# ABSTRACT

Title of Thesis: Combating Terrorism in the Digital Era: How Facebook and Twitter Can Aid American Counterterrorism Efforts

Thesis Adviser: Professor Melvyn Levitsky

Despite the billions of dollars that the American government spends annually to combat terrorism, terrorists maintain a strong presence both domestically and internationally. The rise of social media in the past ten years has added an extra layer of difficulty in the United States' attempts to prevent terrorism. Terrorists use social media to spread their messages, plan attacks, and recruit civilians world-wide. While Facebook and Twitter do track terrorist activity on their sites, they fail to discover all content and to share information with governmental counterterrorism agencies, who could use this data to combat terrorism. But how can American counterterrorism agencies collaborate with Facebook's and Twitter's security teams in order to more effectively counteract terrorism? This thesis argues that, through the creation of a legal policy, Twitter and Facebook can share terrorist content that they identify with the American National Counterterrorism Center (NCTC). The NCTC can then share this information with other counterterrorism agencies in order to identify, track, and arrest or extradite terrorists and to thwart terrorist activities. The thesis discusses the current inefficacies of American counterterrorism strategies and the possible information that counterterrorism agencies could gain from social media in order to prove the necessity of the policy recommendation.

# Combatting Terrorism in the Digital Era:
# How Facebook and Twitter Can Aid American Counterterrorism Efforts

By
Marielle Dewicki

Thesis submitted to the Faculty of the College of Literature, Science, & Arts
at the University of Michigan in partial fulfillment
for the requirements for the degree
of Bachelor of Arts
(International Studies with Honors)
2019

Thesis Committee:

Professor Melvyn Levitsky
Doctor Anthony Marcum

## Dedication

“As a former career intelligence professional, I have a profound appreciation for the value of intelligence. Intelligence disrupts terrorist plots and thwarts attacks. Intelligence saves lives.”

*- John O. Brennan, Director of the Central Intelligence Agency (2013—2017)*

## Acknowledgments

I would first like to thank Professor Melvyn Levitsky and Doctor Anthony Marcum for their assistance in the creation of this thesis. Your advice helped me to create the best work possible, and your encouragement helped me to continue to strive for success, despite the stress of senior year. I could not have crafted such a complex thesis without either of you.

I would also like to thank my family (especially my parents) and friends for supporting me while I wrote this thesis. I know that I likely spent far too much time discussing all of the work that I had to do and that this subject matter sometimes went beyond your understanding, but you continued to listen and to encourage me anyway. You helped me to find the motivation that I needed to develop and finish my writing on time, even when I would have rather done anything else. Beyond this thesis, you have supported and strengthened me to succeed throughout my academic career. Your support was invaluable, and I love you all.

Most importantly, thank you to the “Big Man Upstairs,” without whom nothing would be possible. You have my eternal gratitude.

## Table of Contents

## List of Abbreviations

1. DHS: Department of Homeland Security
2. DoD: Department of Defense
3. DOS: Department of State (State Department)
4. CIA: Central Intelligence Agency
5. FBI: Federal Bureau of Investigation
6. GIFCT: Global Internet Forum to Counter Terrorism
7. OCO: Overseas Contingency Operations
8. OMB: Office of Management and Budget
9. NCTC: National Counterterrorism Center
10. NIMA: National Imagery and Mapping Agency
11. NSA: National Security Agency
12. TTIC: Terrorist Threat Integration Center
13. U.S.: United States
14. USAID: United States Agency for International Development

# Chapter I: Introduction

## I.I An Introduction to Terrorism

September 11, 2001. January 7, 2015. December 19, 2016. These days now remain marked in history, united by one common theme: terrorism. But the attacks on the World Trade Center, Charlie Hebdo newspaper, and Berlin Christmas Market present only three of thousands of terrorist attacks world-wide that have occurred in the past two decades. Beyond the obvious physical impacts of terrorist attacks, including human casualties and infrastructural damage, these events sow and spread fear, hatred, and division in the societies in which they occur. Social media, with platforms that billions of individuals use to connect world-wide, has played a role in some of these attacks, as terrorist organizations use these sites to recruit new followers and to spread propaganda. The American government and social media companies like Facebook and Twitter recognize this threat, but the two factions rarely collaborate on information sharing and other counterterrorism tactics. Thus, American counterterrorism agencies lack crucial sources of information that they could use in conjunction with data from other places to help combat terrorism (Steinbach).

How, then, can American counterterrorism agencies collaborate with Facebook and Twitter's security teams in order to more effectively counteract terrorism? In this thesis I respond that American counterterrorism agencies can create a policy which would obligate Facebook and Twitter to share information gathered from terrorists' accounts and would allow the government to charge suspects based upon social media activity. The content from social media, used in conjunction with other data collection and counterterrorism methods, would help the agencies to prevent attacks and to locate terrorists, which would lead to the arrest of suspects and the destabilization of terrorist organizations. While current counterterrorism tactics in the United

States and world-wide appear to have reduced the number of annual terrorist attacks from major foreign terrorist organizations, the United States faces increased attacks from homegrown terrorists, American civilians inspired to act by the messages and actions of foreign terrorist groups (Allen). The immediate and wide-spread communication on social media facilitates an effective method for terrorists to continuously disseminate their beliefs and to recruit followers. Social media companies such as Facebook and Twitter do attempt to remove this information from their platforms, but the companies do not share terrorists' information with American counterterrorism agencies unless pressured (Steinbach). Thus, in order to allow counterterrorism agencies to tap into and use such data in order to effectively combat terrorism, I argue that a legal policy provides the best solution to the problem of information access, and I outline a model for such a policy.

In this chapter, Chapter 1, I introduce the concept of terrorism. Because no singular definition of terrorism exists in the world, let alone the United States, I create a definition under which my thesis and policy proposal can operate. Because this thesis centers on America and social media, I analyze and incorporate characteristics of terrorism as identified by the U.S. Code § 2331, the Federal Bureau of Investigation, the Department of State, and Facebook. The other governmental agencies that contend with terrorism and Twitter do not define terrorism, so I do not mention them in my definition. After this discussion I outline the thesis' chapters and justify my choices, through a discussion of the methodologies that I utilize, in order to validate the arguments that I pose throughout the thesis. Finally, I conclude with a discussion of the goal that my thesis hopes to achieve: to create a means of information gathering that can effectively assist American counterterrorism agencies in identifying and targeting more terrorists in order to thwart their actions, destabilize their organizations, and promote security world-wide.

## I.II Defining Terrorism

The concept of terrorism might initially appear easy to define. Individuals with extremist ideologies commit violent actions against others. But who are these individuals? Why do they commit acts of violence, and who (or what) do they target? Before American government agencies can begin to combat terrorism, they require one cohesive, specific definition to conceptualize the crime that addresses all of these questions. Private companies, international organizations, and different government beaurocracies currently lack a singular, solid definition of terrorism. The lack of cohesion between these groups' definitions of terrorism results from the differences in the goals of each agency and from the legal weight of the designation as a "terrorist." This classification allows the government to harshly punish accused individuals under national and international laws and effectively brands the accused as violent radicals. If international agencies do not strictly classify crimes pertaining to terrorism, they risk unjustly condemning suspects or freeing truly culpable individuals who may continue to attack civilians and governments (UNDOC). While the United Nations has attempted to create a definition of terrorism since 2000, debates between individual countries continue to bar its attempts. Some countries (like the United States) push for stricter and broader definitions, while Arab countries and groups like the Organization of Islamic Cooperation hope to differentiate between acts of terrorism and valid actions by colonized and oppressed peoples to seek independence under the protection of international law. America's "terrorists" may represent other countries' "freedom fighters" or "guerrilla groups" (European Union, European Parliamentary Research Service 1-2). Because this thesis concentrates on the potential uses of social media by American counterterrorism agencies, my definition will incorporate components from the definitions of the U.S. Legal Code, Federal Bureau of Investigation, the Department of State, and Facebook.

As American law ultimately (or ideally) determines the actions of counterterrorism agencies, I commence with definition of terrorism outlined by the U.S. Code § 2331 under Chapter 113b of Part II of Title 18. The legal code differentiates between international and domestic terrorism, but the characterization remains the same, except for the location of terrorist attacks. The law defines terrorism overall as violent acts that threaten human life and violate American federal or state criminal law codes (if they occurred domestically) or would violate those codes if they had occurred in the US (but occurred internationally). Through these activities, terrorists intend to terrorize civilian groups, dictate government actions or policies through terror, or alter government activity through mass destruction, kidnapping, or assassination (115 Stat. 376). The law code does not identify specific acts of terrorism other than assassinations, kidnapping, and mass destruction, nor does it outline the possible motivations for terrorists' attempts to influence and threaten civilians and governments. Thus, this definition may not include all types of motivations, such as religious motivations (such as those of ISIS), political motivations (such as those of violent communist groups), or ethnic motivations (such as those of the Ku Klux Klan)

The non-specific and broad nature of U.S. Code § 2331, while it provides a base for further definitions of terrorism, remains inadequate because it does not delineate which criminal actions and groups fall under the definition of terrorism or the potential motivations behind acts of terrorism. This lack of detail could permit certain perpetrators of particular acts of terrorism, such as violence that targets a specific ethnic group, to be punished only as general criminals. The classification as only a criminal undermines the threat that these individuals pose to domestic and international security. Even if the Legal Code included motivations for terrorism, violence to overthrow oppression might not apply, as the government may consider this excuse as a legitimate reason for violence. However, as demonstrated by the differing definitions of terrorism by the FBI and DOS, even domestic government agencies cannot agree upon the motivations behind acts of terrorism (U.S., Dept. of Justice, FBI, “Terrorism” and U.S., Dept. of State, Office of the Coordinator for Counterterrorism, “Executive Order 13224”).

The FBI separates its delineation of terrorism into two definitions, one for international and one for domestic terrorism, that encompass a broad variety of crimes from disrupting the peace to mass shootings. The Bureau defines international terrorism as any violent act instigated by groups or individuals and encouraged by or connected to foreign terrorist networks or sponsored by foreign states (U.S., Dept. of Justice, FBI, “Terrorism”). While the ideologies of these foreign entities provide the backdrop for these acts of terrorism, the violent incidents may occur abroad or in the United States. This definition would also include any violent actions committed by ISIS, al-Qaeda, their subgroups, similar terrorist networks, and those who declare allegiance to such organizations. The FBI does not specify which actions constitute terrorism (such as shootings, bombings, stabbings, or other forms of violence), the scale and severity of the acts of terrorism, and the locations of the attacks (such as whether they occur on public or private property). This definition also lacks an explanation for the motives behind these actions, though the political, racial, economic, social, cultural, and religious ideas espoused by foreign governments and foreign terrorist organizations that would likely explain such terrorist attacks.

The FBI specifies the definition of domestic terrorism more than its international counterpart. The Bureau characterizes domestic terrorism as violent actions instigated by American-based groups or individuals that hold extremist political, religious, social, racial, or environmental beliefs against any government or group of people (U.S., Dept. of Justice, FBI, “Terrorism”). This classification includes the Ku Klux Klan (an extremist, whites-only group, which attacked Americans of other ethnicities and races) and the May 19th Communist Organization (a violent anti-capitalist and anti-government group that attacked American civilians and property) (U.S., Dept. of Justice, FBI, “CATHERINE” and “DONNA”). This definition, however, also includes individuals who possess no obvious connection to terrorist ideologies, actions, or groups. The FBI website’s “Most Wanted Terrorists” section lists criminals wanted for aiding and abetting, obstruction of justice, armed bank robbery and killings, and interference with interstate commerce by robbery, though the description of these people does not claim radical/ extremist inspirations or ideologies (U.S., Dept. of Justice, FBI, “CHERI”). The reason for the broad conceptualization of domestic terrorism could result from the government’s desire to severely punish individuals who commit violence directly or indirectly against the United States government and civilians, whether they act as lone-wolves or as groups. However, this theory must remain as mere speculation without tangible proof from the individuals who created this definition.

The U.S. Department of State’s description of terrorism, while it does not differentiate between domestic and international terrorism, differentiates between foreign state-sponsored and non-state sponsored terrorism, per Executive Order 13224. This executive order, from which the DOS derives its definition of terrorism, prohibits the funding of foreign terrorist networks and individuals and identifies the characteristics necessary for the U.S. government to classify organizations and individuals as terrorists (as defined in section 140(b)(2) of the 1988 and 1989 Foreign Relations Authorization Act). Unlike the FBI’s inclusion of domestic individuals and groups, one of Executive Order 13224’s stipulations requires that those entities identified as terrorists must be foreign. These agencies (as recognized by the Secretary of State in association with the Attorney General and the Secretary of the Treasury) perpetrate, or run the risk or perpetrating, terrorist actions that endanger the safety of American citizens, national security, foreign policy, or economy. The order continues on to define "terrorism" as activities which (1) include violence or endanger human life, infrastructure, or property and (2) seem to occur with the intent to terrorize or compel civilian groups; to interfere with government policy-making through fear and compulsion; or to disturb government business through murder, kidnapping, large-scale devastation, or "hostage-taking" (U.S., Dept. of State, Office of the Coordinator for Counterterrorism, "Executive Order 13224"). Under this definition of "foreign terrorism," the DOS published a list of foreign terrorist organizations on October 8, 1997 (before ex-President Bush signed Executive Order 13224) that the Department continues to update, which includes organizations such as Islamic State of Iraq and the Levant (ISIL/ ISIS), Al Qaeda (al-Qaida), al-Shabaab, Boko Haram, and their subgroups and regional branches (U.S., Dept. of State, Bureau of Counterterrorism, "Foreign Terrorist Organizations").

Facebook Inc., while a private company, defines terrorism through a similar lens to the DOS so that it can attempt to control the presence of terrorist individuals and groups on its social media sites (which include Facebook and Instagram). Unlike the DOS, Facebook classifies terrorism as existing both domestically and internationally, regardless of political and religious beliefs and the location of origin. The social media giant identifies groups, not individuals, on its site as terrorism threats if they perpetrate pre-determined violent acts against humans or against public and private property in order to terrorize civilian groups, international organizations, or governments to accomplish religious, ideological, or political goals. Since Facebook recognizes governments' legal rights to a monopoly on violence in most cases, the company does not characterize governments as terrorists, though the site bans certain videos and photos that show state-sponsored violence per its "graphic violence policy." The company sites its examples of terrorist groups as those based upon white supremacy, religious extremism, violent separatism, and violent environmentalism (Bickert). Such delineations would include the Ku Klux Klan (white supremacy), ISIS/ ISIL (religious extremism), Palestinian Hamas (violent separatism), the Earth Liberation Front (violent environmentalism), and all related profiles, pages, and groups. Whether or not Facebook sends potentially useful information from such entities to international governments for terrorism prevention remains unclear through my research. Since the company possesses no legal, physical punitive authority, however, Facebook's interests appear to lie in the elimination of terrorist content in order to protect its profits, which the company gains through investments by other companies.

Because my definition of terrorism aims to set the boundaries for data collection and analysis of terrorists' Facebook pages and groups by American governmental counterterrorism agencies, I propose a new classification that both combines and broadens the definitions of the U.S. Legal Code, FBI, DOS, and Facebook. I characterize terrorism as any verifiable threat or act of violence against civilian and government populations and property committed by individuals or groups in order to promote extremist ideologies or prohibit other ideologies through the fear of future attacks. Terrorism may exist in both the United States and abroad, regardless of terrorist or terrorist group's location of origin. A verifiable threat, in this case, signifies that the threat would likely become an action, as the person or group who makes the threat has a history of violent actions and thoughts and/or possesses ties to a terrorist organization. Violence in this definition of terrorism represents shootings, bombings, stabbings, or other types of destructive behavior that intentionally result in long-standing fear, injury, death, or property destruction. Per the delineation of terrorism by the DOS, this violence violates the right to life, liberty, security, and the pursuit of happiness (so long as this pursuit does not harm others), as said acts of terrorism generally interrupt the flow of everyday life and the stability of countries, even if the acts do not involve human death or injury (U.S., Dept. of State, Office of the Coordinator for Counterterrorism, “Executive Order 13224”). This willingness to resort to violence in order to forward various ideologies does not itself render these ideologies as “extremist” (115 Stat. 376). Extremism also involves an ideological and deep-seated hatred towards particular ethnic, religious, economic, political, or social groups that the individuals or groups holding such beliefs want radically changed or eliminated.

Under this definition of “terrorism,” all groups characterized by acts of violence (delineated above) because of extremist ideals may be classified as “terrorists,” as well as any individuals directly connected to and inspired to act violently by these groups. The most infamous groups (Al-Qaeda, ISIS, Al-Shabaab, Hamas, Hezbollah, and Boko Haram) would thus counts as terrorist networks, as would their sub-groups, regional branches, members, and similar groups. As is the case with the FBI and Facebook’s definition, my description would also include the Ku Klux Klan (because its violence against minorities due to a long-standing hatred of non-whites and non-Protestants) and the May 19th Communist Organization (because of its violence against capitalist and democratic systems) (U.S., Dept. of Justice, FBI, “Terrorism” and Bickert).

My definition’s broad inclusion of who may count as a terrorist sets it apart from the definitions by the government and Facebook. Instead of delineating between international and domestic terrorism (like the U.S. government) or differentiating between groups and individuals (like Facebook), I provide one definition that considers both individuals and organizations to commit acts of terrorism anywhere in the world, regardless of the terrorists’ locations of origin. As demonstrated by the U.S. Code § 2331 and the FBI (but not by the DOS or Facebook), terrorism may occur in the U.S. and abroad, and the terrorist individuals or groups who perpetrate terrorism may station themselves in America or internationally. However, I do not differentiate between domestic and international terrorism, as the U.S. Legal Code and the FBI do, because both types of terrorism encompass similar actions and intentions. I also define the reason for terrorism, extremist ideologies, and provide a description of the meaning of extremism. While the FBI and Facebook somewhat address this characteristic (though they do not define extremism), the U.S. Code § 2331 and the DOS do not. I consider the purpose behind terrorism important because the motivation behind terrorist threats or actions separate it from other cases of threats or acts of violence due to the desire to spread fear in a large population in order to achieve some sort of institutional or policy change. Without this inclusion, the government could apply terrorism to many more or many fewer criminal cases, causing undue punishment or a lack thereof.

### I.III Methodology and Outline

In this thesis I discuss the American government's relation to terrorism and counterterrorism, and how the government can benefit from the collection of information from Facebook and Twitter, in order to create a solution that would allow the government to obtain such information. While the first chapter introduces the concept of terrorism, the second contains a discussion of the inefficacies of counterterrorism tactics in the United States that necessitates an additional strategy. I introduce the modern American history of counterterrorism that begins with the terrorist attacks on September 11, 2001. This information is necessary to understand the government's motivation for high counterterrorism expenditures, as well as the wide variety of tactics employed and agencies involved. The devastation of 9/11 created a belief of "never again" in the government that today drives it to annually spend billions of dollars to combat terrorism and to fund various strategies with arguable degrees of success (Nowrasteh). I begin with a discussion of the United States' total counterterrorism budget, as this information highlights the importance that the government places on counterterrorism. I then discuss the functions of the National Counterterrorism Center (NCTC), because the NCTC combines the efforts and intelligence of all the American counterterrorism agencies and plays a central role as the information distribution point in my policy. Chapter II does refer to other agencies, including the Department of State, Federal Bureau of Investigation, and Department of Defense, in terms of their general contributions to counterterrorism and the total budget of all of their strategies. Because I concentrate on the FBI and DOS in my classification of terrorism, I discuss their tactics in specific detail. I discuss the FBI, DOS, and DoD because their counterterrorism efforts cover those of other agencies. I use older information on the DoD's tactics (from 2006) because many of the DoD's current counterterrorism strategies remain classified, and I do not possess a security clearance to obtain said information (nor could I discuss classified information in this thesis).

In the second major part of Chapter II, after the description of current counterterrorism methods, I present my literature review as a discussion of scholars' views on the efficacy of American counterterrorism strategies. I analyze the tactics' efficacies in terms of money spent versus success in preventing terrorism and their ethics in terms of civilian and infrastructural damage versus terrorism attacks prevented and lives saved. I address military drone strikes, as opposed to other specific military counterterrorism strategies, because of ethical problems that arise from the high death toll and infrastructural damage. The analysis demonstrates the necessity of new counterterrorism tactics, illustrating the importance of my method.

In the third chapter, I begin by discussing the specific benefits that Facebook and Twitter can provide to counterterrorism efforts in terms of the amounts and types of information that these social media sites contain. I focus on social media overall as an effective counterterrorism solution because of the wealth of data that users can instantaneously disseminate world-wide, such as their locations, interests, family, and friends. Because social media permits a rapid spread of information and an easy method to create new accounts, terrorist maintain a constant presence on social media (U.S., Dept. of Justice, FBI, "Terrorism"). The American government already recognizes this threat and convicts suspected terrorists based on publicly-displayed content and tip-offs from other users (U.S., Dept of Justice, U.S. Attorney's Office: District of New Mexico, "Two New Mexico Men"). Government agencies also currently collaborate and share sensitive information with social media companies for reasons other than counterterrorism, such as identifying threats from foreign governments (Breland). I use Facebook and Twitter specifically, as opposed to other sites like Snapchat and Instagram, because these sites directly target terrorism on their platforms (Steinbach). Twitter and Facebook also provide the most information available on terrorists, from detailed profile pages to special interest group participation. The sites also already collect data on their users, and American government could use terrorists' data to identify, track, and arrest or extradite suspects and to prevent terrorist attacks (Domonoske and Geiger). The information that I use comes from articles and from an analysis of my personal pages so that I can identify all potentially available content and the uses for this content (though I do change my specific information for this thesis in order to protect my privacy). I then describe Facebook and Twitter's moral and legal obligations, or lack thereof, to share information on terrorists with American counterterrorism agencies.

After I discuss the benefits of Facebook and Twitter, I provide four case studies of terrorist groups which Facebook and Twitter have identified and repeatedly removed from social media. I include ISIS, Hamas, Hezbollah, and Al Qaeda as my examples because American journalism discourse about terrorism on social media focuses most on these organizations, the DOS identifies them as state-sponsored terrorist organizations, and they fit my definition of terrorism (Silver and Frier and U.S., Dept. of State, Bureau of Counterterrorism, "Foreign Terrorist Organizations"). These four groups all use violent actions against civilian and government populations in order to achieve their objectives. I use these case studies to illustrate the pervasive and persistent existence of terrorists on social media and how Facebook and Twitter attempt, through their own methods, to prevent the spread of terrorism through their platforms. I discuss the problems that the social media companies face in the removal of these organizations to demonstrate that Twitter and Facebook do not effectively detect and remove terrorists' information from the sites.

In the Chapter IV, I detail a counterterrorism policy proposal that would protect American counterterrorism agencies' ability to use the information on terrorists collected from Facebook and Twitter. This policy would legally obligate the social media companies to share with the counterterrorism agencies the information that the companies gather on suspected terrorists. The identification of "terrorism" and "terrorists" would occur under my definition of terrorism so that the government and social media sites could more effectively coordinate their efforts. The policy would also allow the government to charge suspected terrorists based on their social media activity. After detailing the policy, I discuss its positive aspects for both the government and Facebook and Twitter. I then identify the potential downsides of the policy for the government and social media sites, including practical and ethical concerns. To conclude this chapter, I work to negate these issues through a discussion of how the benefits of the policy and historical examples demonstrate why this policy should still be implemented.

In the concluding chapter, Chapter V, I summarize why the inefficacies of current American counterterrorism methods necessitate my new strategy. I then address possible points of expansion for my policy, such as by expanding the subject matter and online platforms covered and by allowing the government to take a more direct role in the identification and collection of terrorism information on social media. After discussing these expansion possibilities, I discuss some of the technical and ethical difficulties that they would face. If I expanded the policy to include sites such as YouTube, Snapchat, or Google, as well as Facebook and Twitter, the amount of data that counterterrorism agencies would need to monitor would increase infinitely. This growth of information would subsequently require a substantial increase in the government personnel necessary for analysis, which could reduce the cost-saving benefit of my policy. Ethical issues, especially concerning the privacy of personal information, would pose a much more severe problem if the government extended the policy in order to take a direct role in the monitoring, collection, and analysis of social media data than if Facebook and Twitter just passed along such information. These issues, I argue, caused me to limit my policy to its current point. To conclude, I speculate briefly on the future of counterterrorism in the United States and the impossibility of a final defeat of domestic and international terrorism.

### I.IV Moving Forward

This thesis serves as a policy proposal for a new counterterrorism method that American counterterrorism agencies could utilize in addition to current tactics. The policy would allow the government to legally obtain information on terrorists gathered by the security teams at

Facebook and Twitter and to then use this information to convict suspected terrorists. The goal of this policy is to eventually reduce the cost of current information gathering techniques by providing the government with data already collected by the social media sites, free of charge. Due to the detailed information contained on social media about each user, the government could also gain a more exact location estimate for suspected terrorists, which would permit it to more directly target terrorist strongholds, theoretically reducing the cost and civilian impact of current military counterterrorism strategies. While U.S. counterterrorism agencies may already utilize this technique, available research from the Edward Snowden leaks only indicates that the National Security Agency monitors and collects data from Facebook activity by exploiting the site's technical weaknesses through project US – 984 BLARNEY (Greenwald 137-64). I therefore treat my thesis as a speculation and suggestion and must explain why current American counterterrorism tactics necessitate my new counterterrorism method.

# Chapter II: Conceptualizing Counterterrorism

## II.I 9/11: America's Rude Awakening

On the morning of September 11, 2001, two hijacked commercial airplanes crashed into the World Trade Center in New York City. A further two hijacked plane attacks followed, with crashes into the Pentagon in Washington D.C. and in a field in Shanksville, Pennsylvania. American intelligence identified the terrorist group Al Qaeda as responsible for the organization and execution of this event. The devastation of the attacks left the world in a state of shock, and leaders from around the world, including Cuba and Russia, sent their condolences to the United States (U.S., White House Press Center, White House Briefing Room). While the crashes occurred on U.S. soil, the approximately 3,000 dead and missing victims represented over 80 nations and prompted international support for what became officially known as the "Global War on Terrorism" (U.S., Dept. of State, The Coalition Information Centers). While the United States recognized and attempted to counteract terrorism before September 11, 2001, the shock and tragedy from that day heightened the government's efforts.

Within the first 100 days, the American government's strategy to rebuild the country and to thwart terrorism included seven tactics executed simultaneously: aiding survivors of the attacks, respecting Islam, homeland security, law enforcement, diplomacy, aid to Afghanistan, and military campaigns. To assist the victims and their families, the federal government donated around $52 million, on top of the approximately $1.3 billion raised by private organizations and companies. President Bush and his staff worked to demonstrate solidarity with Muslims across America and world-wide through meetings and events with Muslim-American communities and messages of solidarity and tolerance. As sporadic attacks in the following months also victimized Muslim and Sikh Americans, the government implemented several non-discrimination laws and assisted local and state law enforcement in prosecuting perpetrators of hate-driven violence against individuals with Middle Eastern backgrounds. In addition to these efforts, the government donated money to aid in the rebuilding of disaster zones, for healthcare for displaced Americans, and for increased law enforcement, intelligence, and military efforts for an estimated cost of $20 billion. President Bush also created the Department of Homeland Security to coordinate information gathered by American intelligence agencies and to defend the country against future terrorist attacks. Outside of the United States, the federal government worked with foreign leaders to condemn and thwart acts of terrorism world-wide. After the first 100 days, America deployed under 3,000 troops to the Middle East, especially in Afghanistan, to seek out and destroy terrorist strongholds. The government also tasked these troops to deliver food, healthcare, and other forms of aid to Afghani civilians in order to counteract the destruction caused by terror attacks and American military tactics (U.S., Dept. of State, The Coalition Information Centers)

Since 9/11 the United States government has both expanded and modified its counterterrorism efforts due to changing technology and terrorism threats. The Department of State still relies mainly on diplomacy and humanitarian efforts in order to prevent the popularization of terrorism, to fight terrorism legislatively, and to contend with the destruction of terrorist attacks (U.S., Dept. of State, Office of the Spokesperson, “Global Counterterrorism Forum”). The Federal Bureau of Investigation and Department of Homeland Security deal with law enforcement and intelligence to ensure internal security (U.S., Dept. of Justice, FBI, “Terrorism”). The Department of Defense handles counterterrorism military campaigns world-wide (U.S., Dept. of Defense, Office of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff 5-8). The Central Intelligence Agency uses all-source intelligence collection and covert operations to target terrorists (U.S., CIA). All of the agencies depend on coordinated information and efforts in order to effectively counteract terrorism, which they conduct through the National Counterterrorism Center, created in 2003 under the name Terror Threat Integration Center, to allow for unrestricted access to intelligence (Wiley). Despite the many agencies involved in counterterrorism, the efficacy and ethics of the United States' efforts since September 11, 2001 remains contested by researchers and scholars. This chapter analyzes the effectiveness of current American counterterrorism strategies in order to promote the necessity of an additional, more effective tactic.

### II.II How the United States Government Combats Terrorism Post 9/11

Regardless of U.S. government agencies' different definitions of terrorism, they each dedicate extensive amounts of time, money, and effort towards combatting terrorism. Because each government counterterrorism agency within America operates under a different definition of terrorism, the specific tactics which each agency uses tend to differ, though the strategies behind the tactics converge. A variety of agencies combat terrorism, including the CIA, FBI, DoD, DHS, DOS, NSA, NIMA, and OMB. Since each of these bureaus and departments contains several counterterrorism agencies, ranging from intelligence collection, analysis, and dissemination to terrorism prevention and crisis responses to military actions overseas, I describe general counterterrorism practices and then focus on the strategies of the DOS, the FBI, and the DoD.

The cost of counterterrorism programs remains difficult to calculate, as the U.S. government does not openly reveal its total (or, in certain cases, departmental) annual counterterrorism budget to members of the public. The best estimate for the Department of

State’s annual counterterrorism budget comes in the form of a testimony before the Subcommittee on Terrorism, Nonproliferation, and Trade of the House Foreign Affairs Committee on September 7, 2017 by Ambassador-at-Large and Coordinator for Counterterrorism Nathan A. Sales. Ambassador Sales requests more than $288 million for DOS counterterrorism efforts in the 2018 Fiscal Year, which represents a steady increase from the budgets of 2016 and 2017 (Sales). Private governmental research institutes, such as DefenseNews, the Cato Institute, and the Stimson Center, estimate the total cost of counterterrorism efforts between 2002 and 2017 to equal $2.8 trillion, for a rough estimate of $150 billion to $186.6 billion per year (Belasco et al). In these fifteen years, the DoD spent $1.7 trillion on emergency and overseas contingency operations, Homeland Security spent around $979 billion protecting American borders and the interior, the DOS/ USAID spent $138 billion on war-related costs, and other agencies spent $11 billion on non-OCO international aid (Mehta).

While each agency involved in counterterrorism may work independently on specific strategies, counterterrorism agencies also collaborate by sharing information. In order to more effectively share information with other agencies involved in counterterrorism across the American government (the DOS, DoD, NSA, DHS, FBI, NIMA, OMB, and CIA), the Directors of Central Intelligence and the FBI, along with the Attorney General and the Secretaries of Defense and Homeland Security, created the Terrorist Threat Integration Center (TTIC) in 2003. The TTIC coordinated intelligence-sharing between all agencies involved in counterterrorism so that the involved agencies could prevent a higher number of terrorist attacks and otherwise disrupt the functions of terrorist networks. The most important elements of the TTIC included full and unedited access for the U.S. government to all intelligence gathered (whether completed or not), control of nation-wide counterterrorism tactics and a regulations organization system, terrorist threat assessments based on intelligence gathered from all involved agencies available to government heads, and upkeep of a database containing certified and potential terrorists open to all federal, and particular non-federal, leaders and agencies. Individuals spanning the public and private sectors debated whether the TTIC achieved its intended goal of intelligence-sharing, but the lack of a coordination center pre-9/11 necessitated some form of cohesion to prevent such devastating terrorist attacks in the future (Wiley). In August 2004, under Executive Order 13354, the TTIC became the National Counterterrorism Center and eventually expanded its functions to include 20 different agencies with functions including mission management, information analysis and dissemination, and terrorism database maintenance. Given the NCTC's relative autonomy from other government sectors and its access to domestic and international terrorism data, the Center can avoid many concerns of other counterterrorism agencies (such as influences from the Legislature) and can more efficiently gather information (United States, Office of the Director of Natl. Intelligence, Natl. Counterterrorism Center).

The Department of State actively concerns itself with international affairs and terrorism. Hence, the DOS participates highly in public transnational counterterrorism efforts. The Global Counterterrorism Forum, a program which started in 2011 and involves 30 countries, devotes itself to categorizing the counterterrorism needs of civilians, coordinating the knowledge and products to tackle those needs, and increasing international collaboration. The GCTF works to counter terrorism at the global civilian level by donating money towards community-building and the development of stable legal and political systems in areas where terrorism is particularly potent, supporting victims of terrorist attacks and establishing organizations to prosecute or rehabilitate (if possible) offenders, and educating on and implementing civilian-led groups to counter violent extremism (U.S., Dept. of State, Office of the Spokesperson, "Global

Counterterrorism Forum”). The DOS also participates in the Global Coalition to Defeat ISIS, inspired by the United Nations Security Council Resolution 2170, which promotes the cooperation of all states as necessary to counteract terrorism. America (through the DOS) actively participates in this coalition and encourages all states to support the cause in any way possible, including military efforts, humanitarian support, defunding ISIS, preventing the influx of fighters, and exposing ISIS’ atrocities (U.S, Dept. of State, “The Global Coalition”). Both the GCFT and the coalition fall under the DOS’s Bureau of Counterterrorism. These programs and initiatives require collaborations with other countries and their counterterrorism organizations in order to function effectively.

The Federal Bureau of Investigation, though relevant international information and intelligence remains crucial to its efficiency, concentrates on counterterrorism efforts as they affect the United States. Thus, the FBI monitors both domestic and foreign terrorist individuals and groups that are known or suspected threats to the security and functioning of America and works to combat terrorism threats in the nation as its priority. Because of the ever-rising popularity of technology and the internet, counterterrorism efforts increasingly target the internet, social media, and homegrown violent extremists (HVEs). Terrorist individuals and networks recognize the potential of the internet and social media to gain new recruits world-wide, to plan attacks, and to spread information and extremist ideologies. To combat these threats, the Bureau utilizes a variety of strategies, including intelligence gathering and analysis, collaboration with other (unspecified) entities, surveillance of suspected and known terrorists, and the promotion of national community preparedness and information sharing (U.S., Dept. of Justice, FBI, “Terrorism”). The FBI also works vertically through its Joint Terrorism Task Forces, coordinating counterterrorism information and efforts with security partners on a local, state, and federal level (Schiff and Heimbach). As the FBI uses various classified missions and methods in its fight against terrorism, the extent of its technology and capabilities remains unknown to the public, especially modern tactics involving the minimization of terrorism threats on social media.

Like the FBI, the Department of Defense also utilizes classified technologies and strategies in its counterterrorism activities, but the DoD covers the military side of counterterrorism. The DoD's counterterrorism strategy contains three main elements: to protect and defend the United States, to provide support to Muslims that attempt to resist extremism, and to target terrorists and their ability to function domestically and internationally. The tactics used to achieve these goals occur both directly and indirectly, with direct strategies concentrating on American interests while targeting terrorists and indirect strategies focusing on the promotion of counterterrorism success by non-American entities (U.S., Dept. of Defense, Office of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff 5-6). Direct tactics undertaken against identified terrorist networks include the destruction of safe-havens, resources, and training camps; the capturing or killing of foot soldiers, senior leadership, and senior operatives; and the interruption of recruitment and training efforts. Indirect efforts comprise the provision of security, humanitarian aid, military-to-military contacts, conduct of operations, and military information operations to assist civilians and counterterrorism groups in areas of pervasive terrorist activity (24-7). The Department attempts to coordinate all information and tactics with both domestic and international governmental partners in order to increase the effectiveness and efficiency of its counterterrorism methods, but it operates alone when necessary. Whether the money spent by the Department of Defense and the U.S. government on counterterrorism measures effectively achieves its goals, however, remains contested by counterterrorism scholars and researchers.

### II.III Literature Review: American Counterterrorism Strategies and Efficacy

Opinions on the efficacy of American governmental counterterrorism efforts and spending vary based upon the position of the analysts and upon their biases and reasons for said analysis. A Cato Institute researcher, Alex Nowrasteh, analyzes general U.S. counterterrorism expenditures (both domestically and internationally), which he deems inefficient. Nowrasteh posits that, to be effective, the $2.8 trillion spent on counterterrorism since 9/11 would have to have saved a total of 188,740 lives since 9/11, or 11,796 per year (given a hypothetical value on life at $6.5 million and a budget of $13 million to save that life).[1] From 2002 to 2017, Nowrasteh estimates that only 174 civilians died on American soil as a result of terrorist attacks. Thus, American counterterrorism tactics would have to have saved 1,074 times as many lives if the total counterterrorism budget were truly effective (Nowrasteh). Nowrasteh's research implies that the inefficient and ineffective use of counterterrorism funds harms lives instead of saving them, as civilians could die from other forms of homicide. This study indicates that American counterterrorism practices, including intelligence, military tactics, security checkpoints, and counterterrorism education suffer from strong inefficacy levels. In order to justify its high counterterrorism budget, the government must consider a redistribution of its funds and the use of more effective counterterrorism techniques.

Counterterrorism scholar John Mueller focuses on an analysis of the FBI's overall counterterrorism spending, particularly in terms of chasing suspected terrorists, instead of on the

[1] Nowrasteh does not address his methodology for these estimates and only indicates that he chooses a value in the millions because of an assumption that people highly value human life.

efficacy and ethics of specific strategies. According to Mueller's estimates, the FBI spends $3 billion a year tracing 10-20 million (mostly false) terrorist leads. Other than the Florida nightclub shooting in 2016, only around 6 people in the U.S. die annually because of domestic terrorist attacks. Mueller argues that these attacks (which do not include school shootings or public shootings not related to terrorism) do not warrant a budget as high as $3 billion, especially when the FBI could focus more heavily on drug cartel activity in the U.S. (Mueller). Given that more than half of this budget does not counter verified acts or threats of terrorism (and instead goes towards the chasing of false or dead-end leads), the inefficiency rate of current FBI seems high, insinuating that the agency should look further into more efficient methods for verifying leads and threats and for tracking leads. As much of the FBI's activities and data remain classified, and John Mueller does not state whether he uses public or classified information, his estimates may not represent the true efficacy of FBI tactics. The FBI may stop more potential terrorist attacks and save more lives through top-secret intelligence tactics that warrant a high counterterrorism budget.

Another analysis performed by John Mueller, in conjunction with Mark G. Stewart, indicates high inefficacies in American domestic counterterrorism intelligence. The researchers measure the efficiency of strategies versus the counterterrorism intelligence budget in terms of the costs of tactics, the reduction rate of attack risks due to the tactics, the chance of a successful terrorist attack, and the cost of a successful attack. Though Mueller and Stewart admit that the results of their research change if they place more weight on deaths from terrorist attacks than those by other dangers, given that only 54 Islamist-related terrorist attacks occurred after September 11, 2001 to 2014, the total cost of damage (including human lives, infrastructure damage, and economic disruption) would only equal about $500 million. As compared to the (conservative) $75 billion estimate that Mueller and Stewart use as their budget example for counterterrorism intelligence, this discrepancy reveals that the cost of preventing verified acts of terrorism does not warrant such high expenditures (Mueller and Stewart 237-248).  The differences in costs also indicate that the involved agencies use most of these funds for strategies with variable degrees of success and for following dead-end or false potential terrorist leads. If counterterrorism agencies spend such a high amount of money on costly and fruitless ventures, they lack the ability and the tools to verify the credibility of terrorism threats and leads. This research study could lack in the knowledge of top-secret government practices and thwarted terrorist attacks (and the extent of government secrecy remains largely unknown); however, given the information available, counterterrorism intelligence practices appear to suffer from high inefficiencies.

Instead of analyzing cost as a measure of effectiveness, researcher Michael J. Boyle concentrates specifically on the efficacy and ethics of drone strikes as a means of counterterrorism. While U.S. government officials under the Obama administration praised the accuracy of drone strikes, arguing that they targeted terrorist groups and not civilian populations, Boyle counters that these proclamations do not accurately represent current research data on drone strikes. According to Boyle, both critics and proponents of drone strikes cite different data sets (from NGO or government reports) about casualty types (terrorist or civilian) from drone strikes, but neither side truly knows the full extent of casualties, as the American government either does not collect such information or will not reveal it. The government also practices guilt-by-association and defines individuals as “militants” or “terrorists” without much evidence. This strategy of committing drone strikes with little information equates to the targeting of possibly innocent civilian populations, leading to mass fear, injury, death, and destruction (Boyle 3-8).

Regardless of the number of civilian casualties, American drone strikes cause fear in the general public of the targeted countries and result in anti-American and anti-Western sentiment. These ideas, in turn, can result in higher recruitment for groups like Al-Qaeda, which the drones initially intended to kill and disrupt, making it one of the most ethically costly American counterterrorism efforts (14-21). From Boyle's analysis, the cost of human death and infrastructure damage may equate to a higher price than that of the drone strike itself, but comprehensive estimations remain impossible to determine without data collection efforts. However, drone strikes seem to be the most psychologically and physically damaging of counterterrorism efforts to civilians, based on the impact on the populations affected by drone strikes. The unintended consequences caused by the aftermath of drone strikes, including the increased support and recruitment for terrorist groups and the anti-American beliefs, could necessitate a higher counterterrorism expenditure by the U.S. government in the future. If counterterrorism does necessitate violence on some level, this information indicates that relevant agencies must develop tactics that directly target known terrorist locations and that minimize attacks on civilians and infrastructure. Otherwise, the American government will continue to create more enemies and feed the growth of terrorism.

### II.IV Necessary Changes

The American government has continued to increase its counterterrorism efforts and budget in the years since 9/11. The total counterterrorism budget now ranges in the trillions of dollars and covers at least a half-dozen agencies. The DoD, DOS, DHS, FBI, NIMA, OMB, NSA, and CIA each include counterterrorism agencies that employ a wide array of strategies.

The tactics of these agencies cover intelligence, military, diplomacy, terrorism and counterterrorism education, and peace-building strategies in the United States and world-wide.

Though the American government publicly promotes the effectiveness of its counterterrorism actions, various international organizations and scholars criticize the fiscal and ethical cost of such practices. Certain critiques involve the financial cost of these efforts as compared to their success rates. Other American counterterrorism practices, such as drone strikes, face heavy international criticism surrounding their ethical viability, as they result in high human casualties, resource loss, and infrastructural damage. Despite the lack of government transparency regarding its counterterrorism budget and successes, scholarly analysis of various counterterrorism actions versus lives saved and terrorist attacks thwarted reveals a large discrepancy of funds that could be spent on preventing other violent crimes (such as drug wars or human trafficking). While the general public may find such high spending necessary, regardless of the authenticity or accuracy counterterrorism efforts, U.S. counterterrorism agencies need to streamline their efforts and to create a cheaper, more efficient, and more effective system through which to track terrorists and thwart their attacks. This new method would work in conjunction with current strategies to reduce the amount of money spent and lives lost as a result of American counterterrorism actions, which would thus increase terrorism prevention world-wide.

## Chapter III: Facebook, Twitter, and Counterterrorism

### III.I Current Efforts

Like the United States government, Facebook and Twitter also acknowledge the threat of terrorism on their platforms. As of 2018 Facebook's counterterrorism team included around 200 employees, who daily monitor and delete new and old terrorist content that the site's algorithm technology detects. While the company's detection tools do not catch all instances of terrorism content, Facebook officials claim that they modify these tools each time in order to keep up with the changing nature of terrorists' posts and accounts. The social media company announced that, in the first fiscal quarter of 2018, it managed to remove around 1.9 million pieces of information from ISIS and Al Qaeda. 99% of the terrorism content removed in the same quarter was, according to the same report, identified by Facebook's detection technology and not by other users (Bickert and Fishman). The counterterrorism security team did not announce what percent of total terrorist content these 1.9 million content pieces represent, perhaps because of the difficulty even roughly estimating the total terrorist content due to the breadth of information stored on Facebook.

Twitter also uses technological tools to identify and eliminate terrorism content on its platform. In the report "Twitter Rules enforcement – January to June 2018," Twitter announced that it suspended 205,156 accounts for incidents related to the promotion of terrorism. According to the study, Twitter's technology identified 91% of these cases, with the remaining 8% reported by other users, including U.S. and foreign government accounts. The report acknowledged that the suspension of accounts in this period represented a 25% decrease from the last study period, but the company correlated the reduction to the increased efficacy of its tools ("Twitter Rules enforcement"). Twitter did not discuss whether its content review teams include a specific subset for terrorism content (included under the company's "Violent Threats Policies"), nor did the site identify whether it modifies detection tools based upon missed threats. Despite these uncertainties, Twitter does appear on the surface to enjoy relative success in discovering and deleting terrorism information.

Regardless of the companies' successes, news sources and private studies from groups such as WIRED and the Digital Citizens Alliance reveal that terrorist content still maintains a firm hold on Facebook and Twitter. To remove all instances of terrorism information from any online site remains impossible, but critics argue that these social media companies' do not expend enough time, money, and technology to cause a significant difference (Macdonald). But what if Facebook and Twitter worked directly with American counterterrorism agencies to defeat these terrorists on social media? The chapter addresses the types of information which the government could obtain on social media from terrorist groups. This chapter identifies four cases of well-known terrorist organizations on Facebook and Twitter, Al Qaeda, ISIS, Hamas, and Hezbollah, in order to identify their persistent nature on social media and the sites' inability (and possible refusal) to remove them completely, which necessitates government intervention due to the threat that these groups pose to civilians. I argue that, if Facebook and Twitter freely shared information with U.S. counterterrorism agencies, the government could more easily identify and target these terrorists, which would thus save the social media sites from having to continuously remove content from these same individuals.

### III.II The Benefits of Facebook

If Facebook did share identified terrorists' information with governments, what types of data could American counterterrorism agencies obtain? Facebook's settings permit privacy for most information. The possible settings include “public,” “friends of friends,” “friends,” or “only me” options in terms of which users can view individual and group account data. Even if a user or group selects “only me” for all possible privacy options, a few pieces of information remain public, which counterterrorism agencies can use regardless of whether Facebook shares information: the name of individuals and group members, all profile pictures, and all cover photos. If the pictures include people, counterterrorism agencies can perform facial recognition analysis. Counterterrorism agencies need to identify the appearances of terrorists in order to determine their exact locations. These individuals, however, could change their appearances in order to evade capture by the government. Facebook already, if unintentionally, covers this problem. The company uses advanced facial recognition tools, which can allow users to tag their friends in photos based on Facebook’s suggestions. If users chose not to tag their friends, Facebook’s facial recognition still stores the names and faces of individuals. The site’s technology analyzes facial features in photos in order to connect faces with names. The new tool can also alert users if someone tries to impersonate him or her through photos (Domonoske). Though the efficacy of this technology remains unknown, Facebook could use facial recognition on accounts that it links to terrorism. This facial recognition technology could thus permit counterterrorism agencies to identify the faces of terrorists without searching for and analyzing photos themselves. This information would also allow agencies to recognize terrorists face-to-face or in other forms of media, potentially facilitating location identification.

Another crucial information from publicly-available account content on Facebook can also derive from photographs: location. Some photographs may originate from photoshop or from online stock photos, but other photographs (especially ones in which Facebook facial recognition connects the individual in the photo to the account owner) may alert the government to current or past locations. Even if a user does not specify a location in his or her posted image, counterterrorism agencies may recognize certain architectural and natural features (such as the Eiffel Tower or Niagara Falls) and thus can track the potential current location or past location patterns of a suspected terrorist. If the user uploads a picture from his or her phone, the photo comes with a publicly-available geo-tag (marker of the location in which the photo was taken) that counterterrorism agencies could also use to determine a user's location. If given full access to terrorists' Facebook data, the government could also identify locations from other posts either created by the users or by friends who "tagged" the users. Besides the location of a user's posts, he or she may also include places in which they live, work, and study either currently or in the past. All content posted to Facebook, whether public of private, also includes the date and time at which the user shared the material. In combination with the location of the post, the date and time can increase American counterterrorism agencies' potential to triangulate the current and past whereabouts of terrorists (Dewicki).

The full content of individual accounts on Facebook ranges from background information to personal interests to friends. The background information may comprise of the user's birthday, age, gender, a short biography, his or her email addresses and phone numbers, languages spoken, the relationship status, sexuality, and family members (Dewicki). Facebook even frequently stores information that users do not self-report, such as email addresses and phone numbers on individuals without Facebook accounts but whose contacts have accounts (a phenomenon called "shadow profiles") (Hatmaker). Counterterrorism agencies can utilize this content to gain background knowledge on an individual and to find possible points of contact with the individual through email, phone number, or family members. Some of the personal interests that users can post on their personal accounts include movies and television series, celebrities, sports, activities, and groups (both in real life and on Facebook) in which the individual either participates or enjoys. Photos, videos, and other content posted by users can verify and add to this information (Dewicki). Users can of course lie about this information, but if Facebook and/or the government could verify the validity of the content, these interests could assist American counterterrorism agencies in determining whether an individual poses a verifiable threat to national security (see I.II for a classification of a “verifiable threat”). If a user hypothetically “likes” many pages and celebrities who promote violence or hatred against specific populations, given that this information proves true, that person could present a terrorism threat to the United States and other countries.

The list of a user’s friends can also connect the individual to other potential or confirmed terrorists. Given open access to users’ friends lists, the government can identify all of the individuals’ Facebook friends, who follows the users’ accounts, and whose accounts the users follow (Dewicki). In analyzing a potential terrorist’s list of friends, a counterterrorism agent may discover connections to suspected terrorists, which would increase the likelihood that the individual is a terrorist. Psychologist Dr. John Horgan at Pennsylvania State University’s International Center for the Study of Terrorism found in his study of 60 former terrorists that terrorists with familial or friendship ties to terrorist sympathizers indicated an openness to terrorist recruitment and radicalization (DeAngelis). If these individuals possess Facebook accounts, they likely follow these friends and family members, identified on the suspects’ friends lists.

Group accounts on Facebook provide much of the same basic public information as individual accounts. The name of the group and its profile and cover images always remain public, as do the names of administrators and members (“Overheard”). Thus, counterterrorism agencies can perform facial recognition and location/ date identification analyses on at least a group’s public information (if Facebook does not give them access to private information). The public information for Facebook groups also lists all of the group members and group administrators (“Overheard”). With full access to private group information (which includes activities such as content posting and sharing), the government can identify other individuals who may create a security threat, especially if these individuals often actively participate in these groups.

While joining a terrorist group on social media does not necessarily mean that an individual is a terrorist, as the user could work as an undercover agent or journalist, a high rate of activity within the group could signify an individual’s interest in terrorism. The more actively a person participates in activities that spread extremist messages and terrorist content, the more likely that person presents a terror threat. According to police units from the United Kingdom, signs of possible online terrorist activity include the posting of content that promotes racial and religious hatred or violence, praises terrorists and violent terrorist activities, encourages individuals to commit acts of terrorism or violent extremism, or instructs on the creation of bombs (“Action Counters Terrorism” and “Signs of Possible Terrorist Activity”). Even if the group does not represent a threat or a terrorist organization, the Facebook interface often provides users with suggested “related groups” that may interest the user (“Overheard”). These similar groups may pose veritable threats. Assuming that Facebook security software already scans individuals, groups, and content related to terrorism and shares that information with American counterterrorism agencies, the agencies could obtain this information from Facebook without scanning for it themselves.

### III.III The Benefits of Twitter

In terms of permanently publicly-available content, Twitter provides much of the same information as Facebook. An account with all privacy settings turned on shows only the user's account name, current profile and cover photos, Twitter handle ("@..."), and the month and year joined (@dew_mari). Thus, assuming the user uploads a real photograph of him or herself in a real location, counterterrorism agencies can still perform facial and location recognition analyses, regardless of whether Twitter shares the individual's full account information. The images on a "fully" private account on Twitter do not, however, include the location, day, and time at which user uploaded the cover and profile images. Past versions of these images remain hidden as well, rendering location patterns difficult to analyze unless the government receives full access to all content from a user's account. If Twitter granted U.S. counterterrorism agencies full access to suspected terrorists' accounts, the agencies could view all photographs and videos uploaded, as the day and time of the upload, and the location at which the users captures that media or at which they posted the content (@dew_mari). This content would allow agencies to analyze location and facial recognition patterns so that the government could identify a suspected terrorist in other media content or in real life and could determine the suspect's potential location.

The Twitter interface also allows for the upload of personal information similar to that of Facebook. A users' account may include his or her biography, birthday, age, gender, languages spoken, current location/ time-zone, email addresses, and phone numbers (@dew_mari). This information can also provide counterterrorism agencies with background knowledge on possible terrorists and with potential points of contact through email and phone. These agencies could also connect to suspects through the individuals' families and friends, included in users' “contacts” section with their names and relationships to users (@dew_mari). Families and friends, as well as a users’ followers and accounts they follow, may also provide an understanding of the types of people with whom the users interact. For example, if the government discovers that a user’s family members, friends, and followers possess connections to terrorist organizations, the user may be a terrorist. This likelihood may increase if that same user’s “interests” section or posting activity also demonstrate an interest in organizations, ideas, activities, and famous people (politicians, celebrities, etc.) who support or are connected to terrorism or terrorist activities. Users can of course easily falsify all of this information, but, if the content represents the truth, this information can provide data crucial to identify and track suspected terrorists. The ability of American counterterrorism agencies to obtain and analyze such data, however, depends on the willingness of Twitter to share it. And, despite the fact that terrorists pose a continuous problem for both Twitter’s and Facebook’s reputations and security teams, both companies appear reluctant to involve government assistance.

### III.IV Case Study 1: Al Qaeda

While the exact date of Al Qaeda’s emergence on Facebook and Twitter remains unknown, this group has maintained a presence on the sites since around 2009. At this time the terrorist group al-Shabab, working on behalf of Al Qaeda, updated its Facebook and Twitter followers on a failed French attempt to rescue a hostage by posting pictures of a uniform and alleging that the group had killed a French soldier. Later posts by Al Qaeda and its subsidiary groups from 2009 to 2013 continued along a different propaganda trend, including pictures and videos of members from the Jabhat al-Nusra group that demonstrated its “humanitarian” side by moving civilians out of lines of fire during battles and delivering aid. Facebook began to remove some of this content around 2013, but Al Qaeda and its sub-groups continued to post content and recruit followers (Prucha and Fisher 18-23). In a 2015 testimony before the U.S. Senate, Peter Bergen, a director at the New America Foundation and professor at Arizona State University, found 62 Americans whom Al Qaeda and similar groups recruited on social media. From these 62 individuals, Bergan discovered that terrorist network mostly targeted vulnerable populations, especially teenagers and young adults, of every ethnicity and gender. The propaganda posted by terrorist groups on social media likely inspired these individuals, as Bergan's study proved that 53 of the 62 individuals actively used social media to download and share jihadi content (U.S., Cong., Senate, Comm. on Homeland Security and Govt. Affairs 4-5).

Twitter and Facebook do attempt to remove the content and pages on their platforms that Al Qaeda uses to promote its cause and inspire civilians to join. In 2014 Twitter started to suspend accounts related to Al Qaeda, but these groups again created new accounts. Around that time the terrorist organization also employed the use of "bots" (accounts controlled by computers) to continuously develop new accounts after Twitter deleted others. The use of these bots results in difficulty for Twitter's security technology to identify and remove all information pertaining to Al Qaeda (Berger). A 2018 article by WIRED reported that, as of that year, content and accounts by Al Qaeda maintained a presence on social media, regardless of these companies' increased efforts to detect and delete related data (Lapowsky).

Despite the difficulty in completely eliminating the Al Qaeda's presence on Twitter and Facebook, private research studies indicate that these companies could take more steps to prevent this content from avoiding detection and continuing to flourish. J.M. Berger, a former research expert at The Brookings Institution, argued that social media companies needed more transparency in terms of their policies on account suspension and that the companies' criteria and rate for terrorism content detection and removal needed to remain consistent. A constant change in Twitter's and Facebook's identification and suspension techniques or a pause in this process could allow terrorists to regrow their social media networks and make them more difficult to manage (Berger). A 2018 report by the non-profit organization Digital Citizens Alliance posed a similar argument to Berger and added that a lack of legal and moral incentives perhaps prevented Facebook and Twitter from devoting as many resources to combatting terrorism on their sites as their extensive resources would allow ("Fool Me"). The report did not address methods or resources that social media companies could use to combat terrorism, but consulting with other companies or governments combatting online terrorism could prove useful.

### III.V Case Study 2: ISIS

Despite other terrorist organizations active presence on social media, ISIS' social media activity remains the most pervasive. In a 2016 testimony before the U.S. House of Representatives, FBI official Michael Steinbach identified ISIS as the greatest terrorism threat on social media. The group uses sites like Facebook and Twitter to recruit and communicate with supporters and to announce its ideologies and activities. Because of the global presence of social media and the rapid rate of communication (especially on social media messaging applications), this terrorist organization has successfully recruited hundreds of individuals from the United States alone, some of whom travelled to strongholds in the Middle East to actively join. Mubin Shaikh, a former Canadian jihadi advocate and current Canadian government employee, spends much of his time on Twitter in an attempt to counteract these recruitments. Shaikh claims that ISIS recruits both males and females of varying ages. In one instance Shaikh successfully intervened in the attempted recruitment of an American girl that the terrorist organization attempted to lure. His statement in a May 7, 2015 hearing before the Senate Committee on Homeland Security and Governmental Affairs proves that ISIS targets a variety of ages and genders on social media, including vulnerable youth, which may necessitate government intervention for the protection of civilians at risk of recruitment (U.S., Cong., Senate, Comm. on Homeland Security and Govt. Affairs 9-11)

ISIS' advocacy of violence, which the group posts on social media, poses another terrorism threat. The organization urges individuals across the world to take up arms and to attack, which caused several attacks and near-attacks in the United States and Europe in 2016 (Steinbach). The content that Facebook and Twitter do not detect contains messages along these lines, often including violent content. A report by WIRED Magazine in May 2018 analyzed several studies and concluded that Facebook and Twitter might not detect much of the terrorism content on their sites. Photographs and videos that promote anti-Western sentiments and show acts of violence still exist undetected and easily searched on social media. Researchers from the Global Intellectual Property Enforcement Center (GIPEC) and the Digital Citizens Alliance discovered a multitude of accounts still present on Facebook through chasing hashtags and keywords in Arabic and English. While Facebook may have deleted the content of these accounts, the site did not delete the accounts themselves (possibly because the accounts do not all post violent content), which permits terrorists to post more information. This content also continues to exist because Facebook algorithms mainly search related account clusters, which allows others to avoid detection (Lapowsky). Facebook detection technology scans for accounts with similar names or groups with connections through group members and administrators. Thus, Facebook's security systems often do not detect pages with names not included in these clusters and groups who contain different members and administrators than the account clusters.

The data pertaining to ISIS that the social media sites do discover also poses its own problems to civilians and to government counterterrorism efforts world-wide. No laws exist that would require Facebook and Twitter to share their stored information with the United States government unless agencies directly request the information through legal processes. Even when counterterrorism agencies request such data, social media sites may have deleted the content (though not the accounts) permanently from all storage platforms (Steinbach). This deleted content could prove crucial to counterterrorism efforts, from possible locations of terrorists and terrorist strongholds to planned terrorist attacks. As the social media companies possess no legal obligation to disseminate or store the information that they detect on terrorists, however, American counterterrorism agencies continue to lose a potential wealth of information.

### III.VI Case Study 3: Hamas

Hamas' use of social media creates a different issue than that of Al Qaeda and ISIS. Certain governments identify Hamas as a terrorist group, and others (especially Muslim-majority countries in the Middle East) recognize it as a legally-elected Palestinian political party or a group of "freedom fighters" that fights for Palestinian legal rights. The United States and certain allies may not distinguish Hamas as a legal ruling entity, but Palestinians in Israel's Gaza Strip elected this political party as a pseudo-governing entity. The fact that Hamas uses tactics such as suicide bombings and missile strikes against Israeli civilians causes Israel (and, thus, its American ally) to consider the group as a terrorist organization (Davidson). Facebook and Twitter, per their policies, may also not frame Hamas as a terrorist organization and thus may not focus their security sensors on Hamas' accounts and content. The fact that Facebook and Twitter focus their detection tools on Al Qaeda and ISIS may also explain why Hamas remains largely active on the sites. Posts by this group serve as a virtual "war" between Hamas and Israel. Hamas simultaneously shares content that shows the violence of Israeli troops against Palestinian civilians in order to gain international sympathy and content that shows the group kidnapping and killing Israeli soldiers in order to demonstrate the country's "weakness" (Patrikarakos).

Unlike Al Qaeda and ISIS, Facebook and Twitter barely target and remove content and propaganda posted by Hamas. Only after the Israeli government sent a letter in 2018 that threatened legal action against the companies did Facebook and Twitter remove content from Hamas in early 2018 (Carbone). Twitter suspended about twenty accounts related to Hamas after the Israeli Ministry Justice Cybercrime Department threatened to take legal action against the company (Middle East Monitor). Other than the few removed accounts, Facebook and Twitter generally remain popular spots for Hamas to spread propaganda and garner sympathy (Patrikarakos). Research into statements by Facebook and Twitter does not indicate if these companies consider Hamas as a terrorist organization and treat its content in the same way that they do for Al Qaeda and Hamas. Personal searches for Hamas on Facebook and Twitter, however, demonstrate that the group continues to post content under pages of its name. If threats of legal measures by governments primarily cause the social media companies to remove content by Hamas, then governmental laws requiring the companies to do so may present an effective solution.

### III.VII Case Study 4: Hezbollah/ Al-Manar

Like Hamas, Hezbollah's presence on social media remains contentious because, while some foreign governments may recognize it as a terrorist organization, other governing entities consider Hezbollah as a legal governing party. Despite its history of violent and anti-Western actions, the political party and militant group gained its power in the Lebanese government from the 1990s to 2000s through legal elections (Masters and Laub). Hezbollah and its media outlet, Al-Manar, use social media to spread messages of terrorism. Al-Manar specifically promotes violence against Americans and other troops in the Middle East, the implementation of Sharia Law, and suicide attacks (Grabinsky and Jorisch).

Facebook and Twitter treat Hezbollah content and pages in much the same way as they do for Hamas. Facebook did remove some pages related to Hezbollah's Al-Manar, Al-Ahed, and the Islamic Resistance in Lebanon, but the groups quickly reemerged. Facebook also eliminated one of Al-Manar's pages in 2018, but searches by *Bloomberg Businessweek* found replacements within two weeks (Silver and Frier). Twitter suspended Hezbollah's main pages around the same time in 2018, but officials from the organization directed followers to other pages. Twitter's actions against Hezbollah likely resulted from the same threats by Israeli officials that caused the removal of several of Hamas' accounts (Carbone). The problem with Hezbollah's existence on Twitter and Facebook mirrors that of Hamas. The social media sites appear only to remove the content of this organization under legal pressure. Facebook may avoid removing content and accounts pertaining to Hezbollah and Hamas either because specific pages contain non-violent content (and Facebook's policies may permit only the removal of violent terrorist content) or because the company does not consider Hezbollah and Hamas as terrorist organizations. If Facebook's and Twitter's classifications of terrorism and violent content do not, in fact, cover Hamas or Hezbollah, then these organizations may continue to recruit followers on social media and to threaten international security through their violent tactics. If the social media companies provided American counterterrorism agencies with information on these groups, however, the agencies could help to prevent terrorist recruitment and attacks facilitated through social media activity.

### III.VIII Social Media's Obligations

Whether Facebook and Twitter provide United States counterterrorism agencies with terrorists' content from their sites relies on the companies' obligations to do so. Mark Zuckerberg, the CEO and creator of Facebook, has stated that he now holds the site responsible for posted content. Zuckerberg did not specify, however, in what way Facebook takes responsibility for content. Several critics of Zuckerberg and his company contest this statement, because of its vague nature and because the CEO does not imply an obligation to prevent terrorist activities on the social media site. Vernon Silver and Sarah Frier of *Bloomberg Businessweek* argued that Zuckerberg's statement does not signify a moral or legal obligation but a public service (Silver and Frier). The Digital Citizens Alliance expressed skepticism towards Zuckerberg's sense of responsibility and moral duty, arguing that the monetization of Facebook users' content, regardless of the source, appears more important to the company ("Fool Me"). Jack Dorsey, the CEO of Twitter, did not make a statement like Zuckerberg's, but given that a research report written by the *Scientific American* in June 2018 indicated that Twitter allowed more freedom for terrorists, whether Dorsey feels a responsibility towards the content on his site appears questionable (Macdonald). The Digital Citizens Alliance contended that, in order to fully motivate Twitter and Facebook's capacities to remove the presence of terrorism, the U.S. government may need to make the companies legally accountable ("Fool Me").

The government can dictate legal requirements, especially those pertaining to terrorism. On January 24, 1995, former President Bill Clinton created Executive Order 12937, which prohibited both foreign entities (including companies) from financially, materially, and technologically aiding state-sponsored and non-state-sponsored terrorist organizations (as listed by the DOS) and allowed the FBI to investigate these cases and to counteract them (U.S., Executive Office of the President, White House Office of the Press Secretary). Thus, the current president could argue that Facebook and Twitter technologically assist terrorist organizations by allowing them to gain recruits and spread messages of terrorism. If an FBI investigation proves these allegations true (and research seems to indicate this truth, at least in the cases of Hamas and Hezbollah), the FBI could require Twitter and Facebook to save all terrorism content from their pages and to share it with American counterterrorism agencies. In order to forego another FBI investigation into a subject that has already been studied by private researchers and government officials (See Section III.II), the American government could create a new law that would specifically obligate social media companies to save and share all information posted by suspected terrorists with government counterterrorism agencies.

# Chapter IV: Solutions and Effects

## IV.I Intervention

If Facebook and Twitter cannot obligate themselves to effectively overcome the pervasive presence of terrorist groups on social media, then the American government must intervene. As Twitter's reaction to Israel's threat of legal action demonstrates, legal compulsion appears as likely the most effective method to disrupt terrorism on social media, even though social media companies could push back through campaigns against such laws. This intervention should not occur in a way which would eliminate the companies' abilities to generate income and to achieve the purposes of their existence, of course, but which would benefit the companies and the government and would thwart terrorists' activities on social media sites. A government policy that requires Facebook and Twitter to disseminate to counterterrorism agencies all information that their security systems collect on terrorist activity presents one solution. In this chapter, I outline my policy proposal, which contains several parts. I number and title each stipulation in terms of the general idea that relates to the function of each proposed requirement. Below the title of each policy specification, I describe its function. The specifications of the policy relate to setting parameters to define terrorism, to disseminate and store information, and to apprehend and convict suspects of terrorism. I then discuss the policy's benefits for American counterterrorism agencies, Facebook, and Twitter. I also discuss practical and ethical downsides of the policy. I conclude the chapter by attempting to refute the downfalls of the policy and discussing why, despite the risks of the policy, it presents an important counterterrorism tactic.

## IV.II A Policy Proposal

1. *Policy operation under one definition of terrorism*

Because each counterterrorism agency and social media site operates under a different delineation of "terrorism," a policy that involves this concept requires a single definition under which it may operate. As my classification of terrorism from Chapter 1 combines the definitions from the U.S. Legal Code, the Department of State, the Federal Bureau of Investigation, and Facebook, it serves as the guideline for this policy proposal. I define terrorism as any veritable threat or act of violence against civilian and governmental populations and property in order to promote extremist ideologies through the fear of future attacks. "Extremist ideologies" or "extremism," in this case, involves an ideological and deep-seated hatred towards any ethnic, religious, economic, political, or social groups that the individuals or groups holding such beliefs want severely changed or eliminated, with a willingness to resort to violence to achieve these objectives. The use of this classification of terrorism would require Facebook and Twitter to label both American and foreign entities as terrorists, including non-governmental organizations (such as ISIS ad Al Qaeda) and official political parties (such as Hamas and Hezbollah). While the inclusion of political parties (especially those legally elected to governments) under the concept of terrorism represents a change for Facebook and Twitter, who have allowed such groups to moderately thrive on their sites, the U.S. government already classifies some of these entities as terrorist organizations and works to combat them. As this definition of terrorism does not profile individuals or groups as terrorists based upon their religious or ethnic identities, Facebook, Twitter, and government agencies should not use profiling for this policy, either.

2. *Distribution of content from Facebook and Twitter to the National Counterterrorism Center, other American counterterrorism agencies, and foreign governments*

As demonstrated in Chapter 3, the information contained on Facebook and Twitter that pertains to terrorist organizations could greatly assist U.S. counterterrorism agencies in their missions to prevent acts of terrorism and to track terrorists. As the National Counterterrorism Center (NCTC) functions as the nexus for all American counterterrorism agencies and information, the Center creates an ideal primary distribution point. Because these social media companies often delete such data and do not share it with any government unless pressured, this policy obligates Twitter and Facebook to distribute to the NCTC information from their sites, as identified by the companies' security teams and detection technologies, that pertains to terrorism. This content includes users' social media activity, account details, and personal information. The social media companies can also choose to share relevant content with foreign governments and to enter into policies with foreign governments similar to this one. To ensure that the security of the program and that the social media companies accurately and actively target terrorists and terrorist organizations, American counterterrorism agencies should vet and contract individuals on the companies' security teams to target and disseminate information on suspects. The government should certify these contracts through separate legislation or agreements with Twitter and Facebook. Upon receiving information from Facebook and Twitter, the NCTC must distribute this data to all other relevant U.S. counterterrorism agencies for analysis. The social media companies can also choose to share relevant content with foreign governments and to enter into policies with foreign governments similar to this one.

3. *Use of terrorism content by American counterterrorism agencies*

Should American counterterrorism agencies, after analyzing the data provided by Facebook and Twitter, discover veritable and documented proof of terrorist activity in the form of recruitment, incitement to violence, verifiable threats, or planned attacks against the United States government, its citizens, or inhabitants or the recruitment of United States citizens or inhabitants for terrorist organizations or activities that pose a security threat for any country, the agencies may use the information provided by these companies as legal grounds for further investigation and prosecution of domestic and foreign individuals and groups for charges of terrorism. If individuals found guilty of terrorism charges live outside of the Unites States, the government may request a warrant from the governments of the countries in which the suspects reside for their extradition or extraordinary rendition to and arrest in the United States. Once the government jails said terrorists, they will have no access to social media until the time at which the legal system either acquits the suspects of all charges or until they complete their sentences. In the case that the data provided on suspected terrorists demonstrates a threat solely to a foreign government, U.S. counterterrorism agencies may choose to deport them to the appropriate countries if the individuals live in the U.S., may request the provisional arrest of these suspects in the countries which hold warrants for their arrests, or may share said data with any and all relevant foreign governments. Should the information provided by these social media companies on suspected terrorists, after further analysis, not find any veritable and documented evidence of terrorist activity, the investigating agencies should destroy all of its copies of this information. In order to protect the identities of suspects, their cases and information should remain private at all times.

### 4. *Further stipulations for Facebook's and Twitter's future use of terrorism content*

After disseminating pertinent information to the NCTC, the social media companies should remove all terrorist content and accounts from their platforms that demonstrate or incite violence, per their current rules. The social media companies may not sell or in any way disseminate this content to entities other than American counterterrorism agencies or foreign governments that could benefit from such content. Facebook and Twitter should eliminate accounts on a case-by-case basis, depending on the amount of activity on such platforms, as demonstrated by the number of views, followers, and posts. American cybersecurity experts will set the limit for terrorist accounts' activity before the social media sites must eliminate such pages and information. In order to ensure the efficacy and security of this policy, all involved entities (both governmental and private) should strive to keep its existence private (not secret). Facebook and Twitter must continue to store all information on separate platforms. In case future activity by users previously found to be innocent of terrorism actions and connections demonstrate a potential threat of terrorism, the social media companies must resend the old data to American counterterrorism agencies along with the new evidence.

5. *Penalties for Facebook's and Twitter's non-compliance with the policy*

Should U.S. counterterrorism agencies find proof of non-compliance to the policy by Facebook and Twitter, the agencies should investigate and contend with the companies as appropriate for the situation. Examples of non-compliance may include a failure to collect information on terrorism as stipulated by the policy's definition, a failure to disseminate all relevant information on terrorism to American counterterrorism agencies, or the dissemination of knowingly falsified information to American counterterrorism agencies. If American counterterrorism agencies find documented examples of non-compliance, they may lead a further investigation into those allegations. In the case that subsequent investigations into allegations of Facebook's and Twitter's non-compliance with the policy prove correct, the investigating agencies may declare these agencies as accomplices to terrorist groups and "unusual and extraordinary threats" to the security of the United States, per Section 1701 of the International Emergency Economic Powers Act (IEEPA) and Executive Order 12947 (91 Stat. 1626, 94 Stat. 2025, and U.S, Executive Office of the President, White House Office of the Press Secretary). These agencies may then take any action necessary to mitigate the threat caused by these social media companies, provided that such action does not prevent the non-terrorist users' ability to utilize the communication services provided by such companies, as such disruption would interfere with American civilians' freedom of speech. If necessary, the American government may enact new legislation to expedite this process of investigation and to outline appropriate penalties.

### IV.III Benefits for American Counterterrorism Agencies

Easy access to a wealth of information on suspected and known terrorists presents one of the main advantages of this policy for American counterterrorism agencies. Distribution of data from Facebook and Twitter to one distribution point (the NCTC) would ensure that all pertinent counterterrorism agencies would receive the same content, instead of the social media companies sending different information to individual agencies. The agencies would then possess access to a centralized point of information (the social media sites), which would provide them data from potential locations to possible future attacks on known and suspected terrorists and terrorist organizations. Certifying the locations of individual terrorists and terrorist organizations could furthermore reduce the amount of military strikes on civilian populations, which would in turn decrease the human and financial costs of such strategies. Counterterrorism agencies would not need to hire additional staff themselves to gather this information, as social media security teams already perform the collection activities, though they can contract individuals on the social media security teams. And by allowing small terrorist accounts to continue to exist on Twitter and Facebook, this factor reduces the risk of terrorists catching on to the U.S. government's involvement, which could lead terrorists to provide false information or to instead utilize more secure platforms, such as the Dark Web (Berger). Thus, the policy could promote social media as a sustainable source of information on terrorist activity. While information collection from social media should certainly not replace all other sources of data, this method provides a useful tool through which American counterterrorism agencies can obtain a diverse spread of information.

U.S. counterterrorism agencies may furthermore bring charges against and prosecute suspected terrorists and terrorist organizations based solely on their social media activity. If suspects' actions on social media prove that they make valid threats against the American government, its citizens, or its inhabitants (in other words, the suspects would act on such threats), the accused individuals and groups may be arrested and charged for incitement to terrorism-related violence based on this information alone. Proof that the suspected individuals assist in the planning of terrorist attacks against America as in the above scenario also provide grounds for the same actions taken against said accused individuals and groups. Finally, the U.S. government can arrest suspected terrorist individuals and groups (if the U.S. holds a warrant for their arrest) or request the provisional arrest of suspects (if foreign governments, not the U.S. possess a warrant for their arrest) based on their recruitment of American citizens or inhabitants of the United States for terrorist groups or activities, if the groups and activities threaten the security of America or of a foreign state. Basing charges on information from social media also allows counterterrorism agencies to expend less time, effort, and money on tracking every activity of terrorists and terrorist groups across a variety of platforms in order to prosecute these suspects. If the U.S. government can slow the recruitment stream on social media and can prosecute enough terrorists, especially those who play an important role in terrorist organizations, the government could destabilize terrorist groups and reduce the threats that they pose to America and to the world.

### IV.IV Benefits for Facebook and Twitter

While the benefits of this policy undoubtedly appear more in favor of American counterterrorism agencies than of Facebook and Twitter, these companies can still profit from the policy. The government can contract individuals or groups in the social media companies to perform the security checks, which would allow the companies to generate some profit. The permitted existence of smaller terrorist pages under this policy also provides the social media sites with a continuous cash influx (as the companies accrue funds through the sale of their users' information), despite the fact that the sites may lose some revenue from the removal of large terrorist accounts and their contents from the social media platforms (as the companies accrue funds through the sale of their users' information). The decreased presence of terrorism on these platforms may also encourage users' trust in and praise for the companies, which currently face heavy criticism from social media skeptics, current users, and researchers. While the policy should remain private, Twitter and Facebook can certainly publicize their increased removal of terrorist accounts and content in order to garner support. This increased effort to combat terrorism may encourage more investors, who previously avoided social media due to the pervasive presence of terrorism, to invest in the social media platforms. If Facebook and Twitter fully comply with the policy, they can certainly benefit monetarily from the decrease in legal measures threatened and undertaken by the U.S. government due to the existence of terrorism on the sites.

The section of the policy which allows the U.S. government to prosecute suspected terrorists and terrorist organizations based on their social media activity can also assist Facebook and Twitter, though in a more indirect manner. Terrorists continue to create pages and post information even after social media security teams remove their other accounts and content, which creates a sort of endless disease on the sites. However, if American counterterrorism agencies caught and arrested terrorists, especially those with an active presence on social media, Facebook and Twitter would have less content and fewer pages to track, creating less strain on security teams. The ban on social media usage for arrested suspects would also help to slow terrorist activity, as jailed terrorists would possess virtually no outlet for which to use social media. While capturing terrorists remains difficult, and new terrorist cells and individual users can pop up on social media platforms, U.S. and foreign counterterrorism agencies possess a variety of tactics in their arsenal that can mitigate this issue (including community building and terrorist rehabilitation, which could draw individuals away from terrorism support).

Virtual “bots” used by terrorists to formulate accounts and content on social media platforms do pose a separate concern (Berger). However, terrorists must oversee and maintain these bots but if Facebook and Twitter’s security systems can continue to discover and eliminate bot-generated content and the sources of these bots, and counterterrorism agencies can arrest the creators and maintainers of the bots with the companies’ assistance, this collaboration can reduce the strain that bots cause on social media security systems. Of course, the elimination of the presence and threat of terrorist individuals and organizations on Facebook and Twitter will remain impossible to achieve completely, even with this policy. Despite this impossibility, the combined efforts of Facebook, Twitter, and American counterterrorism agencies can compound on the success of the social media companies’ current efforts.

## IV.V Practical and Ethical Concerns

Though this policy provides many positive outcomes for both Facebook and Twitter and U.S. counterterrorism agencies, the policy faces potential setbacks in terms of the implementation of all of its parts and the ethical issues surrounding privacy breaches. One of the practical concerns of the policy pertains to Facebook and Twitter's compliance. The policy makes many demands of these companies, from the requirement to share information that pertains to terrorist activity to the requirement to remove all terrorist accounts and content with more than a few hundred followers, likes, and shares, with little direct benefit for either social media site. While Facebook and Twitter would profit from the dissemination of information to the NCTC, they currently profit from the sale of their users' data (regardless of the users' criminal statuses) to private companies ("Fool Me"). Thus, the social media companies could lose money by not selling to a variety of private companies. Other than the legal obligation to comply to all facets of the policy, the companies currently seem to possess no incentive to comply. As Facebook's and Twitter's track records demonstrate, their main objectives center around the accrual of profits through the connection of users from around the world and the sale of those users' information ("Fool Me").

The negative consequences of non-compliance by Facebook and Twitter for U.S. counterterrorism agencies range from inconvenient to potentially disastrous, depending on the type of non-compliance. The failure of these social media companies to share important terrorism-related information from their sites to pertinent agencies presents one problem. While receiving some information from Twitter and Facebook benefits government counterterrorism actions more than no information, which closely represents the current relationship between the social media sites and counterterrorism agencies, the missing information could prove crucial to the location and arraignment of wanted terrorists and to the prevention of terrorist attacks. The consequences of this missing information on potential terrorists and terrorist attacks could result in human casualties and infrastructure damage as a result of acts of terrorism. In theory Facebook and Twitter would share the most crucial data with the relevant governmental agencies if legally obligated. However, this assumption remains untested, since this policy remains as a mere proposal, and thus could prove incorrect. The companies could also share over-share data with very little connection to terrorism (a form of malicious compliance), which would increase the amount of information that counterterrorism agencies would need to analyze (which would necessitate an increase in funding, labor, and time) and would compromise the privacy of innocent individuals.

The dissemination of knowingly-falsified information (data that the sites either falsified themselves or that external sources falsified with the prior knowledge or consent of Facebook and Twitter) to counterterrorism agencies presents another form of possible non-compliance by Facebook and Twitter. Depending on the nature of the falsification, such as a change in the suspect's name, and the government's reaction to the information prior to the discovery of the falsification, such as questioning the wrong suspect for further information, the results could present simply a waste of the government's and the suspect's time. However, if the falsification presented itself as a change in the location of a planned terrorist attack or the government reacted hostilely towards a suspect, this disinformation could result severe consequences, such as the deaths or injuries of innocent civilians. This second scenario presents an extreme and highly unlikely possibility, as Facebook and Twitter possess no discernable reason to risk so many innocent lives. As the companies have no clear need to falsify information, as well, this scenario seems unlikely to occur. However, as in the first example of potential non-compliance, this supposition of the social media companies' potential motives and actions remains unverified.

The publicization by Facebook or Twitter of the policy's existence or the contents of the policy represents the third and final form of non-compliance. As the policy and its stipulations suggest privacy, a leak of any nature could threaten the policy’s efficacy and sustainability. If Facebook and Twitter (or government agents) reveal this policy to the public, terrorists targeted by the policy will undoubtedly learn of its existence as well. If terrorists realize that the government uses their information on social media to locate and arrest them, terrorist individuals and groups may begin to spread false information (false flags) on their accounts or to switch to a different platform (such as the dark web) in order to spread their messages. These consequences would severely reduce (if not eliminate) the usefulness of terrorism content on social media to counterterrorism agencies (Berger). U.S. counterterrorism agencies would then lack a valuable source of data on terrorist activity and would have to concentrate their efforts on other online platforms.

Public knowledge of this counterterrorism policy, whether obtained from a leak by social media companies, government employees, or other sources, would also undoubtedly lead to backlash from civilians and foreign governments world-wide regarding the ethics of such a policy. Even though this policy intends that American counterterrorism agencies only analyze suspected terrorists’ social media accounts, would not actively search for said accounts themselves (allowing Twitter’s and Facebook’s security teams to collect relevant data), and must remove from their systems all information that does not clearly prove a connection to terrorist organizations and activities, the public may consider this practice as a breach of privacy. Public outrage from previous privacy breaches by the U.S. government and social media companies demonstrates the likelihood that this policy would spark controversy. When Edward Snowden leaked information that proved the public’s suspicions that the NSA tapped and analyzed civilians’ electronic communications, the American government overall faced heavy criticism and the decreased trust of the American community (Geiger).

Facebook and Twitter’s dissemination of data to the American government represents another ethical concern of the policy that would likely cause backlash if knowledge of the policy became public. When the international community discovered in 2018 that Facebook sold its users’ data to advertising companies and other businesses, the public and the media criticized the company for violating the privacy of its users, and the U.S. government sued the company, although Facebook’s user policy allowed the site to sell such data (Hern and Pegg). Despite the fact that, in the case of this policy, the selling of data would facilitate the U.S. government’s ability to carry out counterterrorism actions, the public could criticize the government’s hypocrisy of condemning the selling of social media data while simultaneously buying and using it. Given the historical public criticism surrounding counterterrorism policy and privacy scandals in the public and private sectors, a policy that required Facebook and Twitter to share suspected terrorists’ information with American counterterrorism agencies would certainly cause criticism, even if the policy demonstrated large successes. The result of such backlash could cause current users of Facebook and Twitter to leave the platform, reducing revenue for the companies. The government to revoke this policy as a result of public criticism, which would remove an important source of knowledge on current terrorists and their activities.

Another ethical concern of this policy relates not necessarily to non-compliance by Twitter and Facebook but to racial and religious profiling. The social media companies and counterterrorism agencies could set the parameters of their security and information collection and analysis tools to specifically target certain ethnic or religious groups (such as Arabs or Muslims). Profiling under this policy would mean that social media users of some identities would more likely face accusations and investigations of terrorist activity than users of other backgrounds. The users of target backgrounds could also face a denial of service by social media companies. The Office of the United Nations High Commissioner for Human Rights found in 2018 that Facebook's current definition of terrorism, which broadly associates non-state armed groups and violence with terrorism, could cause governments to further stigmatize and repress dissent and opposition and the rights of specific ethnic groups, whether or not these groups use violence. This non-specific definition could also result in Facebook over-regulating certain accounts or denying its services to individuals with no verifiable connection to terrorism (OHCHR). Besides the injustice of targeting individuals and groups based on their ethnicities or religions, counterterrorism agencies could miss out on important information and leads on suspected terrorists and terrorist organizations who do not fit into these target parameters. Since terrorists come from a wide variety of ethnic, cultural, and religious backgrounds world-wide, this profiling could pose a major problem for the government's counterterrorism actions.

### IV.VI A Necessary Step Forward

Although this policy proposal undoubtedly presents several practical and ethical concerns, the policy contains certain caveats in order to ameliorate these issues. In terms of Facebook's and Twitter's potential non-compliance with the policy, the proposal includes a section that stipulates the actions that the United States government may undertake in regard to these actions, if the government can find evidence of non-compliance. The government may first investigate such allegations against the social media companies. If the accusations against the companies prove true, the government may declare that Twitter and Facebook present threats to the security of the United States by aiding terrorists. The legal system can then "punish" the companies in any method that the government sees fit, as long as the discipline does not impact the freedom of speech of the users of the social media sites. This punishment could take the form of heavy fines against executives or central shareholders (although this tactic has not always proven effective against companies in the past). In this way the social media companies can continue to function without disruption for their users. This stipulation that allows the American government to penalize Facebook and Twitter for a breach of the policy would theoretically prevent the companies from doing so. Even if the companies do not provide U.S. counterterrorism agencies with all of the identified information from their sites that pertained to terrorism, access to even some of that content (assuming the content proves true) would benefit counterterrorism agencies more than no information (Steinbach). In terms of malicious compliance by Facebook and Twitter, the policy attempts to mitigate this threat by setting boundaries for the characteristics of terrorism and the types of content that the companies should share and by not specifying that the companies need to share all content discovered. These factors cannot completely eliminate the possibility of malicious compliance but can assist in ameliorating it.

As long as Facebook, Twitter, and American counterterrorism agencies with knowledge of this policy attempt to maintain its privacy, the policy can likely avoid discovery by individual terrorists and terrorist organizations. Twitter and Facebook already publicize the fact that they target and remove terrorists' accounts and content from the sites, and since the policy does not require the removal of all accounts and information pertaining to terrorism (so long as the amount of activity remains low), the government and the social media companies can mitigate terrorists' suspicion. Though the policy does allow the U.S. government to arrest suspected terrorists based upon the information that they post on social media, and the prosecutors may need to demonstrate that they obtained the content lawfully and without a violation of due process, the government does not need to reveal the full extent of the policy. The government currently uses content from social media to arrest individuals on suspicion of terrorism, though tip-offs from other users and publicly available content generally provide the source of information, but sometimes leave the name of the informant anonymous (U.S, Dept. of Justice, U.S. Attorney's Office: Eastern District of Virginia). This step can further protect the policy's existence from the knowledge of terrorists who use social media, which in turn can promote the policy's efficacy and sustainability. If small-time accounts can continue to utilize the platforms without the knowledge American of government interference, they can continue to post veritable content on the social media sites, thus providing U.S. counterterrorism agencies with a reliable source of information on current terrorism trends (Berger).

Even if the policy can remain private from the eyes of the international public and the media, however, the ethical and legal concern surrounding the American government's interference with personal information still exists. While the information analyzed by counterterrorism agencies ideally relates to terrorists, who can pose a global threat to civilians and governments, the government's right to analyze private information posted online remains questionable due to a potential violation of individuals' privacy and the freedom of speech. In order to diminish this criticism, a section of the policy proposal stipulates that if the government agencies who analyze the data sent by Facebook and Twitter find no verifiable connection to terrorism, the agencies must delete all copies of this information from their files. The government therefore cannot discriminate against or harass users based on their social media activity if the users possess no connection to terrorism. The stipulation that the identities and data collected on suspects must remain privates further assists to protect the identities and reputations of individuals found guilty or innocent. In order to protect the identities and reputations of individuals who might otherwise be targets of ethnic or religious profiling, the policy also recommends that Facebook, Twitter, and American counterterrorism agencies not utilize profiling for any part of the policy.

The fact that Twitter and Facebook, not the United States government, identify and collect only content that appears to pertain to terrorism per a set definition further mitigates the policy's ethical dilemmas. The government should not have access to the information of individuals who do not fit under the delineation of terrorism used by the policy. Critics could still target American counterterrorism agencies (or the government in general) and the social media companies for the sharing and use of private information to arrest individuals. However, the policy will likely demonstrate success in the arrest of terrorists and the prevention of terrorist attacks, and thus the benefits of this policy far outweigh the ethical and practical concerns.

# Chapter V: Conclusion

## V.I Future Policy Expansions

While the policy proposal in Chapter IV centers on the use of terrorist content from Facebook and Twitter (as disseminated by these companies) for counterterrorism actions, the U.S. government could expand the subject matter, online platforms, and level of involvement covered by the policy. Terrorism on social media does present an easily-identifiable threat to the American government and civilians, but several other entities threaten the United States as well. Both state-based and non-state-based actors target the U.S. on social media. And the threats posed by these actors present themselves on platforms beyond Facebook and Twitter, including YouTube, Google+, and Instagram. Several sites have uncovered some of the content by subversive entities but do not always share this knowledge with the government. This lack of information distribution may signify that the American government needs to play a more direct role in the collection of relevant data from social media and general online sites. In this chapter I elaborate on the possible expansions of the policy proposal from Chapter IV, including subject matter, online platforms, and government involvement level. I discuss the potential downfalls for each form of expansion, highlighting the reasons for which I did not include the factors as a part of my policy.

## V.II Subject Matter Expansion

Many countries and coalitions besides terrorists and terrorist organizations threaten the security of the United States. Since the Cold War, Russia has used various forms of media to spread disinformation about America. With the rise of social media, the Russian government became proficient at spreading deliberately falsified information at a rapid rate. This tactic of disinformation has, in combination with the use of fake accounts on social media, caused social and political destabilization in the United States that led to public riots and influenced the 2016 American Presidential Elections (Ellick). The American government possessed little knowledge of this involvement until 2016 but did not know much about the extent until the 2017 and 2018 investigations into allegations of Russian election interference and Facebook's privacy problems. Though Russia used Facebook to influence elections and spread disinformation, only government investigations uncovered this information, of which Facebook admitted knowledge only under legal pressure. Later in 2018 Facebook security teams did share information with the American and British government of Iran's involvement in 2016 election tampering on social media, but the company's openness in this case appears as a means to salvage its reputation after the aforementioned privacy scandal (Breland). If the government cannot trust social media companies to share this information or to stop the spread of disinformation by subversive countries unless under duress, the government may need to undertake legal action in order to obtain such content. With this data, the American government can analyze and expose the subversive actions of countries like Russia and Iran and hopefully work to prevent future threats by the states.

Besides countries whose actions on social media threaten the security and stability of the United States, groups such as human and sex traffickers and drug gangs use social media to carry out their functions. The FBI has identified and charged several individuals of sex trafficking and human trafficking on social media, especially involving the trafficking of children. In 2014 the Bureau investigated and arraigned a Texan man on allegations of using social media to lure in young girls for sex trafficking and sexual exploitation (U.S., Dept. of Justice, FBI, "Sex Trafficker"). Drug trafficking, which also affects the health and safety of American youth, represents another pervasive problem that the U.S. government attempts to handle. The Department of Justice sentenced 15 defendants in August 2018 for drug trafficking heroine from Ciudad Juarez to Las Cruces, New Mexico. Social media facilitated this drug trafficking pipeline for several years (U.S., Dept. of Justice, U.S. Attorney's Office: District of New Mexico, "Multi-Agency Investigation"). These articles and investigation reports do not state whether civilian tip-offs or social media companies alerted the government to these instances of trafficking, nor did the government announce whether the social media companies knew of these activities. Given the threat that trafficking in its many forms poses to communities world-wide, if social media security teams either do not notice or do not report of their own volition these crimes to pertinent governments, countries around the world besides America may have to resort to legal force. After the U.S. government brought so many of these trafficking crimes that involve social media to court, the social media companies cannot deny knowledge of the crimes' existence on their platforms. And if the companies know of these crimes on their platforms and still do nothing to correct the situation, are they not guilty of aiding and abetting these criminals? Though this thesis and proposal focus on terrorism, due to the existence of other threatening activities on social media, government agencies could expand my policy proposal to include subversive activities and trafficking crimes among the content that Facebook and Twitter must turn over to the agencies.

### V.III Online Platform Expansion

Facebook and Twitter do not represent the only online sites, let alone social media sites, which traffickers, terrorists, and other entities use to carry out their destructive activities. While these two social media companies arguably contain the most diverse types of information in one location and already take some action against terrorists and other subversive groups, these entities also utilize sites such as YouTube, Instagram, and Google+. To combat criminal activity on the sites, Facebook (including its site Instagram), Twitter, Google (including its sites YouTube and Google+), and Microsoft created the Global Internet Forum to Counter Terrorism (GIFCT) in 2017. The GIFCT uses computer algorithms to target terrorist content on the sites and to alert other sites to the same content so that all involved online platforms can delete the threatening information (Macdonald). These computer algorithms, though, do not catch all terrorist content, as terrorists now use code-words in their posts in order to avoid detection, nor do the algorithms target other forms of criminal activity (like trafficking). Even when the algorithms do reveal strong signs of terrorism activities and beliefs, social media companies do not always address these issues. Members of the GIFCT also did not announce whether they share terrorism-related content with any governments in order to track the terrorists (Lapowsky). Thus, the U.S. government again loses valuable data, from photographs to videos to personal information, that it could use to capture and arrest or extradite terrorists. I did not include platforms beyond Facebook and Twitter in my thesis and proposal because those two present the greatest diversity of data in one location, but the government could nonetheless expand my policy to include other sites in order to obtain further content on terrorists.

### V.IV Direct Government Involvement

Regardless of whether the American government expands my current policy proposal, social media sites covered by the policy may not disseminate any or all required content, despite the consequences of non-compliance, or may engage in malicious compliance. In this instance the government may chose to grow the policy in another direction in order to legally protect its direct involvement in the collection of terrorist information and to assure that the government receives all (and only) relevant data. As revealed by Edward Snowden, the National Security Agency already uses advanced technological programs to analyze and gather content on suspected terrorists from Facebook. The NSA does share this information with the FBI and certain allied foreign counterterrorism agencies when necessary, but content from the Snowden leaks did not reveal the extent of information disseminated or if the NSA shared information with other American counterterrorism agencies (Greenwald 137-64). Following the Snowden leaks, the NSA also faced criticism from civilians and governments world-wide on the legality of its operations (Geiger). With a policy that would legally permit the National Counterterrorism Center to collect information on terrorists' social media activities and to then share this data with all other U.S. counterterrorism agencies, the government could ensure that all pertinent agencies received the information necessary to carry out counterterrorism activities and that the NCTC collected this data by legal means. This type of direct involvement, though, would likely necessitate a greater increase in funding, labor, and time for American counterterrorism agencies than my policy would.

Even if my policy legally protected the NCTC's right to gather and share content from social media, these actions would likely still fuel the same debate on security versus privacy that the NSA's actions did, should someone reveal this policy to the public. Both my current policy and the NSA's strategies contain the caveat that, if agencies find the content that they collected to be innocent of criminal activity, the agencies cannot save this information (Greenwald 137-64). Despite this rule governments and civilians still criticized the NSA for its breach of privacy (as critics possessed no way to assure that their information was not saved by the NSA), and thus my policy would likely face the same backlash if publicly disclosed (Geiger). Social media sites could also file lawsuits against the government for interfering with their abilities to function, make money, and protect the privacy of users. In case Facebook and Twitter do not comply with the policy and disseminate terrorist content, the government must decide whether the benefits from the direct collection of data from social media outweigh the potential risks. While I found the risks of direct U.S. government involvement too great to include in the policy proposal, and thus attempted to find other means by which counterterrorism agencies could obtain the same data, agencies that potentially use this policy may disagree.

### V.V Current Implications

Though my policy proposal in Chapter IV offers several options for its expansion, if Facebook, Twitter, and American counterterrorism agencies follow the stipulations of the policy as intended, the policy should increase these actors' capacities to combat terrorism both online and in the real world. If the social media companies and government agencies all operate under one definition of terrorism, as the policy dictates, they can assure a cohesion of information and understanding of terrorism. The use of the NCTC as the main distribution center further helps to streamline the process of content dissemination, as Twitter and Facebook only need to share information with one government point, not several, and the NCTC can then send this data to all relevant counterterrorism agency (as it already serves as a hub for U.S. counterterrorism information and activity). Counterterrorism agencies can then use this information to investigate, track, and arrest suspected terrorists, and can charge individuals for terrorism-related crimes based on their social media content.

Certain setbacks do exist within the policy, though I do attempt to ameliorate them as much as possible. Agents from American counterterrorism agencies, employees Facebook and

Twitter, or spies for other governments could reveal the policy and its contents to the public or to terrorists, making the policy less effective and causing criticism world-wide. Facebook and Twitter could also decide not to disseminate any or all terrorist content with the NCTC, which would cause counterterrorism agencies to lose potentially crucial information. I try to diminish the severity of these potential issues by not allowing the counterterrorism agencies themselves to breach privacy and personally examine social media, by requiring counterterrorism agencies to delete the social media information of individuals found innocent of terrorism after analysis, and by including consequences for policy non-compliance by Facebook and Twitter. Only an official test of this policy could, unfortunately, reveal the efficacy of these attempts to reduce the policy's problems.

Despite the potential drawbacks of my policy, though, the information that the American government could obtain from suspected terrorists' social media accounts. From Facebook and Twitter data, counterterrorism agencies could obtain information on suspected terrorists' personal information, such as their identities, locations, friends, family, interests from the content that the terrorists post (@dew_mari and Dewicki). Counterterrorism agencies could use this content to track terrorists, build cases against them, arrest them, and punish them under U.S. law or deport them to other countries who brought charges against the individuals (U.S., Dept. of Justice, U.S. Attorney's Office: District of New Mexico, "Two New Mexico Men"). The Department of Justice (and its subsidiary, the FBI) already use data from social media to arrest and charge terrorists, but this information comes primarily from civilian tip-offs, and thus the government lacks a wealth of information that it could use to find and charge other suspects (Steinbach). This content could permit American counterterrorism agencies to investigate and arrest individuals and break up the functions of major terrorist organizations, such as Al Qaeda, ISIS, Hamas, and Hezbollah, which maintain a constant presence on social media (Silver and Frier).

The United States government already utilizes several different tactics in a variety of agencies in order to combat terrorism. Drone strikes, espionage, community-building, and humanitarian aid represent only a few of the strategies used by agencies such as the DOS, FBI, DoD, CIA, and NSA (Wiley). Facebook and Twitter also employ their own counterterrorism techniques, including the identification of terrorism-related accounts and content by sophisticated computer technology and the removal of these accounts and content from the social media platforms (Macdonald). Counterterrorism researchers from private institutions such as the Stimson Center and Digital Citizens Alliance, however, criticize the efficacy of governmental and social media counterterrorism methods and argue that the agencies should find cheaper, less destructive, and more precise means of combatting terrorism (Belasco et al. and "Fool Me"). Despite the impossibility of completely and permanently defeating terrorism, my policy attempts to diminish the setbacks faced by U.S. counterterrorism agencies, Facebook, and Twitter so that they possess the information necessary to improve their current techniques and to destabilize terrorist organizations both online and offline. When combatting terrorism and protecting human lives, the joint efforts of the private and public sectors together present a more potent threat to terrorism than several disjointed actions from a variety of independent groups.

## References

"18 U.S. Code § 2331 - Definitions." *LII/ Legal Information Institute*, Cornell University, www.law.cornell.edu/uscode/text/18/2331.

"50 U.S. Code § 1701 - Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities." *LII/ Legal Information Institute*, Cornell University, https://www.law.cornell.edu/uscode/text/50/1701.

"50 U.S. Code § 1702 – Presidential authorities." *LII/ Legal Information Institute*, Cornell University,

https://www.law.cornell.edu/uscode/text/50/1702.

@dew_mari. "Mari Dew." *Twitter*, Sept. 2018,

https://twitter.com/dew_mari.

"Action Counters Terrorism: Report suspicious activity and behaviour to tackle terrorism." *Nottinghamshire Police*, Nottinghamshire Police and Crime Commissioner, www.nottinghamshire.police.uk/advice/action-counters-terrorism-act.

Allen, John R. "I Was Special Envoy to Fight the Islamic State. Our Gains Are Now at Risk." *The Washington Post*, WP Company, 3 Jan. 2019, www.washingtonpost.com/opinions/i-was-special-envoy-to-fight-the-islamic-state-trump-could-unravel-our-gains/2019/01/03/2339f1a4-0ebe-11e9-84fc-d58c33d6c8c7_story.html?utm_term=.4473140ddf2b.

Belasco, Amy, et al. "US Counterterrorism Spending Since 9/11." The Stimson Center, 16 May 2018, Washington DC,

https://www.stimson.org/content/us-counterterrorism-spending-911.

Berger, J. M. “The Evolution of Terrorist Propaganda: The Paris Attack and Social Media.” *Brookings*, The Brookings Institution, 27 Jan. 2015, www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/.

Bickert, Monika and Brian Fishman. “Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook?” *Facebook Newsroom*, 23 Apr. 2018, newsroom.fb.com/news/2018/04/keeping-terrorists-off-facebook/.

Boyle, Michael J. “The costs and consequences of drone warfare.” *International Affairs*, vol. 89, no. 1, 1 Jan. 2013, pp. 1–29, https://doi-org.proxy.lib.umich.edu/10.1111/1468-2346.12002.

Breland, Ali. “Facebook Finds Evidence of Iranian Disinformation Campaign.” *The Hill*, Capitol Hill Publishing Corp., 26 Oct. 2018, 12:41 PM EDT, thehill.com/policy/technology/413344-facebooks-finds-evidence-of-iranian-disinformation-campaign.

Carbone, Christopher. “Hezbollah Reportedly Claims Facebook, Twitter Have Disabled Their Main Accounts.” *Fox News*, FOX News Network, LLC., 25 June 2018, www.foxnews.com/tech/hezbollah-reportedly-claims-facebook-twitter-have-disabled-their-main-accounts.

Davidson, Adam. “Hamas: Government or Terrorist Organization?” *NPR*, NPR, 6 Dec. 2006, www.npr.org/2006/12/06/6583080/hamas-government-or-terrorist-organization.

DeAngelis, Tori. “Understanding Terrorism.” *Monitor on Psychology*, vol. 40, no. 10, Nov. 2009, pp. 60,

doi:10.1037/e537342009-007.

Dewicki, Marielle. “Marielle Dewicki.” *Facebook*, 1 Jan. 2019, https://www.facebook.com/profile.php?id=100010255831423.

Domonoske, Camila. “Facebook Expands Use Of Facial Recognition To ID Users In Photos.” *NPR*, NPR, 19 Dec. 2017, 1:39 PM ET, www.npr.org/sections/thetwo-way/2017/12/19/571954455/facebook-expands-use-of-facial-recognition-to-id-users-in-photos.

Ellick, Adam B., et al. “Meet the KGB Spies Who Invented Fake News.” *The New York Times*, The New York Times, 12 Nov. 2018, 15:34, www.nytimes.com/video/opinion/100000006210828/russia-disinformation-fake-news.html.

European Union, European Parliamentary Research Service. “Understanding Definitions of Terrorism.” *At a Glance*, by Patryk Pawlak and Members’ Research Service, Nov. 2015, http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf.

“Fool Me Once...” *Digital Citizens Alliance*, Digital Citizens Alliance, May 2018, digitalcitizensalliance.org/clientuploads/directory/Reports/DigitalCitizens_FoolMeOnce-Final.pdf.

Geiger, Abigail. “How Americans Have Viewed Surveillance and Privacy since Snowden Leaks.” *Pew Research Center*, Pew Research Center, 4 June 2018, www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

Grabinsky, Jonathan, and Avi Jorisch. “Fighting Terrorism and Radical Media: The Impact of al-Manar.” *Chicago Policy Review*, Chicago Policy Review, 7 June 2013, chicagopolicyreview.org/2013/06/07/fighting-terrorism-and-radical-media-the-impact-of-al-manar/.

Greenwald, Glenn. “Documents from *No Place to Hide*.” *Glenn Greenwald*, Holtzbrink Publishers, LLC., pp. 137-64, static.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Uncompressed.pdf.

Greenwald, Glenn. “No Place to Hide: Edward Snowden, the N.S.A., and the U.S. Surveillance State.” *Glenn Greenwald*, Holtzbrink Publishers, LLC., glenngreenwald.net/#BookDocuments.

Hatmaker, Taylor. “Zuckerberg Denies Knowledge of Facebook Shadow Profiles.” *TechCrunch*, Verizon Media, 11 Apr. 2018, techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/.

Hern, Alex, and David Pegg. “Facebook Fined for Data Breaches in Cambridge Analytica Scandal.” *The Guardian*, Guardian News and Media Limited, 10 July 2018, 19:01 EDT, www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal.

“John O. Brennan Quotes.” *BrainyQuote*, Xplore, www.brainyquote.com/quotes/john_o_brennan_524831.

Lapowsky, Issie. “Gruesome Jihadi Content Still Flourishes on Facebook and Google+.” *WIRED*, Conde Nast, 17 May 2018, 12:00, www.wired.com/story/jihadi-content-still-on-facebook-google/.

Macdonald, Stuart. “How Tech Companies Are Trying to Disrupt Terrorist Social Media Activity.” *Scientific American*, Springer Nature America, Inc., 26 June 2018, www.scientificamerican.com/article/how-tech-companies-are-trying-to-disrupt-terrorist-social-media-activity/.

Masters, Jonathan, and Zachary Laub. “Hezbollah.” *Council on Foreign Relations*, Council on Foreign Relations, 3 Jan. 2014, www.cfr.org/backgrounder/hezbollah.

Mehta, Aaron. “Here's How Much the US Has Spent Fighting Terrorism since 9/11.” *Defense News*, Sightline Media Group, 16 May 2018, https://www.defensenews.com/pentagon/2018/05/16/heres-how-much-the-us-has-spent-fighting-terrorism-since-911/.

Middle East Monitor. “Twitter Blocked Hamas, Hezbollah Accounts at Israel's Demand.” *Middle East Monitor*, Middle East Monitor, 21 Dec. 2018, 2:17 PM, www.middleeastmonitor.com/20181221-twitter-blocked-hamas-hezbollah-accounts-at-israels-demand/.

Mueller, John. “US Counterterrorism Spending Since 9/11.” *Stimson*, The Stimson Center, 16 May 2018, 12:00, https://www.stimson.org/content/us-counterterrorism-spending-911.

Mueller, John, and Mark G. Stewart. “Evaluating Counterterrorism Spending.” *The Journal of Economic Perspectives*, vol. 28, no. 3, 2014, pp. 237–247. JSTOR, JSTOR, www.jstor.org/stable/23800585.

Nowrasteh, Alex. “Counterterrorism Spending.” *Cato Institute*, Cato Institute, 25 May 2018, 11:12, www.cato.org/blog/counter-terrorism-spending.

Office of the United Nations High Commissioner for Human Rights (OHCHR). “UN human rights expert says Facebook’s ‘terrorism’ definition is too broad.” *United Nations Human Rights Office of the High Commissioner*, Office of the United Nations High Commissioner for Human Rights (OHCHR), 3 Sep. 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23494&LangID=E.

“Overheard at umich.” *Facebook*, 1 Jan. 2019, https://www.facebook.com/profile.php?id=100010255831423.

Patrikarakos, David. “Why Israel Is Losing the Social Media War.” *Tablet Magazine*, Nextbook Inc., 25 June 2018, 9:30 PM, www.tabletmag.com/jewish-news-and-politics/265160/israel-losing-social-media-war.

Prucha, Nico, and Ali Fisher. “Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda.” *CTC Sentinel*, vol. 6, no. 7, June 2013, pp. 19–23, https://ctc.usma.edu/tweeting-for-the-caliphate-twitter-as-the-new-frontier-for-jihadist-propaganda/.

Sales, Nathan A. “U.S. Department of State Counterterrorism Bureau: The FY 2018 Budget.” *Statement Before the Subcommittee on Terrorism, Nonproliferation, and Trade of the House Foreign Affairs Committee, U.S. Department of State*, Office of Website Management, Bureau of Public Affairs, 7 Sept. 2017, https://www.state.gov/j/ct/rls/rm/273854.htm. Text transcription of hearing.

Schiff, Neal, and Michael Heimbach. “Counterterrorism - I.” *FBI.gov*, U.S. Department of Justice, 21 Aug. 2009, www.fbi.gov/audio-repository/news-podcasts-inside-counterterrorism-2013-i.mp3/view.

"Signs of Possible Terrorist Activity." *Metropolitan Police*, Metropolitan Police, www.met.police.uk/advice/advice-and-information/t/terrorism-in-the-uk/signs-of-possible-terrorist-activity/.

Silver, Vernon and Sarah Frier. "Terrorists Are Still Recruiting on Facebook, Despite Zuckerberg's Reassurances." *Bloomberg Businessweek*, Bloomberg L.P., 10 May 2018, 6:00, www.bloomberg.com/news/articles/2018-05-10/terrorists-creep-onto-facebook-as-fast-as-it-can-shut-them-down.

Steinbach, Michael. "ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media." *Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations*, *FBI.gov*, U.S. Department of Justice, 6 July 2016, https://www.fbi.gov/news/testimony/isil-online-countering-terrorist-radicalization-and-recruitment-on-the-internet-and-social-media-. Text transcription of hearing.

The United Nations Office on Drugs and Crime (UNDOC). "Module 4: Criminal Justice Responses to Terrorism." *E4J University Module Series: Counter-Terrorism*, The United Nations Office on Drugs and Crime (UNDOC), www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html.

"Twitter Rules enforcement - January to June 2018." *Transparency Report*, Twitter, 2018, transparency.twitter.com/en/twitter-rules-enforcement.html.

United States, Central Intelligence Agency, "Support to the War on Terrorism and Homeland Security." *Annual Report 2003,* Central Intelligence Agency, 3 Jan. 2012, www.cia.gov/library/reports/archived-reports-1/Ann_Rpt_2003/swtandhs.html.

United States, Congress, Senate, Committee on Homeland Security and Governmental Affairs. *Jihad 2.0: Social Media in the Next Evolution of Terrorist Recruitment*. United States Government Publishing Office, 7 May 2015, https://www.hsdl.org/?view&did=798565. Text transcription of hearing.

United States, Executive Office of the President, White House Office of the Press Secretary. "Executive Order 12947: Prohibiting Transactions with Terrorists Who Threaten to Disrupt the Middle East Peace Process; January 23, 1995." *The Avalon Project: Documents in Law, History, and Diplomacy*, Lillian Goldman Law Library, 2008, avalon.law.yale.edu/20th_century/pal05.asp.

United States, Office of the Director of National Intelligence, National Counterterrorism Center. "History." *Who We Are, National Counterterrorism Center*, Office of the Director of National Intelligence, https://www.dni.gov/index.php/nctc-who-we-are/history.

United States, U.S. Department of Defense, Office of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff. *National Military Strategic Plan for the War on Terrorism*, U.S. Department of Defense, 25 Jan. 2006, archive.defense.gov/pubs/pdfs/2006-01-25-Strategic-Plan.pdf.

United States, U.S. Department of Justice, Federal Bureau of Investigation. "CATHERINE MARIE KERKOW." *FBI.gov*, U.S. Department of Justice, 25 Nov. 2013, www.fbi.gov/wanted/dt/catherine-marie-kerkow/.

United States, U.S. Department of Justice, Federal Bureau of Investigation. "CHERI LAVERNE DALTON." *FBI.gov*, U.S. Department of Justice, 2 Feb. 2015, www.fbi.gov/wanted/dt/cheri-laverne-dalton/.

United States, U.S. Department of Justice, Federal Bureau of Investigation, “DONNA JOAN BORUP.” *FBI.gov*, U.S. Department of Justice, 26 July 2011, www.fbi.gov/wanted/dt/donna-joan-borup/.

United States, U.S. Department of Justice, Federal Bureau of Investigation. “Sex Trafficker Receives 40-Year Sentence.” *FBI.gov*, U.S. Department of Justice, 14 /oct. 2014, https://www.fbi.gov/news/stories/sex-trafficker-receives-40-year-sentence.

United States, U.S. Department of Justice, Federal Bureau of Investigation. “Terrorism.” *FBI.gov*, U.S. Department of Justice, 3 May 2016, www.fbi.gov/investigate/terrorism.

United States, U.S. Department of Justice, U.S. Attorney's Office: District of New Mexico. “Multi-Agency Investigation Disrupts Heroin Trafficking Pipeline Between Ciudad Juarez and Las Cruces, N.M., Facilitated by Social Media Messaging Platform.” Department of Justice, 28 Aug. 2018, https://www.justice.gov/usao-nm/pr/multi-agency-investigation-disrupts-heroin-trafficking-pipeline-between-ciudad-juarez-and.

United States, U.S. Department of Justice, U.S. Attorney's Office: District of New Mexico. “Two New Mexico Men Facing Federal Charges Arising From Social Media School Shooting Threats.” Department of Justice, 23 Feb. 2018, www.justice.gov/usao-nm/pr/two-new-mexico-men-facing-federal-charges-arising-social-media-school-shooting-threats.

United States, U.S. Department of Justice, U.S. Attorney’s Office: Eastern District of Virginia. “Manassas Man Sentenced to 11 Years for Providing Material Support to ISIS.” *FBI.gov*, U.S. Department of Justice, 28 Aug. 2015, https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/manassas-man-sentenced-to-11-years-for-providing-material-support-to-isil.

United States, U.S. Department of State, “The Global Coalition to Defeat ISIS.” *U.S. Department of State*, Office of Website Management, Bureau of Public Affairs, www.state.gov/s/seci/.

United States, U.S. Department of State, Bureau of Counterterrorism. “Foreign Terrorist Organizations.” *U.S. Department of State*, The Office of Website Management, Bureau of Public Affairs, www.state.gov/j/ct/rls/other/des/123085.htm.

United States, U.S. Department of State, Office of the Coordinator for Counterterrorism. “Executive Order 13224.” *U.S. Department of State*, Office of Website Management, Bureau of Public Affairs, 23 Sept. 2001, www.state.gov/j/ct/rls/other/des/122570.htm.

United States, U.S. Department of State, Office of the Spokesperson. “Global Counterterrorism Forum Co-Chairs' Fact Sheet: About the GCTF.” *U.S. Department of State,* Office of Website Management, Bureau of Public Affairs, 27 Sept. 2015, 2009-2017.state.gov/r/pa/prs/ps/2015/09/247369.htm.

United States, U.S. Department of State, The Coalition Information Centers. “The Global War on Terrorism: The First 100 Days.” *U.S. Department of State*, Office of Website Management, Bureau of Public Affairs, 2001, 2001-2009.state.gov/s/ct/rls/wh/6947.htm.

United States, White House Press Center, White House Briefing Room. “Press Briefing by Attorney General, Secretary of HHS, Secretary of Transportation, and FEMA Director.” *The American Presidency Project*, UC Santa Barbara, 11 Sep. 2001, https://www.presidency.ucsb.edu/documents/press-briefing-attorney-general-secretary-.

“Violent Extremist Groups.” *Twitter*, Twitter, help.twitter.com/en/rules-and-policies/violent-groups.

Wiley, Winston P. “Testimony Before Senate Governmental Affairs Committee.” *Central Intelligence Agency*, Central Intelligence Agency, 20 June 2008, https://www.cia.gov/news-information/speeches-testimony/2003/wiley_speech_02262003.html.