

**Emerging Theme 6: Social Media Platforms Respond With Policy Changes**

The data showed that the social media platforms responded to the Christ Church, New Zealand attack with policies and policy changes, which set the stage for future policies and industry standards. It was evident that the New Zealand shooting was a turning point in the problem of terrorist misuse of social media platforms. On March 15, 2019, 28-year-old Brenton Tarrant attacked two mosques, killing 50 and wounding 50 others in a shooting as he streamed the shootings on Facebook Live. The responses from platforms highlighted the commitment of social media companies to removing terrorist content from their platforms.

In a letter, Facebook COO Sheryl Sandberg addressed what Facebook would do in response to the New Zealand shooting. Sandberg stated that the platform was exploring restrictions about who can go on Live video based on factors like prior Community Standard violations. According to Sandberg, Facebook was also putting more resources towards systems that can identify violent content even if edited (Forbes, 2019).

In late March 2019, Facebook further announced that they would ban "praise, support and representation of white nationalism and separatism" (Chowdhry, 2019, para. 7). This announcement was made after talking with civil society members and race relations experts in the wake of the Christchurch shootings. Facebook CEO Mark Zuckerberg stated that there needs to be a universal common framework for privacy and

data protection, and said that more countries should adopt a regulation framework in line with the General Data Protection Regulation in the European Union.

Zuckerberg added that regulation should guarantee the principle of data portability, meaning that data shared with one service should be able to be moved to another service. Zuckerberg stated,

> True data portability should look more like the way people use our platform to sign into an app than the existing ways you can download an archive of your information. But this requires clear rules about who's responsible for protecting information when it moves between services. (Forbes, 2019, para. 6)

A Twitter spokesperson, in response to the shootings on March 15, 2019, stated,

> We are deeply saddened by the shootings in Christchurch today. Twitter has rigorous processes and a dedicated team in place for managing exigent and emergency situations such as this. We also cooperate with law enforcement to facilitate their investigations as required. (Feiner, 2019, para. 5)

In response to many comments in support of the Christchurch, New Zealand attack, YouTube stopped its livestream of the House Judiciary Committee on white nationalism. In a statement, You Tube said: "Hate speech has no place on YouTube. We've invested heavily in teams and technology dedicated to removing hateful comments and videos and we take action on them when flagged by our users" (Rodrigo, 2019, para. 3). On its Twitter account, YouTube posted the following on March 15, 2019, after the shooting: "Our hearts are broken over today's terrible tragedy in New Zealand.

Please know we are working vigilantly to remove any violent footage" (Serrels, 2019, para. 9).

## Summary

Chapter 4 discussed the process of data collection and analysis of the research study, including evidence of trustworthiness. The results were organized according to four case studies that examined the existing responses to terrorists' misuse of four social media platforms. Emerging themes were presented as figures and tables.

Six themes that emerged from the data were: government collaboration with online platforms, a "new era" of regulation, online platforms taking greater responsibility, online platforms' ability to remove content, imposing consequences on online platforms, and platform policies and policy changes. The six themes were further examined to identify sub-themes. Based on the analysis, the findings suggested the six emerging themes can be used to develop industry policies from existing responses and policies to misuse of social media. The six themes revealed the areas in which the industry could focus its attention to form standardized responses to the misuse of social media by terrorists.

The next chapter presents the interpretation of the findings. It also discusses limitations that arose and recommendations for further research. Chapter 5 concludes by providing implications for positive social change.

# Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of the study was to develop long overdue industry standards based on existing platform policies so that social media platforms can respond to the misuse of their services by terrorists. The following questions guided the study:

RQ1: What were the existing responses to terrorists' misuse of social media platforms?

RQ2: Could industry policies be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists?

This study was qualitative multiple case in nature. I sought to understand and inform the decision-making processes of social media platforms to mitigate the online culture of terrorist groups, which depend on social media platforms for global growth (Pacheco-Vega, 2020). I conducted a systematic review of the terms of service, policies, and precedents of social media platforms. The review addressed approaches by the world's leading SDOs as well as organizational software for classifying and arranging content. The aim was to develop industry policies based on insights and commonalities that can equip social media platforms with standardized industry responses, thereby hindering the growth of terrorist groups.

Six themes emerged that could be used to develop industry policies from existing responses and policies to prevent the misuse of social media. The six themes revealed the areas in which the social media and technology industry could focus its attention to form standardized responses to the misuse of social media platforms by terrorists. Preventing the misuse of social media platforms by terrorists could lead to positive social change.

## Interpretation of the Findings

The peer-reviewed literature reviewed in Chapter 2 revealed key variables and concepts related to the problem of inadequate industry policies by platforms in response to terrorist misuse of social media. The findings of this qualitative multiple case study confirmed and disconfirmed various areas of the peer-reviewed literature. Findings also extended the knowledge of some aspects of the literature.

### Findings Confirming Peer-Reviewed Literature

Findings confirmed four key concepts in the peer-reviewed literature. First, the emergence of terrorist use of the Internet that was documented in the 1990s showed that cyber jihad quickly gained momentum as the most important weapon for the growth of terrorist groups (Denning, 1999; Fielding, 2008; MEMRI Cyber & Jihad Lab, 2011; Weimann, 2006). Scholars shifted their attention to extremist groups, including studying the roles of governments and organizations in response to the emerging threat, and extremist groups' use of cyber jihad remains the primary focus of researchers' attention today. Second, early studies of cyber terrorism predicted the nefarious uses of the internet by terrorist groups against Western nations and their citizens (Furnell & Warren, 1999). By 2002, researchers had detailed four observable uses evident today: propaganda, fundraising, information dissemination, and secure communications (Arquilla & Ronfeldt, 2001; Bunt, 2003; Cohen, 2002; Furnell & Warren, 1999; Rogan, 2006; Weimann, 2006).

Third, early studies on cyber jihad underscored the fast pace at which the technologies and cyber jihad strategies progressed from low to high numbers of users and

from private websites of terrorist organizations to social media platforms. As was evident in the current study, social media platforms such as Facebook, Telegram, Twitter, and YouTube served as the preferred channels of choice for terrorists (Rogan, 2006). Fourth, the gap between social media policy guidelines and industry standards in addressing terrorist content still existed (Cohen-Almagor, 2013). Earlier researchers noted the use of social media platforms and encryption as integral parts of terrorist communication, particularly recruitment for terrorist organizations and activities related to terrorist attacks, but the literature lacked detailed information on exact actions and responses to these terrorist communications and activities (Ahlberg, 2014; Klausen, 2014; Weimann, 2014). The speculations came to fruition but remained a problem without a resolution.

**Findings Disconfirming Peer-Reviewed Literature**

Findings disconfirmed two concepts that were studied in peer-reviewed literature, both of which were controversial. First, in diverging thoughts on what to do with terrorist content, some believed that allowing jihadist content to remain online was beneficial for three reasons: providing a large amount of information about the movement as a means to collect intelligence, creating a systematic understanding of the jihadist, and preventing terrorist attacks (Rogan, 2006). They argued that in preventing online jihadist content, a remarkable amount of information was lost. However, the level of scrutiny on social media platforms and the demand for immediate removal of terrorist content today did not allow for this line of thought (Rogan, 2006).

Another controversial aspect in the literature was the blaming of U.S. leadership for its historical lack of effective response to terrorists' use of the internet. As Arquilla

(2009) pointed out, this omission was more than the U.S. presidents alone, as none of the key military, intelligence, and law-enforcement arms of the U.S. government did enough to curtail terrorist use of the internet. One report recommended a close working relationship between the U.S. administration and social media platforms to develop resources that would accelerate the removal of extremist content that violated their terms of service (Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel, 2015). *The Economist* (2017) concurred, arguing for transparent cooperation with lawmakers and stating that the exploitation of the free internet by jihadis indicated a need to regulate an industry that was previously unregulated, a necessity that would create new problems and responsibilities for firms.

However, the pinning of blame and the relationship between the government and social media platforms became more complex. Although Western government officials acknowledged the problem of terrorist misuse of social media, it was evident in panel remarks, speeches, interviews, and media statements that government representatives held social media platforms responsible for the continuing problem of cyber jihad. Criticism by politicians of platforms increased, including the accusation that platforms prioritized profit ahead of their responsibility to the community (Adapting to defend the homeland against the evolving international terrorist threat, 2017; Bennet & Williams, 2015; Chalfant, 2017; Jones et al., 2017; Perez, 2017; Sperry, 2015; The White House: President Barack Obama, 2015; Travis, 2017; Washington Post, 2015). Additionally, citizens filed lawsuits against social media companies because those platforms were used by terrorists in attacking them or their loved ones. The lawsuits by citizens underscored

the prevailing thought that platforms bore the responsibility of taking sufficient action to remove terrorist content (*The Economist*, 2017).

**Findings Extending the Knowledge of Peer-Reviewed Literature**

The findings extended the knowledge of peer-reviewed literature necessary for social media platforms to develop responses to terrorist misuse of their services (see Twitter, 2012). This study's findings established a connection between social media and terrorist attacks, and how platforms took action in response to this relationship; however, many of the corporate efforts were met with criticism or were proven inconclusive or ineffective, as censored terrorists continually created new accounts (see Lewis, 2015). My findings advanced the efforts of platforms to leverage their commonalities and make advancements together as an industry, such as through initiatives such as the GIFCT, the anti-terrorist formation of Facebook, Twitter, and YouTube that was undermined by insufficient resources and terrorists finding new ways to circumvent rules (see Levin, 2017).

The current study also extended the prevailing thought that social platforms were less a place to gather intelligence and more appropriately approached as a battlespace (see Rogan, 2006). In the context of the SMT framework, the findings added to one of the most complete frameworks used by researchers in examining terrorism, including the process of radicalization and violent extremism. The current study revealed the critical role of social media platforms in mitigating the development of terrorist groups (see Metzger, 2014). Findings also reflected the movement of terrorist groups and the correlating responses by platforms in interrupting the life cycle of terrorist growth.

The findings supported the joint battles against terrorist misuse of social media platforms that were waged by Europol's Internet Referral Unit and members of Internet Referral Units from Belgium, France, and the United Kingdom through Referral Action Day, an effort to remove terrorist and violent extremism content uploaded on Facebook and Instagram. The study may contribute to future joint actions in the early stages of development by the EU in conjunction with social media platforms to combat cyber jihad (see Eurpol, 2018). Additionally, the findings may help reinforce the groundwork established by research organizations and nongovernmental organizations (NGOs) for relatively new industries such as social media in dealing with terrorist activity on its platforms. In conjunction with best practices by The National Institute of Standards and Technology (NIST, n.d.) and the System Audit Network Security Institute (SANS, n.d.), platforms may use the findings to develop industry standards in the technology realm. These standards may make it easier and cheaper for platforms to provide technology securely.

## Limitations of the Study

There were six limitations to trustworthiness that arose from the execution of this study. The limitations involved the participant group and the industry that the study aimed to impact. Limitations were also inherent in the study methodology.

Regarding the limitations of the participant group, the four platforms varied in the levels of misuse of social media and encryption services by terrorists. The levels of mitigation by platforms also varied; their willingness and/or ability to track and react to the misuse of their services influenced the impact of this study. The limitations of an

inherently fast-paced industry included the continual change that could impact a platform's ability and resources to proactively track and/or respond to the misuse of their services. The fast pace of the industry also constrained the time frame of this study. Another limitation of this study was its design; the multiple case study relied on the four largest social media platforms as the best sources for existing responses to terrorist misuse of services, and the study focused on the misuses of social media and the existing response to those misuses at a certain point in time.

I addressed issues of trustworthiness in five ways. First, data were downloaded directly from the websites of the participants to ensure that any industry standards resulting from the study resonated with the participants for practical implementation. Second, data saturation was achieved by selecting critical cases and industry leaders as participants and minimizing the inefficiency and redundancy of data. Third, triangulation of the multiple perspectives across the cases corroborated best practices, provided a more comprehensive understanding of responses to the misuse of social media across the industry, and verified findings as consistent and repeatable. Fourth, transferability to other social media platforms and other industry sectors was reinforced by selecting participants from among industry leaders, collecting data from open sources, and using software tools. Finally, an audit trail containing notes, policies, and sources confirmed the data, process, results, and rationale of the researcher.

## Recommendations

Recommendations included the development of industry policies to interrupt the activities of terrorist groups online. There were two specific recommendations from the

findings in the development of industry policies that could be used to detect and disrupt terrorists online and could hinder the development of terrorist groups. The first recommendation was to combine and build on the strengths of existing platforms in the development of policies. The merging of multiple perspectives across platforms may compound benefits, provide a more comprehensive understanding of responses to the misuse of social media across the industry, corroborate best practices, and verify policies as consistent and repeatable. Building on existing strengths could also help platforms mitigate industry limitations, such as sharing the varying levels of resources and accountability, keeping up with the fast pace of the industry, and increasing the speed of responses.

In this multiple case study, six themes emerged from the data analysis: government collaboration with online platforms, a new era of regulation, online platforms taking greater responsibility, online platforms' ability to remove content, imposing consequences on online platforms, and platform policies and policy changes. The six themes revealed the areas in which the industry can focus its attention to form standardized responses to the misuse of social media by terrorists. A second recommendation, particularly for a relatively new industry such as social media, was to build policies on the groundwork established in peer-reviewed literature by research organizations and NGOs. In conjunction with best practices by NIST (n.d.), SANS, n.d.), and the Information Technology Industry Council (ITI, n.d.), platforms could use the findings to develop industry standards in the technology realm. These standards may make it easier and cheaper for platforms to provide technology for a more secure world.

The standardization process would encourage platforms and other stakeholders to speak to each other in a common language, which could result in an open, voluntary, consensus-based process around the world.

## Implications

The study may promote positive social change at every level of society (civilians, the technology industry, the business sector, national governments) to stop the activity of terrorist groups. Within the technology industry, the findings could help social media platforms overcome limitations and advance their ability to proactively respond to the misuse of services by terrorist groups. Standardized responses that combine the strengths of platforms could reduce the propaganda by terrorist groups, protect the intent of social media platforms, and fortify the industry against financial liability. A standardized approach to policy formation built on the groundwork of peer-reviewed literature by research organizations and NGOs could also serve as a model for the policy development of new platforms as well as that of the entire business community regarding terrorist activity. The methodology of the study positions other platforms to join in data sharing and analysis.

The findings may strengthen the collaboration between the U.S. government and the technology industry. The observations, data, and policies from social media platforms on terrorist use of social media and encryption technology may contribute to the efforts of the Department of Homeland Security in examining the threat to national security. Findings may be transferred for use by other governments.

Based on the SMT framework, standardized policies may help platforms detect and disrupt terrorists' propaganda efforts, thereby interrupting the life cycle of the growth of terrorist groups and leading to positive social change. With terrorist groups no longer utilizing social media platforms for their purposes, civilians would be less exposed to terrorists' politics, religion, and ideology and would be less susceptible to becoming radicalized. A reduction in online terrorist activity may result in fewer terrorist attacks, thereby creating a safer world.

The findings also impacted the prevention of domestic extremist content by social media platforms. While jihadis used the internet and social media for over 15 years, moving from platform to platform and adopting different tactics for usage, and while social media companies were slow to take effective measures to stop it, domestic extremists were learning social media tactics from jihadis. Jihadis even had advice for Neo-Nazis, white supremacists, and other domestic extremists in the April 14, 2021 issue of the *Al-Qaeda Ummah Wahida ("One Ummah")* magazine, which advised them to follow in Al-Qaeda's and other jihadis' footsteps and benefit from their knowledge when mainstream social media removed their accounts: "Learn from the experience of the jihadi fighters who faced these risks and how they avoided them. . . . Find answers in [Al-Qaeda's English-language] Inspire magazine" (MEMRI Jihad & Terrorism Threat Monitor, 2021a). Domestic extremists also followed jihadis' footsteps in moving to the use of encryption and cryptocurrency.

However, the social media companies learned from their experiences with jihadis, resulting in more difficulties online for domestic extremists than initially faced by jihadis.

Many posts and accounts by domestic terrorist and posts were swiftly removed from social media and from traditional banking and financing platforms, particularly following the August 2017 Unite the Right rally and the January 6, 2021 Capitol riot. Social media companies were much better equipped to deal to address the flood of neo-Nazis and white supremacists using their services (MEMRI Jihad & Terrorism Threat Monitor, 2021).

## Conclusion

This qualitative study examined the growing misuse of social media by terrorists for their strategic development. Since the inception of social media in 1999, user-generated content shared through fundamentally collaborative platforms ushered in a new era of open communication – and a new problem – for the world. As social media advanced, so had its unintended consequences, most notably the development of radical Islamic militant groups such as the Islamic State (ISIS) and Al-Qaeda. The lack of a unified response system to the urgent threat of terrorism increased corporate liability, threatened national security, and enabled the international growth of terrorist groups. The problem was part of the national security conversation for over a decade as a growing number of lawmakers raised the alarm and as social media platforms received unprecedented attention and pressure to mitigate terrorist activity.

Scholars and think tanks pointed to three major themes that emerged in research: the alarming misuse of social media by terrorists, the persistent lack of an effective response to that threat, and the resulting development of terrorist groups. Peer-reviewed research revealed that terrorists use platforms for networking, influential recruitment strategy, fundraising, information-gathering, training, and planning attacks. The research

was consistent with social movement theory (SMT), one of the most complete frameworks in examining terrorism; SMT asserts that the development and movement of terrorist groups follow a life cycle complemented by networks of continued propaganda. The research also revealed the gap that remains between global expectations and industry action by platforms.

The purpose of the study was to build on existing platform policies so that industry standards could be developed in response to the misuse of their services by terrorists. Rooted in social movement theory (SMT), this study confirmed the critical role of social media platforms and sought to disrupt the life cycle of the development of terrorist groups. The following research questions guided the study:

RQ1: What were the existing responses to terrorists' misuse of social media platforms?

RQ2: Could industry policies be produced from existing platform policies to form standardized responses to the misuse of social media by terrorists?

Secondary data was collected on four leading social media platforms – Facebook, Telegram, Twitter, and YouTube – across multiple cases of terrorism in the United Kingdom, France, the United States, and New Zealand. Open sources included government websites, media articles, and the online corporate websites of the four participants from which the following was collected: community standards, privacy policy, terms of services, user agreements, rules and policies, press releases, congressional testimonies, interviews with leadership, and/or other literature. The data was analyzed to find commonalities and precedents using organizational software NVivo.

Six themes emerged from the data: government collaboration with online platforms, a "new era" of regulation, online platforms taking greater responsibility, online platforms' ability to remove content, imposing consequences on online platforms, and platform policies and policy changes. I recommended the development of industry policies to interrupt the life cycle of terrorist groups. The six themes that emerged from the data revealed the areas in which the industry could focus its attention to form standardized responses to the misuse of social media by terrorists. When platforms combined and built on their strengths in the development of policies, they mitigated industry limitations and were provided a more comprehensive understanding of responses, corroborate best practices, verify policies as consistent and repeatable, keep up with the fast pace of the industry, and increase the speed of responses.

I also recommended building policies on the groundwork established in peer-reviewed literature by research organizations and non-governmental organizations (NGOs). These standards made it easier and cheaper for platforms to provide technology for a more secure world. The standardization process encouraged platforms and other stakeholders to speak to each other in a common language, resulting in an open, voluntary, consensus-based process around the globe.

The study aimed to support the development of industry policies in combatting the misuse of social media and encryption services. The potential for positive social impact included providing a blueprint for newer platforms, contributing to government efforts, and detecting and disrupting the use of the internet by terrorist groups and

domestic extremists. Ultimately, the study aimed to stop the radicalization of individuals, particularly youth, in performing terrorist attacks.

# References

Adapting to defend the homeland against the evolving international terrorist threat: Hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs, 115th Congress. (2017). Senate Hearing 115-400. https://www.govinfo.gov/content/pkg/CHRG-115shrg31263/html/CHRG-115shrg31263.htm

Ahlberg, C. (2014a). *How Al-Qaeda uses encryption post-Snowden (Part 1)*. Recorded Future. https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/

Ahlberg, C. (2014b). *How Al-Qaeda uses encryption post-Snowden (Part 2)*. Recorded Future. https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2

American National Standards Institute. (n.d.). *Resources: Standards developing organizations (SDOs)*. ANSI. https://www.standardsportal.org/usa_en/resources/sdo.aspx

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2014). Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. *Journal of Vocational Rehabilitation*, *41*, 87–98. https://doi.org/10.3233/JVR-140709

Arden, J. (2019, May 16). *Christchurch call to eliminate terrorist and violent extremist online content adopted*. New Zealand Government. https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

Arquilla, J. (2009, December 12). *How to lose a cyberwar.* Foreign Policy. https://foreignpolicy.com/2009/12/12/how-to-lose-a-cyberwar

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy.* RAND Corporation. https://www.jstor.org/stable/10.7249/mr1382osd

Barbaschow, A. (2019, March 25). *Canberra 'underwhelmed' with Facebook's live-streaming defence*. ZDNet. https://www.zdnet.com/article/canberra-underwhelmed-with-facebooks-live-streaming-defence/

Bartlett, L., & Vavrus, F. (2016). *Rethinking case study research.* Taylor & Francis.

Bartz, D. (2019, April 11). *U.S. Senator Warner eyes social media bills for hate speech, data portability.* Rueters. https://www.reuters.com/article/us-usa-tech-warner/u-s-senator-warner-eyes-social-media-bills-for-hate-speech-data-portability-idUSKCN1RN314?il=0

BBC News. (2017, June 13). *UK and France to work together to tackle online extremism*. BBC News. https://www.bbc.com/news/uk-politics-40258799

Bennet, C., & Williams, K. B. (2015, November 17). *Paris revives battle over government access to encrypted data.* The Hill. http://thehill.com/policy/cybersecurity/260522-paris-revives-battle-over-data-encryption

Berrebi, C., & Ostwald, J. (2013). Exploiting the chaos: Terrorist target choice following natural disasters. *Southern Economic Journal*, *79(4),* 793–811. https://doi.org/10.4284/0038-4038-2012.268

Birnbaum, E. (2019, April 9). *Facebook, Google face tough questions over white nationalism.* The Hill. https://thehill.com/policy/technology/technology/438000-facebook-and-google-seek-to-assure-congress-about-tamping-down

Birnbaum, E. (2019, April 12). *Pelosi puts tech on notice with warning of 'new era' in regulation*. The Hill. https://thehill.com/policy/technology/438652-pelosi-warns-its-a-new-era-for-regulating-big-tech

Bjeloper, J.P. (2013, January 23). *American jihadist terrorism: Combating a complex threat*. Congressional Research Service. Report Number R41416. https://sgp.fas.org/crs/terror/R41416.pdf

Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security*, *4*(4), 7–36. https://doi.org/10.5038/1944-0472.4.4.1

Bunt, G. (2003). *Islam in the Digital Age: Jihad, Online Fatwas and Cyber Islam Environment*. London, United Kingdom: Pluto Press.

Buran, B. (2011). *Enablers of Terrorism: Technology and the Web* (Bachelors of Science dissertation, The Pennsylvania State University). https://honors.libraries.psu.edu/catalog/1940

Carbone, C. (2017, October 4). *Family of American killed in Barcelona terror attack sues Facebook, Google and Twitter*. FoxNews. https://www.foxnews.com/tech/family-of-american-killed-in-barcelona-terror-attack-sues-facebook-google-and-twitter

Cardiff University. (2019, March 6). *Research sparks calls for tougher enforcement on social media companies*. Phys.org. https://phys.org/news/2019-03-tougher-social-

media-companies.html

CBS News. (2017, January 19). *Facebook, Twitter sued by families of Brussels, Paris terror attacks*. CBS News. https://www.cbsnews.com/news/facebook-twitter-sued-families-brussels-paris-terror-attacks/

Chalfant, M. (2017, December 6). *GOP chairman warns of ISIS's 'cyber caliphate.'* The Hill. http://thehill.com/policy/cybersecurity/363554-gop-chair-warns-of-islamic-states-cyber-caliphate

Chan, Z. C. Y., Fung, Y. L., & Chien, W. T. (2013). Bracketing in phenomenology: only undertaken in the data collection and analysis process? *The Qualitative Report, 18(59)*, 1-9. https://doi.org/10.46743/2160-3715/2013.1486

Chowdhry, A. (2019, March 31). *Social media roundup: Twitter may label abuses, Zuckerberg wants regulation, Pinterest adds to board*. Forbes. https://www.forbes.com/sites/amitchowdhry/2019/03/31/social-media-roundup-twitter-may-label-abuses-zuckerberg-wants-regulation-pinterest-adds-to-board/?sh=6511a372bd14

Christchurch call (n.d.). Christchurch call: To eliminate terrorist and violent extremist content online. https://www.christchurchcall.com/index.html

Citizendium (n.d.). *Self-radicalization/Definition*. Citizendium. http://en.citizendium.org/wiki/Self-radicalization/Definition

Cohen, F. (2002). Terrorism and cyberspace. *Managing Network Security*, *5*, 17-19. https://doi.org/10.1016/S1353-4858(02)05015-8

Cohen-Almagor, R. (2013). In internet's way: Radical terrorist Islamists on the free

highway. *International Journal of Cyber Warfare and Terrorism, 2,* 39-58. https://doi.org/10.2139/ssrn.2334640

Collins, K. (2017, May 5). *Families of San Bernardino victims sue Facebook, Google, Twitter.* CNET. https://www.cnet.com/au/news/families-of-san-bernardino-shooting-massacre-victims-sue-facebook-google-twitter-over-terrorism

Conway, Maura. (2007). *Terrorism and internet governance: Core issues.* Disarmament Forum, United Nations. http://www.unidir.ch/bdd/fiche-article.php?ref_article=2644

Cook, J. & Vale, G. (2019, July 23). *From Daesh to 'Diaspora': Tracing the women and minors of the Islamic State*. International Centre for the Study of Radicalisation, https://icsr.info/2018/07/23/from-daesh-to-diaspora-tracing-the-women-and-minors-of-islamic-state/

Corera, G. (2017, June 15). *Facebook reveals measures to remove terrorist content*. BBC. https://www.bbc.com/news/technology-40290258

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, California. Sage Publishing.

Creswell, J.W., & Plano Clark, V.L. (2017). *Designing and conducting mixed methods research.* (3rd ed.) Thousand Oaks, California. Sage Publishing.

Crosby, E., Ruiz, C., & Reyes, Y. (2016). *Crosby, et al. v. Twitter, Google, and Facebook, complaint for damages.* United States district court eastern district of Michigan. https://assets.documentcloud.org/documents/3243361/2016-1220-Crosby-vs-Twitter-Et-Al.pdf

Crusco, P. (2015, December 22). *Confronting smartphone encryption*. New York Law Journal. Available from https://news.bloomberglaw.com/?target=https%3A%2F%2Fwsauth.bloombergindustry.com%2Fwsauth%2Fblawauth%3Ftarget%3Dhttps%253A%252F%252Fwww.bloomberglaw.com%252Fcitation%252F1202745236073

Dailey, N. (2021, January 12). Telegram hits 500 million active users following backlash over WhatsApp's changing privacy policy. Business Insider. https://www.businessinsider.com/telegram-hits-500-million-users-after-whatsapp-backlash-2021-1

Denning, D. E. (1999, December 10). *Activism, hacktivism, and cyber terrorism: The internet as a tool for influencing foreign policy*. https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Department of Defense. (2019, August 21). Instruction. Number 5205.15-13. https://irp.fas.org/doddir/dod/i5205_13.pdf

Department of the Prime Minister and Cabinet. (2020, February 18). *New Zealand's countering terrorism and violent extremism strategy*. DPMC. https://dpmc.govt.nz/publications/new-zealands-countering-terrorism-and-violent-extremism-strategy

Digital Team. (2019, March 25). F*rench Muslim group sues Facebook and YouTube over Christchurch video*. WQuad8 (ABC). https://www.wqad.com/article/news/local/drone/8-in-the-air/french-muslim-

group-sues-facebook-and-youtube-over-christchurch-video/526-5075f617-1a83-4bc2-bbb0-fff4d069a8f8

Dreyfuss, E. (2017, May 23). *Think before you tweet in the wake of an attack*. Wired. https://www.wired.com/2017/05/think-tweet-wake-attack/

Du, A. B. (2017). *A state safety filed man was convicted for massively consulting Jihadist websites*. Lavoix. http://www.lavoixdunord.fr/269229/article/2017-11-24/un-homme-fiche-s-condamne-pour-avoir-massivement-consulte-des-sites-djihadistes

Duhaime (n.d.). Duhaime's Encyclopedia of Law. *Internet Service Provider.* http://www.duhaime.org/LegalDictionary/I/InternetServiceProvider.aspx

Durov, P. [@durov]. (2019, November 26). *We support free speech and peaceful protest, but terrorist propaganda has no place on our platform. The success of our* [Tweet]. Twitter. https://twitter.com/durov/status/1199333186439794688?lang=en

D.W. (2019, April 9). *EU hails social media crackdown on hate speech*. D.W. https://learngerman.dw.com/en/eu-hails-social-media-crackdown-on-hate-speech/a-47354465

Economic Times. (2008, October 26.) *Terrorist 'tweets'? US army warns of Twitter dangers.* Economic Times. https://economictimes.indiatimes.com/tech/internet/terrorist-tweets-us-army-warns-of-twitter-dangers/articleshow/3642198.cms?from=mdr

Facebook. (2005, November 26). *Statement of rights and responsibilities*. Facebook. https://www.Web.archive.org/web/20091231192755/https://www.facebook.com/t

erms.php

Facebook. (2011, January 27). *Facebook community standards.* Facebook. https://www.Web.archive.org/web/20130101112018/https://www.facebook.com/communitystandards/

Facebook. (2018, November 15). *Product policy forum minutes.* Facebook. https://about.fb.com/news/2018/11/content-standards-forum-minutes

Facebook. (2019). *Writing Facebook's rule book*. Facebook. https://about.fb.com/news/2019/04/insidefeed-community-standards-development-process

Facebook. (2022a). *Legal terms*. Facebook. https://www.Web.archive.org/web/20191231013206/https://www.facebook.com/legal/terms/

Facebook. (2022b *Terms of service*. Facebook. https://www.facebook.com/term.php

Federal Bureau of Investigation. (2009, April 1). Spear Phishers: Angling to Steal Your Financial Info. FBI. https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109

Federal Trade Commission (2015, January*). Internet of things: Privacy and security in a connected world*. FTC Staff Report. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Feiner, L. (2019, March 15). *Facebook, YouTube and Twitter are struggling to remove*

*New Zealand mosque shooting videos*. CNBC. https://www.cnbc.com/2019/03/15/facebook-youtube-and-twitter-struggle-to-remove-mosque-shooting-videos.html

Fielding, Nick. (2008). *Al Qaeda's propaganda war.* Perspectives on Radicalization and Political Violence. https://icsr.info/wp-content/uploads/2012/10/1234516938ICSRPerspectivesonRadicalisation.pdf

Final Report of the Task Force on Combatting Terrorist and Foreign Fighter Travel. U.S. House of Representatives, *114th Congress* (2015, October). https://www.govinfo.gov/content/pkg/CPRT-114HPRT97200/pdf/CPRT-114HPRT97200.pdf

Financial Times. (2018a, November 22). *MPs criticise tech groups and UK government over terror attacks*. Financial Times. https://www.ft.com/content/11d863e0-ee30-11e8-89c8-d36339d835c0

Financial Times. (2018b, December 6). *Australia passes anti-terror law to access encrypted messages.* Financial Times. https://www.ft.com/content/cc36cee4-f8fc-11e8-af46-2022a0b02a6c

Financial Times. (n.d.). *Four ways Google will help to tackle extremism*. Financial Times. https://www.ft.com/content/ac7ef18c-52bb-11e7-a1f2-db19572361bb

Finklea, K. (2017, March 10). *Dark web*. Congressional Research Service Report Number R44101. https://sgp.fas.org/crs/misc/R44101.pdf

First Post. (2018, August 30). *Telegram CEO says despite changes in privacy policy platforms is still secure.* FP. https://www.firstpost.com/tech/news-

analysis/telegram-ceo-says-despite-change-in-privacy-policy-platform-is-still-secure-5077281.html

Furnell, S., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers & Security, 18(1)*, 28-34. https://doi.org/10.1016/S0167-4048(99)80006-6

Ghaffary, S. (2019, June 10). *Twitter's top policy exec said there's "no doubt" that some social media content contributes to radicalization*. Vox. https://www.vox.com/recode/2019/6/10/18660088/twitter-radical-vijaya-gadde

Guynn, J. (2017, March 22). *AT&T, other U.S. advertisers quit Google, YouTube over extremist videos.* USA Today. https://www.usatoday.com/story/tech/news/2017/03/22/att-pulls-google-youtube-ads-over-offensive-content/99497194/

Guynn, J. (2017, March 27). *Facebook, Google, Twitter pressured to do more to fight terrorism on platforms*. USA Today. https://www.usatoday.com/story/tech/news/2017/03/27/uk-amber-rudd-facebook-google-twitter-silicon-valley-companies-terrorism/99703250/

Hamilton, F. (2017, June 13). *Tech giants that promote extremism face new fines*. The Times. https://www.thetimes.co.uk/article/tech-giants-that-promote-extremism-face-new-fines-2s6t02js7

Help Center. (2010a, August 2). *The Twitter rules*. Twitter. https://www.Web.archive.org/web/20131230195022/twitter.com/rules

Help Center. (2010b, July 16). *The Twitter rules.* Twitter.

https://www.Web.archive.org/web/20161207105156/https://support.twitter.com/articles/18311

Help Center. (2017, December 6). *The Twitter rules*. Twitter. https://www.Web.archive.org/web/20171228005200/https://help.twitter.com/en/rules-and-policies/twitter-rules

Help Center. (2022). *The Twitter rules*. Twitter. https://www.Help.twitter.com/en/rules-and-policies/twitter-rules

Hern, A. (2018, January 25). *May calls again for tech firms to act on encrypted messaging.* The Guardian. https://www.theguardian.com/technology/2018/jan/25/theresa-may-calls-tech-firms-act-encrypted-messaging

HG.org Legal Resources. (n.d.). *What is the relevance of "industry standards" under the law?* https://www.hg.org/legal-articles/what-is-the-relevance-of-industry-standards-under-the-law-36794

Information Technology Industry Council, (n.d.). *Industry standards*. ITI. https://www.itic.org/policy/industry-standards

Instagram (n.d. a). *Community guidelines.* Instagram. https://help.instagram.com/477434105621119/

Instagram (n.d. b). *Terms of use*. Instagram. https://help.instagram.com/478745558852511

Institute of Electrical and Electronics Engineers' Standards Association (2017, March 1). *Q&A with Konstantinos Karachalios, IEEE Standards Association managing*

*director*. https://beyondstandards.ieee.org/ethics-new-green/

Jamshed, S. (2014). Qualitative research method – interviewing and observation. J*ournal of Basic and Clinical Pharmacy, 5(4)*: 87-88. https://doi.org/10.4103/0976-0105.141942

Joint Chiefs of Staff (2014, October 24). *Counterterrorism* (JP 3-26). https://irp.fas.org/doddir/dod/jp3_26.pdf

Jones, S. G., Dobbins, J., Byman, D., Chivvis, C. S., Connable, B., Martini, J., Robinson, E., & Chandler, N. (2017). Rolling back the Islamic state. RAND Corporation. https://doi.org/10.7249/RR1912

Kang, S, & Frenkel, S. (2018, September 4). *Facebook and Twitter have a message for lawmakers: We're trying.* The New York Times. https://www.nytimes.com/2018/09/04/technology/facebook-and-twitter-have-a-message-for-lawmakers-were-trying.html

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53(1)*, 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Kaplan, S. (2015, November 19). *Founder of app used by ISIS once said 'We shouldn't feel guilty.' On Wednesday he banned their accounts.* The Washington Post. https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts

Kelly, M. (2019, March 19). *Facebook, YouTube, and others asked to brief Congress on*

*New Zealand shooting response*. The Verge. https://www.theverge.com/2019/3/19/18273257/facebook-youtube-microsoft-twitter-congress-zealand-shooting-response

Klandermans, P. & Stekelenburg, J. (2009). *Social movement theory: Past, present and prospect.* Research Gate. https://www.researchgate.net/publication/254828894_Social_movement_theory_Past_present_and_prospect

Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict and Terrorism. 38*, 1-22. https://doi.org/10.1080/1057610X.2014.974948

Kottasova, I. (2018, September 12). *Europe could hit tech companies with huge fines over terrorist content*. CNN. https://money.cnn.com/2018/09/12/technology/online-terrorist-content-eu/index.html

L.A. Times. (2017, January 19). *Lawsuits blame Facebook and Twitter in terror attacks in Paris, Brussels.* Los Angeles Times. https://www.latimes.com/business/technology/la-fi-tn-lawsuits-social-media-terror-20170119-story.html

Lamar University (n.d.). *Social Media Policy*. https://www.lamar.edu/marketing-communications/guidelines/policies-and-guidelines/social-media-policy.html

LAWS. (n.d.). *Easy definition of hacking.* https://cyber.laws.com/hacking

Levin, S. (2017, June 26). *Tech giants team up to fight extremism following cries that*

*they allow terrorism*. The Guardian. https://www.theguardian.com/technology/2017/jun/26/google-facebook-counter-terrorism-online-extremism

Lewis, J. (2015). *Media, Culture and Human Violence: From Savage Lovers to Violent Complexity.* Lanham, Maryland. Rowman and Littlefield.

Lomas, N. ((2017, April 11). *French presidential candidate Macron talks tough on tech firms over terrorism.* TechCrunch. https://techcrunch.com/2017/04/11/french-presidential-candidate-macron-talks-tough-on-tech-firms-over-terrorism/

Longman Dictionary of Contemporary English. (2003). Theory. In *Longman dictionary of contemporary English online*. https://www.ldoceonline.com/dictionary/theory

Marvin, G. (2017, June 21). *With brand safety in mind, YouTube steps up efforts to 'fight online terror.* Martech. https://martech.org/brand-safety-youtube-efforts-fight-online-terror

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research, 11(3)*. http://www.qualitative-research.net/index.php/fqs/article/view/1428/3027

Matthews, K. (2015, May 28). *Global cyber-strategy needed to confront 'IS' and other terror groups*. Deutsche Welle. http://www.dw.com/en/global-cyber-strategy-needed-to-confront-is-and-other-terror-groups/a-18481090

Mekhennet, S. (2020, April 10). *Far-right and radical Islamist groups are exploiting coronavirus turmoil.* The Washington Post. https://www.washingtonpost.com

MEMRI. (2014, August 1). *Following Twitter shutdown of hamas' Al-Qassam brigades*

*account - One week later, a new account is active*. MEMRI. https://www.Web.archive.org/web/20161207105156/https://support.twitter.com/articles/18311

MEMRI Cyber & Jihad Lab. (2011). *Online jihadi brings forward the importance of e-jihad in the muslims' fight against their enemies.* MEMRI. http://cjlab.memri.org/uncategorized/online-jihadi-brings-forward-the-importance-of-e-ihad-in-the-muslims-fight-against-their-enemies/

MEMRI Jihad & Terrorism Threat Monitor. (2007, May 31). *Video of abducted BBC journalist Alan Johnston* [Video]. MEMRI. https://www.memri.org/jttm/video-abducted-bbc-journalist-alan-johnston

MEMRI Jihad & Terrorism Threat Monitor. (2008, December 2). *Islamist websites launch online campaign for general strike in Egypt.* MEMRI. https://www.memri.org/jttm/islamist-websites-launch-online-campaign-general-strike-egypt

MEMRI Jihad & Terrorism Threat Monitor. (2014, March 13). *Syria-based Saudi Sheikh launches second campaign to purchase ammunition for jihadi groups fighting in Syria.* MEMRI. https://www.memri.org/jttm/syria-based-saudi-sheikh-launches-second-campaign-purchase-ammunition-jihadi-groups-fighting

MEMRI Jihad & Terrorism Threat Monitor. (2021a, February 17). *Taliban commander's interview revealing the details of their print magazines and international media operations, says: 'We are also active on Facebook And Twitter where we publish the news every day'*. MEMRI. Available from

https://www.memri.org/jttm/taliban-commanders-interview-revealing-details-their-print-magazines-and-international-media.

MEMRI Jihad & Terrorism Threat Monitor. (2021b, April 19). *New Issue Of Al-Qaeda Magazine Focuses On Internal Situation Of The U.S. And The Coronavirus*. MEMRI. https://www.memri.org/jttm/new-issue-al-qaeda-magazine-focuses-internal-situation-us-and-coronavirus

Merriam-Webster. (n.d.). Propaganda. In *Merriam-Webster.com dictionary*. https://www.merriam-webster.com/dictionary/propaganda

Meta. (2017, June 15). *Hard questions: How we counter terrorism*. FaceBook NewsRoom. https://about.fb.com/news/2017/06/how-we-counter-terrorism/

Meta. (2018, November 8). *Hard questions: What are we doing to stay ahead of terrorists?* FaceBook NewsRoom. https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/

Meta. (2022a). *Coordinating harm and promoting crime*. Facebook. https://www.Transparency.fb.com/policies/community-standards/coordinating-harm-publicizing-crime/

Meta. (2022b). *Dangerous individuals and organizations*. Facebook. https://www.Transparency.fb.com/policies/community-standards/dangerous-individuals-organizations/

Meta. (2022c). *Violence and incitement*. Facebook. https://www.transparency.fb.com/policies/community-standards/violence-incitement/

Metzger, T. (2014). Social movement theory and terrorism: Explaining the development of Al-Qaeda. *Inquiries Journal, 6(9).* https://www.studentpulse.com/a?id=916

Microsoft. (2019, May 15). *The Christchurch call and steps to tackle terrorist and violent extremist content*. Microsoft Corporate Blog. https://blogs.microsoft.com/on-the-issues/2019/05/15/the-christchurch-call-and-steps-to-tackle-terrorist-and-violent-extremist-content

Mullins, S. J. (2015). *Home-Grown Jihad: Understanding Islamist Terrorism in the U.S. and U.K.* London: Imperial College Press. https://books.google.com/books?id=q7DACwAAQBAJ&lpg=PA197&dq=jihad%20propaganda%20recruitment%20training%20plan%20attacks%20fundraising&pg=PA197#v=onepage&q=jihad%20propaganda%20recruitment%20training%20plan%20attacks%20fundraising&f=false

Murphy, E. (2017, June 4). *Talking points: Stopping extremism on the internet.* CBS Minnesota. https://minnesota.cbslocal.com/2017/06/04/talking-points-al-franken-terrorism/

National Institute for Cybersecurity Careers and Studies. (n.d.). *Cybersecurity Glossary.* https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#E

National Institute of Standards and Technology (2009). About NIST. https://www.nist.gov/about-nist

NATO Cooperative Cyber Defense Centre of Excellence. (n.d.). *Cyberspace: Definition and implications* https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/

Nicas, J. (2017, December 12). *Cuomo points to tech companies after New York bombing attempt*. The Wall Street Journal. https://www.wsj.com/articles/google-others-take-uneven-approach-to-policing-extremist-content-1513074601

Nieles, M., Dempsey, K., & Yan Pilliterri, V., (2017, June). An introduction to information security. NIST Special Publication 800-12. Revision 1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NVivo. (n.d.) https://www.qsrinternational.com/nvivo/nvivo-products

O'Brien, C. (2019, May 15). *Facebook, Microsoft, Google, and other tech companies join governments in pledging to fight terrorist content in wake of Christchurch shooting, but U.S. refuses to join*. Business Insider. https://www.businessinsider.com/facebook-google-microsoft-twitter-christchurch-pledge-terrorism-content-2019-5

O'Reilly, A. (2016, December 19). *Exclusive: Families of Orlando nightclub shooting victims sue Facebook, Twitter and Google*. Fox News. www.foxnews.com/us/2016/12/19/exclusive-families-orlando-nightclub-shooting-victims-sue-facebook-twitter-and-google.html

Pacheco-Vega, R. (2020). Ethnography as a Method for Comparative Public Policy Analysis: Premises, Promises and Perils. In Peters, G., Falk, M., & Fontaine, G. (Eds.), *Handbook of Research Methods and Applications in Comparative Policy Analysis.* United Kingdom: Edward Elgar Publishing.

Parveen, N., & Dodd, V. (2019, March 15). UK Muslim leaders urge protection for mosques after Christchurch. The Guardian. https://www.theguardian.com/uk-

news/2019/mar/15/uk-muslim-leaders-urge-protection-for-mosques-after-christchurch

Patton, M. Q., & Cochran, M. (2002). *A Guide to Qualitative Research Methodology*. Medecins Sans Frontieres. http://evaluation.msf.org/sites/evaluation/files/a_guide_to_using_qualitative_research_methodology.pdf

PC Magazine. (n.d.). *Encyclopedia: Terms of service.* https://www.pcmag.com/encyclopedia/term/terms-of-service

Perez, E., & Ford, D. (2015, December 14). *San Bernardino shooter's social media posts on jihad were obscured.* CNN. https://www.cnn.com/2015/12/14/us/san-bernardino-shooting/index.html

Perez, Y.B. (2017, September 20). *Theresa May: Tech giants must take down extremist content within two hours.* UKTN. https://www.uktech.news/news/government-and-policy/theresa-may-tech-giants-must-take-extremist-content-within-two-hours-20170920

Price, R. (2017, June 5). *Tech companies respond to Theresa Mays call for internet regulation after London terror attack.* Business Insider. https://www.businessinsider.com/tech-companies-respond-to-theresa-mays-call-for-internet-regulation-after-london-terror-attack-2017-6

Rodrigo, C. M. (2019, April 9). *YouTube shuts down comments on House hearing on white nationalism over hateful remarks*. The Hill. https://thehill.com/policy/technology/438055-hateful-comments-force-youtube-

to-shut-down-chat-on-livestream-of-house

Rogan, H. (2006). *Jihadism Online – A Study of How Al-Qaida and Radical Islamist Groups Use the Internet For Terrorist Purposes.* FFI. https://publications.ffi.no/nb/item/asset/dspace:3212/06-00915.pdf

Rutenberg, J. (2017, November 1). *Terrorism is faster than Twitter*. NY Times. https://www.nytimes.com/2017/11/05/business/media/terrorism-social-networks-freedom.html

Salkind, N. J. (2010). Triangulation. *Encyclopedia of Research Design*. https://doi.org/10.4135/9781412961288.n469

Samarov, M. (2008). *A social movement theory analysis of islamist totalitarianism.* Marine Corps Library. http://www.dtic.mil/dtic/tr/fulltext/u2/a504756.pdf

SANS. (n.d.). Information security policy templates. SANS. https://www.sans.org/security-resources/policies

Serrels, M. (2019, March 15). *Facebook, YouTube trying to rein in footage of New Zealand mosque shooting*. CBS News. https://www.cbsnews.com/news/new-zealand-mosque-shooting-facebook-youtube-trying-to-rein-in-footage-of-new-zealand-mosque-shooting/

Shaban, H. (2017, July 31). *Sheryl Sandberg: WhatsApp encryption actually helps governments combat terrorism.* The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2017/07/31/sheryl-sandberg-whatsapp-encryption-actually-helps-governments-combat-terrorism

Shaban, H. (2019, March 21). *Facebook to reexamine how livestream videos are flagged*

*after Christchurch shooting*. The Washington Post. https://www.washingtonpost.com/technology/2019/03/21/facebook-reexamine-how-recently-live-videos-are-flagged-after-christchurch-shooting/

Shinal, J. (2018, January 17). *Facebook, Google tell Congress they're fighting extremist content with counterpropaganda*. CNBC. https://www.cnbc.com/2018/01/17/facebook-google-tell-congress-how-theyre-fighting-extremist-content.html

Spangler, T. (2019, March 15). *New Zealand shootings: Facebook, YouTube, Twitter scramble to pull alleged attacker's video, hate content*. Variety. https://variety.com/2019/digital/news/new-zealand-shootings-facebook-youtube-twitter-video-hate-1203164251/

Sperry, P. (2015, November 22). *900 'Homegrown' ISIS cases being investigated in US: FBI.* New York Post. http://nypost.com/2015/11/22/obamas-isis-strategy-only-increases-risk-of-a-us-attack.

Stahl, L. (2016, March 13). *The encryption debate.* CBS News. https://www.cbsnews.com/news/60-minutes-encryption-debate-lesley-stahl

Stalinsky, S. (2010, July 1). *Youtube-The internet's primary and rapidly expanding jihadi base-Part III: Despite removal efforts, Taliban Youtube page promising terror attacks on U.S. cities remains active*. MEMRI. https://www.memri.org/reports/youtube-%E2%80%93-internets-primary-and-rapidly-expanding-jihadi-base-%E2%80%93-part-iii-despite-removal

Stalinsky, S. (2011, December 29). *Hamas tweets for jihad and martyrdom, for expelling*

*and killing jews, and for conquering Jerusalem - Another U.S.-designated foreign terrorist organization served by using Twitter.* MEMRI. https://www.memri.org/reports/hamas-tweets-jihad-and-martyrdom-expelling-and-killing-jews-and-conquering-jerusalem-%E2%80%93

Stalinsky, S., & Sosnow, R. (2014). *From Al-Qaeda to the Islamic state (ISIS), jihadi groups engage in cyber jihad: Beginning with 1980s promotion of use of 'electronic technologies' up to today's embrace of social media to attract a new jihadi generation.* MEMRI. https://www.memri.org/reports/al-qaeda-islamic-state-isis-jihadi-groups-engage-cyber-jihad-beginning-1980s-promotion-use-0

Stalinksy, S., Sosnow, R., & Khayat, M. (2016, January 6). *ISIS's use of Twitter, other U.S. social media to disseminate images, videos of Islamic religious punishments-beheading, crucifixion, stoning, burning, drowning, throwing from buildings - free speech?* MEMRI. https://www.memri.org/cjlab/isiss-use-of-twitter-other-u-s-social-media-to-disseminate-images-videos-of-islamic-religious-punishments-beheading-crucifixion-stoning-burning-drowning-throwing-from-buildings

Stalinsky, S. & Zweig, E. (2013, April 9). *Youtube question in U.K. house of commons over keeping terrorism-promoting videos active on its webstie: Of 125 videos of al-qaeda commander Al-Zawahiri flagged on Youtube by MEMRI, Youtube keeps 57 active*. MEMRI. https://www.memri.org/reports/youtube-questioned-uk-house-commons-over-keeping-terrorism-promoting-videos-active-its

Stewart, H. & Elgot, J. (2018, January 24). *May calls on social media giants to do more to tackle terrorism*. The Guardian.

https://www.theguardian.com/business/2018/jan/24/theresa-may-calls-on-social-media-giants-to-do-more-to-tackle-terrorism

Stone, J. (2017, June 4). *Theresa May says the internet must now be regulated following London Bridge terror attack.* Independent. https://www.independent.co.uk/news/uk/politics/theresa-may-internet-regulated-london-bridge-terror-attack-google-facebook-whatsapp-borough-security-latest-a7771896.html

Swan, B. (2019, April 11). *Democrats in congress tell social media companies to reveal size of their counter-terror budgets*. The Daily Beast. https://www.thedailybeast.com/democrats-in-congress-tell-social-media-companies-to-reveal-size-of-their-counter-terror-budgets

Tan. R. (2017, June 30). *Terrorists' love for Telegram, explained*. Vox. https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter

Taylor, R. (2019, April 4). *New Zealand shooter to face 50 murder charges*. The Wall Street Journal. https://www.wsj.com/articles/new-zealand-shooter-to-face-50-murder-charges-11554359134

Techopedia. (n.d.) *Hack.* https://www.techopedia.com/definition/3804/hack-security

Telegram. (2018, May 19). *Terms of service*. Twitter. https://www.Web.archive.org/web/20180519105844/Telegram.org/tos

Telegram. (2022). *Terms of service*. Twitter. https://www.Telegram.org/tos

Telegram. (n.d.) *Telegram F.A.Q.* https://www.telegram.org/faq

The Economist. (2017, June 8). *Tech giants are under fire for facilitating terrorism.* Economist. http://www.economist.com/news/international/21723106-some-criticism-unfair-there-more-they-could-do-tech-giants-are-under-fire

The Hill. (2017, June 7). *House democrat invites UK prime minister to Silicon Valley*. The Hill. https://thehill.com/policy/technology/336730-house-dem-invites-uk-pm-to-silicon-valley[June%207th]

The White House: President Barack Obama. (2015). Fact sheet: The White House summit on countering violent extremism. The White House. https://www.whitehouse.gov/the-press-office/2015/02/18/fact-sheet-white-house-summit-countering-violent-extremism

Theohary, C. A., & Rollins, J. (2011). *Terrorist use of the internet: Information operations in cyberspace.* Congressional Research Service. Report Number R41674. https://www.fas.org/sgp/crs/terror/R41674.pdf

Timberg, C., Harwell, D., Shaban, H., Tran, A. B., & Fung, B. (2019, March 15). *The New Zealand shooting shows how YouTube and Facebook spread hate and violent images — yet again.* The Washington Post. https://www.washingtonpost.com/technology/2019/03/15/facebook-youtube-twitter-amplified-video-christchurch-mosque-shooting/

Toor, A. (2017 March 14). *Germany considers 50 million euro fines for social media companies that fail to remove hate speech*. The Verge. https://www.theverge.com/2017/3/14/14920812/germany-facebook-twitter-hate-speech-fine-law

Travis, A. (2017, October 2). *Amber Rudd: Viewers of online terrorist material face 15 years in jail.* The Guardian. https://www.theguardian.com/uk-news/2017/oct/03/amber-rudd-viewers-of-online-terrorist-material-face-15-years-in-jail

Tuck, H., & Silverman, T. (2016). *The Counter-Narrative Handbook.* The Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2016/06/Counter-narrative-Handbook_1.pdf

Tufts University. (n.d.) *Guidelines and tools for managing and developing policies.* Digital Collections and Archives. http://sites.tufts.edu/dca/records-management/records-policies/guidelines-and-tools-for-managing-and-developing-policies

Twitter. (2016, February 5). *Combating violent extremism.* Twitter. https://blog.twitter.com/en_us/a/2016/combating-violent-extremism

Twitter. (2017, June 26). Global internet forum to counter terrorism. Twitter. https://blog.twitter.com/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism

Twitter. (2021, August 19). *Twitter terms of service*. Twitter. https://www.Twitter.com/en/tos

Twitter. (2012) Tweets still must flow. https://blog.twitter.com/official/en_us/a/2012/tweets-still-must-flow.html

Twitter Help Center. (n.d.a) The Twitter rules. https://support.twitter.com/articles/20169997#

Twitter Help Center. (n.d.b) Twitter media policy. https://support.twitter.com/articles/20169199#

Twitter Public Policy. (2017). Global internet forum to counter terrorism. Twitter. https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html

U.K. Government. (2019, June 13). *UK and France announce joint campaign to tackle online radicalisation*. Gov.UK. https://www.gov.uk/government/news/uk-and-france-announce-joint-campaign-to-tackle-online-radicalisation

UN Business. (2017, June 13). *Tech firms may face new legal liability as PM and Macron target extreme content*. Business Insider. https://business-reporter.co.uk/2017/06/13/tech-firms-may-face-new-legal-liability-as-pm-and-macron-target-extreme-content/#gsc.tab=0

United Nations Office on Drugs and Crime. (2017). *Handbook on children recruited and exploited by terrorist and violent extremist groups.* https://www.unodc.org/documents/justice-and-prison-reform/Child-Victims/Handbook_on_Children_Recruited_and_Exploited_by_Terrorist_and_Violent_Extremist_Groups_the_Role_of_the_Justice_System.E.pdf

U.S. Department of Health & Human Services. (2013). *Health information privacy: What is encryption?* https://www.hhs.gov/hipaa/for-professionals/faq/2021/what-is-encryption/index.html

U.S. Embassy. (2019, May 15). *Statement on Christ Church call for action.* U.S. Embassy & Consulate in New Zealand Cook Islands and Niue.

https://nz.usembassy.gov/statement-on-christchurch-call-for-action/

Van Boom, D., & Keane, S. (2019, March 19). Facebook: New Zealand shooting video had fewer than 200 real-time viewers. CNET. https://www.cnet.com/tech/services-and-software/facebook-new-zealand-shooting-video-had-fewer-than-200-real-time-viewers/

Vincent, J. (2018, August 20). *EU considers fines for tech companies that don't remove terrorist content within an hour*. The Verge. https://www.theverge.com/2018/8/20/17758542/eu-terrorist-content-legislation-facebook-youtube-takedown

Vidino, L., & Hughes, S. (2015) *Countering violent extremism in America.* Report, George Washington University Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/CVE%20in%20America.pdf

Walden University, Center for Research Quality. (n.d.) *Research ethics and compliance: Application and general materials*. Academic Guides. http://academicguides.waldenu.edu/researchcenter/orec/application

Walker, K. (2017a, June 18). *Four steps we're taking today to fight terrorism online*. Google in Europe. https://www.blog.google/around-the-globe/google-europe/four-steps-were-taking-today-fight-online-terror/

Walker, K. (2017b, September 20). *Working together to combat terrorists online.* Google, the Keyword. https://blog.google/outreach-initiatives/public-policy/working-together-combat-terrorists-online

Washington Post. (2015, May 1). *5th Republican debate transcript, annotated: Who said what and what it meant.* Washington Post. https://www.washingtonpost.com/news/the-fix/wp/2015/12/15/who-said-what-and-what-it-meant-the-fifth-gop-debate-annotated/?utm_term=.c36f1903346

Waskiewicz, T. (2012). *Friend of a Friend Influence in Terrorist Social Networks.* Homeland Security Research Laboratory. https://www.hsdl.org/c/

Watts, J. (2019, March 15). *New Zealand attack: Downing Street demands all media firms remove video of Christchurch mosque shooting*. Independent. https://www.independent.co.uk/news/uk/politics/new-zealand-attack-video-theresa-may-shooting-facebook-twitter-youtube-a8824491.html

Weimann, G. (2004). *How modern terrorism uses the internet.* United States Institute for Peace. https://www.usip.org/sites/default/files/sr116.pdf

Weimann, G. (2006). *Terror on the internet: The new arena, the new challenges.* Washington, DC: United States Institute of Peace Press, 391-393.

Weimann, G. (2010.). *Terror on Facebook, Twitter, And Youtube.* Brown Journal of World Affairs. https://bjwa.brown.edu/16-2/terror-on-facebook-twitter-and-youtube

Weimann, G. (2014). *New terrorism and new media.* Woodrow Wilson International Center for Scholars. https://www.wilsoncenter.org/publication/new-terrorism-and-new-media

West, L. J. (2016). #jihad: Understanding social media as a weapon. *Security Challenges, 12(2),* 9-26. https://www.regionalsecurity.org.au/resources/Documents/WEST.pdf

Whitehouse, K. (2017, January 9). *Brussels attack victim's wife sues Twitter for being 'weapon of Terror.'* New York Post. https:.///www.nypost.com/2017/01/09/brussels-attack-victims-wife-sues-twitter-for-being-a-weapon-of-terror

Wiktorowicz, Q. (2002). Islamic activism and social movement theory: A new direction for research. *Mediterranean Politics, 7*, 187-211. https://doi.org/10.1080/13629390207030012

Yahoo Finance. (2019, April 7). *UK unveils plans to hold social media bosses liable for harmful content.* Yahoo. https://www.yahoo.com/now/uk-unveils-plans-hold-social-media-bosses-liable-231755781.html

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA. Sage.

Youn, S. (2019, March 17). *Why it took YouTube, Facebook and Twitter so long to remove video of New Zealand mosque shootings*. ABC News. https://abcnews.go.com/ABCNews/youtube-facebook-twitter-scrambling-video-zealand-mosques-shooting/story?id=61707307

YouTube. (2017, June 24). *Policies and safety*. Youtube. http://web.archive.org/web/20181227075800/https://www.youtube.com/yt/about/policies/#community-guidelines

YouTube (2019, May 23). *Hate speech policy*. Google. https://support.google.com/youtube/answer/2801939?hl=en&ref_topic=9282436