PEPPERDINE UNIVERSITY

Pepperdine Policy Review

Volume 13 Article 4

5-7-2021

Tweeting Terror: Evaluating Changes to the Terror Recruitment and Radicalization Process in the Age of Social Media

Jackson T. Grasz
Pepperdine University, jacksongrasz@gmail.com

Follow this and additional works at: https://digitalcommons.pepperdine.edu/ppr

Recommended Citation
Grasz, Jackson T. (2021) "Tweeting Terror: Evaluating Changes to the Terror Recruitment and Radicalization Process in the Age of Social Media," *Pepperdine Policy Review*: Vol. 13, Article 4.
Available at: https://digitalcommons.pepperdine.edu/ppr/vol13/iss1/4

This Article is brought to you for free and open access by the School of Public Policy at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Policy Review by an authorized editor of Pepperdine Digital Commons. For more information, please contact bailey.berry@pepperdine.edu.

INTRODUCTION

"Every time there's a new tool, whether it's Internet or cell phones or anything else, all these things can be used for good or evil. Technology is neutral; it depends on how it's used." ~ Rick Smolan

Although the internet itself is not new, it is continually reinventing itself. As it changes, people use it in novel ways that bring new and sometimes terrible consequences. And so, in late August of 2014, one of the internet's newer evolutions, social media, was thrust into the center of controversy as popular social media websites like Twitter began circulating a terrifying video far and wide throughout the vast reaches of their audiences. A man clad in black, waving a knife in his hand and issuing threats to America, stood menacingly in a desert scene. Another man knelt calmly before him. This man, James Foley, was just moments from death when his captor's blade would separate his head from his body . The aftermath of the gruesome scene and the threating message that accompanied it were suddenly catapulted across all reaches of society as people on social media sites shared the video, some for its shock value and others who were simply in disbelief of what they just watched. But there were others who, with their estimated 45,000 associated Twitter accounts, intentionally shared the video for its message and helped launch ISIS and its quest for a caliphate onto the global center stage (Berger, 2015).

Since then, social media platforms have waged a hard, but ill-fought battle against terror groups using the platforms to spread propaganda, recruit, and ultimately radicalize new individuals for their cause around the world. But what, if any, notable effects does this method have on these individuals and how they are recruited and radicalized? Is social media really a drastically new form of recruitment, or is it simply the latest technological convenience being used to communicate just as cell phones were when they were invented? This paper will examine this research question: do any significant differences exist between social media radicalization and recruitment methods as compared to other more traditional methods. This author hypothesizes that social media has created significant new recruiting advantages for terror organizations and that it has also introduced a new form of online self-radicalization that did not previously exist. This theory will be examined through a meta-analysis of researchers' studies on the recruitment strategies of terror groups and the radicalization process of group and lone-wolf terrorists. The hypothesis of a new kind of online self-radicalization will be examined through a case study of the 2019 terror attack on Christchurch, New Zealand. Finally, in light of these findings, recommendations will be made as to how the government, social media companies, and society should address these

new trends in terror recruitment. Special attention is given to poorly understood concepts such as how communications through social media platforms and other internet forums function different than more direct, traditional methods of communication.

VIRTUAL RECRUITMENT AND RADICALIZATION: A LITERATURE REVIEW

Internet-based communication platforms, and social media in particular, have quickly become the predominant communication and recruitment mediums for new members of international terror organizations (Aly; Blaker; Hamm; Koehler; Smith). They are used to target recruits from younger generations who are already familiar with this technology as a regular part of their everyday lives. For example, groups like al-Qaeda and ISIS have been known for posting martyrdom videos to the internet to inspire new recruits while regularly engaging in online chatrooms and instant messaging through sites like Facebook and Twitter to communicate directly with potential recruits (Smith, 2018). Extreme right-wing groups have begun to migrate from political rallies and specific websites to using social media as their main propaganda tools for radicalizing new individuals (Koehler, 2014). While other more traditional methods of recruitment are still utilized by these kinds of groups, the dominance of recruiting via social media is an important trend to analyze because of the significant recruiting advantages it affords radical groups over other forms of communication like cell phones, radio, email, and face-to-face meetings.

Social Media as a Recruitment Tool

The ability to recruit via social media offers terror organizations several distinct advantages when attempting to find, recruit, and radicalize new individuals for their cause. First, social media sites afford organizations with limited resources an immediate global audience. The growing interconnectedness of the world via the internet is helping radical terror groups effortlessly expand their reach across international borders that their recruitment capabilities might otherwise be confined to (Aly; Blaker; Gill; Huey). This dramatically expands the number of potential recruits and supporters these groups can reach and creates second-order effects with substantial benefits. For example, by virtually recruiting individuals overseas to carry out foreign terror attacks, these groups save significant sums of money that would have been spent on international travel. Additionally, by avoiding frequent travel in and out of their host country to the target nation, they also avoid the risk of being detected by authorities abroad.

A second recruitment benefit is that social media enables individuals with a high potential of being radicalized to seek out the terror groups on their own by

browsing digital content and initiating dialogue (Aly; Gill; Hamm; Huey). This saves these organizations from bearing the entire burden of trying to locate potential recruits and helps them connect with many who would otherwise be overlooked simply because of a lack of direct personal connections. In particular, "lone wolf" radicals, individuals who may carry out acts of violence by themselves, now have access to digital communication mediums that help them seek out other people with similar radical beliefs. This provides opportunity for dialogue with other radicals when previously they were isolated individuals and lacked the confidence that comes from group identity (Hamm; Smith). This process also has the potential to serve as a risk reduction tool for recruiters. As individuals who are comfortable with radical messaging will seek out, find, and engage with the recruiters online, the organizations reduce the risk of exposing their ties to terror with non-radical individuals who would report their activity.

The most widely researched recruitment benefit afforded by social media is its ability to cultivate an echo chamber for the radical beliefs of new recruits while creating a community to draw them into (Behr; Gill; Hamm; Klausen; Smith; United Nations Office on Drugs and Crime). Social media, unlike traditional forms of media such as cable television or newspapers, provides content that can be curated exclusively by the end user. As people have a natural tendency to follow sources of information with which they agree, recruiters can encourage new recruits to follow and digest more radical sources of thought and tune out other ideas (Behr; Klausen). This reinforcement of ideas proves effective in getting the individual to more closely identify with the expressed radical sentiments. More importantly, the recruits now see similar information coming from a number of people, accounts, organizations, etc. and begin to build a sense of belonging to a community beyond their individual self (Behr; Gill; Smith; United Nations Office on Drugs and Crime). Additionally, this creates a sense of "strength in numbers" or "pack" mentality that can encourage individual "lone wolves" to carry out actions they would not otherwise do on their own without encouragement from the group.

Social Media as a Radicalization Mechanism

Recruitment is only the first step in interacting with a radical individual who could potentially commit acts of terror. In order for the individual to progress to the point where they are willing to carry out acts of violence, typically against a rational understanding of self-interest, a more robust process of radicalization must take place. Whether or not social media can actually provide a sufficient medium for the full radicalization process to take place is a matter of debate. On one end of the spectrum, some research indicates there are cases where the vast majority of an individual's radicalization occurred via the internet and social media (Blaker, 2015). This was the case for more than 3000 individuals who left behind their lives

in developed Western nations to join the enlisted ranks of the Islamic State of Iraq and Syria (ISIS). Cases like these, however, are often associated with particular groups and do not necessarily warrant extrapolation to other instances of radicalization. On the other end of the spectrum are those who argue that full radicalization can only occur from real-world interactions between people and that social media only acts as a transmitter of information (Huey, 2015). This assertion, though, does not offer a robust explanation for terror attacks carried out by individuals or small groups with no direct, physical access to the parent terror organization.

As such, the majority of the literature on this subject falls somewhere between these two extremes. It is widely thought that social media is at minimum a successful facilitator of radicalization, but it must be coupled with other factors (Behr; Gill; Huey; Smith). The most significant factors are group dynamics, such as affinity for one another (perceived or real), and group strength (Klausen; Smith). It is also commonly held that radicalization is not dependent on the use of social media and it is debatable whether or not it can accelerate the radicalization process (Behr; Gill). It is, however, particularly effective at radicalizing lone individuals who require group interaction and encouragement in order to progress to the more advanced stages of radicalization that create a willingness to commit violent acts. The psychological effects are particularly strong on these individuals as recruiters are able to more easily manipulate them to alter their beliefs by rewarding them with group affinity. Ultimately, they lead the recruit to create a sense of identity associated with more extreme behaviors (Aly; Hamm; Klausen; United Nations Office on Drugs and Crime).

The question that looms over the debate on the efficacy of radicalization via social media is whether or not this new medium differs in substantial and significant ways from traditional media and other means of communication such that it is more effective, or if it is simply a new tool in the recruiter's toolbox that has limited capabilities. While no studies are conclusive on this point, the current literature does provide clues as to what makes social media so potent as a medium for recruitment and radicalization.

Social Media's Impact on Terrorism

A number of factors work seamlessly together to facilitate social media's impact on terror organization recruitment. First, social media provides complete control over messaging to the terror organization (Aly; Huey; Klausen). This differs drastically from the traditional terror/media/audience relationship of newspapers and television where an organization could commit an act to get their message out, but whether or not it was portrayed sympathetically was at the mercy of the media. Now, these organizations can reach just as broad of an audience, while tailoring the

messaging attached to their acts to those they are trying to influence the most. This relates to the second compounding factor. Social media allows for the rapid dissemination of information to the intended audience (Huey; Klausen; United Nations Office on Drugs and Crime). Terror organizations can message followers around the world with minute-by-minute details. A clear example of this occurred in 2013 when al-Shabaab live-tweeted their attack on the Westgate shopping center in Nairobi (Aly, 2017). This ability to not only send information quickly, but to be able to include videos, professionally made images, or other culturally relevant forms of messaging heightens the effectiveness of this recruitment method (Aly; Huey; Klausen).

These factors and others contribute to the efficacy of social media recruitment and radicalization that make this form of communication fundamentally different than previous forms. They have replaced the need for physical contact of recruits and brought professional-grade messaging formats to an instant audience of the organization's own choosing, making social media one of the most important factors in individual radicalization (Huey; Koehler; United Nations Office on Drugs and Crime). Those who disagree largely base their argument on the notion that social media by itself has rarely been the sole factor in radicalization, claiming that other forms of contact or communication are needed (Behr; Gill). But this does not disprove the idea that radicalization *can* be achieved solely online nor does it negate that social media platforms and virtual interactions like web chats often double for the other factors such as community and personal interaction. So, while there are some natural advantages to recruiting new operatives through in-person interactions, social media has nonetheless expanded the recruiter's reach far beyond what would otherwise be possible.

Research Gaps

As it stands, the current literature provides deep analysis of an array of modern terror recruitment techniques conducted via the internet and social media platforms. What is missing, generally, is actionable data. Too little is known, publicly at least, to be able to draw wide conclusions or make comparisons about different forms of terror-related messaging and their overall efficacy in converting followers into violent terrorists. The literature is also currently limited almost exclusively to Islamic terrorism and some American right-wing radical groups' recruitment tactics. Other kinds of radical, terroristic organizations need to be studied to find patterns or dissimilarities between their utilization of social media and the ones described. If and when these deeper conclusions can be made across violent groups, better-informed decisions about how to disrupt these recruitment tactics can be made. Presently, most of the efforts focus on simply banning the social media accounts supporting terror groups, but it has proven to be nearly impossible to shut

them all down as they can be created just as quickly as they are shut down (Blaker, 2015). This "whack-a-mole" approach is not sustainable in the long term as terror groups can find ways to avoid such bans by utilizing social media websites and apps that are more difficult for law enforcement to track their activity on. Instead, the present challenge demands a more robust approach to locate, counter, and disempower this messaging.

METHODS

This paper examines recommended best practices for the three principal players in addressing the use of social media in spreading terror: the government, social media companies, and society at large. These three entities were chosen because they bear unique roles in how terror groups are able to spread their messaging through social media via their abilities to curb it legally, prevent and remove it voluntarily, and respond to it, respectively. Specifically, sources were chosen for their documentation of such prevention efforts in recent history and for their analysis and recommendations of best practices going forward. The conclusions drawn from this wide analysis will be applied to a recent case, the March 15th, 2019 terror attacks on two mosques in Christchurch, New Zealand. This particular attack was chosen among other examples for several reasons. First, it is one of the clearest examples of the evolving roles of the internet and social media platforms as they pertain to radicalizing individuals towards violence as well as their use for spreading the intended message of the terror attack. Second, this attack challenges popular notions of what kinds of extremism should be most pertinent to prevention efforts. While it can be shown that much work has been done to curtail social media messaging of prominent jihadist organizations like ISIS and Al Qaeda, far less attention has been given to smaller terror organizations of varying intents, including those promoting racial supremacy or anti-Islamic sentiments such as those the Christchurch terrorist was linked with. Finally, by examining this attack in detail, clues about gaps in the current prevention system can be assessed, the responses to the attack by the three chosen stakeholders can be critiqued, and further recommendations can be made as a result. If this attack is at all predictive of future developments in terror and the use of social media, it is thus important that it is examined in detail against current methods and assumptions.

This paper will not examine the use of private messaging apps or other one-to-one electronic communication platforms in detail. These will be addressed in general as the use of encrypted messaging is pertinent to the larger issue of terrorism but falls beyond the scope of this paper. Rather, this paper will look more closely at how messaging on large public forums for social interaction should be addressed as it has vastly different implications for society at large, as opposed to infiltrating the messaging systems of terror networks that are composed of

established members. So, while these trends are important to note, their solutions are markedly different than those that can be employed by the government, social media network giants, and the public for responding to propaganda that is ultimately intended to reach a public audience. Between them, these three groups also face different legal and moral questions regarding the actions they can take.

NEW ZEALAND CASE STUDY

March 15, 2019. 40 injured. 51 dead. These simple statistics cannot begin to describe the visceral pain inflicted upon New Zealand's Christchurch and its Muslim community. As details trickled out about this devastating terror attack, one realization was quickly made clear: the terrorism of the past several decades was over, and terrorism in the age of social media had just begun. The lone terrorist made a field day out of the capabilities of social media in this new age. On the day before the attack, he posted pictures of his weapons on 8chan. On the day of, he released his lengthy political manifesto, filled with references to social media culture, on Twitter. A video of the attack itself was live streamed on Facebook for the whole world to see (Bogost, 2019). The attacker was virtually linked with multiple white supremacist groups from Australia, including through the Facebook pages of the United Patriots Front (UPF) and the True Blue Crew (Mann et al., 2019).

It is immediately clear that this attack, while ultimately stemming from extreme white supremacist and anti-immigrant beliefs, was largely influenced by the use and powers of social media. The shooter had been actively following online groups and participating in chat rooms that supported his beliefs and he played to the strengths of social media to get his manifesto and video of the attack to spread as far and wide and as quickly as possible. The most shocking revelation from this attack, however, is that this terrorist not only acted alone, but he was completely self-radicalized. Contrary to what many of the authors in the previous literature review have theorized, this shooting concretely demonstrated the ability for social media to be used to completely radicalize a terrorist for a cause without any direct communication or influence from an actual violent group. The shooter had isolated himself from community by choosing to live off of an inheritance and not seek out work (Zaczek, 2019). From there, he became radicalized by far-right anti-immigrant views through looking at message boards and Facebook groups. Despite deriving his views from these online mediums, he received no direct calls to violence from any members of these groups and never formed any sort of actual group identity with other extremists (Ravndal, 2019). Rather, the group bonding and group identity that is normally thought necessary to radicalize someone to commit acts of terrorism for a specific, shared ideology never took place. This vindicates the proposed hypothesis that direct recruitment and traditional group

isolation and identity formation processes are not required to fully radicalize a terrorist. They can self-isolate and self-radicalize entirely on their own through the use and influence of online propaganda and social media, even when it is not used for two-way communication. This case should serve as a cause for major rethinking about what is required in the radicalization process and how we go about trying to prevent it in the first place. Traditional methods may apply to traditional cases, but they will be of little use in stopping violent terrorists who are effectively isolated, indoctrinated, and radicalized to action without ever even corresponding with the groups that they are being influenced by.

After this terror attack, the New Zealand government responded quickly. Besides placing a ban on semi-automatic rifles, they took action regarding media content as well. First, they asked the social media platforms themselves to help curtail the spread of the shooter's messages. Facebook reported taking down 1.5 million copies of the video. The New Zealand police quickly urged people not to share the video of the attack or the manifesto, under threat of law (Lieu, 2019). In fact, an eighteen-year-old was arrested and charged for sharing the livestream of the shooting (Australian Associated Press, 2019). The New Zealand Government's response demonstrated a clear desire to swiftly combat the terrorist's social media goals with force while collaborating with the private companies the propaganda was hosted on. The success of their attempts to stop the dissemination of the content should be closely studied from multiple perspectives as the methods they used to suppress the information will likely prove controversial in other countries like the United States. Whether or not these heavy-handed approaches will effectively prevent another similar attack cannot be known for some time. Nations around the world would be wise to study the response to this attack closely as test of whether or not their own anti-terrorism methods need to be altered or enhanced in the age of social media.

GOVERNMENT RESPONSE

From the Joint Terrorism Task Force, counter-terrorism military units, and the Department of Homeland Security, to city police forces and local school district memorandums, terrorism has forcefully seized the attention of every level of government and poses hard questions that must be addressed by every governing body involved in public security. While many lessons have been learned and turned into effective policy, the recent trend in social media influence on terrorism has opened up a new set of quandaries. This medium of terror can't be fought with bullets and is resilient to deterrence by laws. Nevertheless, government agencies must be determined to act on this trend and prevent further tragedy through legal means that value both the lives of citizens and their individual rights.

As is often the case in analysis, determining what not to do is just as important as figuring out what to do. The government certainly has its place in addressing this issue, but the boundaries of what are useful must first be set. Without the ability to directly remove terror propaganda online or arrest inciters abroad, many initial plans by the federal government involved counter-messaging. These kinds of initiatives have roots in the early 2000s when the Bush administration attempted to improve the United States' image in the Middle East through government sponsored messaging via TV broadcasting. Studies showed, however, that this government-sponsored messaging actually worsened attitudes towards the U.S. (Bipartisan Policy Center, 2018). With the rising prominence of ISIS, the State Department's Center for Strategic Counterterrorism Communications (CSCC) (today it functions under the State Department's Global Engagement Center) began counter-messaging campaigns online that directly interacted with extremist sympathizers. The intent this time around, having learned from previous mistakes, was not to make the U.S. and its allies look good, but rather to be critical of the terror organizations themselves. This endeavor has also been regarded as largely unsuccessful and has even created unintended consequences such as legitimizing and drawing attention to otherwise unimportant, minor social media accounts by extremists (Bipartisan Policy Center, 2018). Other federal programs housed in places like the Department of Defense have met similar embarrassing failures.

While counter-messaging from state-sponsored media is generally ill-advised, the government does have another option that can be drastically more successful, though it is met with its own challenges. Rather than combatting existing online rhetoric, the government can attempt to remove and prevent the spread of violent extremist propaganda online. Instead of trying to counter messages, simply denying terror organizations the ability to utilize these public-facing platforms may be more effective. Given all the benefits of online recruitment outlined in the literature review, it should be considered a worthwhile endeavor. The primary hindrances to this approach, however, are typically the laws of the country wanting to counter online extremism. Many nations protect inflammatory speech from government censorship, although this varies country-to-country. European nations, for example, often have more flexibility to outlaw certain kinds of speech, such as Germany did in 2017 when it mandated social media platforms remove illegal terror speech within 24 hours of it being posted (Bipartisan Policy Center, 2018). Nations like the United States, on the other hand, face more obstacles as concerns about protecting the constitutional right to free speech are brought into question. Typically, graphic images and speech that would be considered "hate speech" are protected under the First Amendment to the United States Constitution. In order for speech to meet standards that allow for it to be censored, it must insight direct violence or pose a "clear and present danger" to other people (Haughom,

2016). While some terror propaganda can meet this threshold, the Federal Government is typically reserved in how it handles such cases. While it is wise for the government to continue to show deference to the free speech rights of its own citizens, it nevertheless cannot afford to dismiss the real danger posed by terror organizations' influence online. For instance, ISIS frequently claimed responsibility for lone-wolf terror attacks perpetrated by people influenced through its online calls for violence. E lectronic literature published by Al Qaeda affiliates influenced the Boston Marathon Bombers, the Pulse Nightclub shooter was radicalized online, and dozens of ISIS videos were found on the cellphone of the perpetrator of the 2017 New York City truck ramming attack (Isacson, 2018). In the case of the New Zealand terror attack in Christchurch, the government did respond by outlawing the sharing of any terror content related to the incident through social media (Lieu, 2019). It has yet to be seen if their government will attempt any counter-messaging campaigns or if they will focus strictly on targeting the removal of terror propaganda online. Other nations should closely watch this case as it continues to unfold and see whether or not these methods were successful in preventing the distribution of these materials, reducing future incidents of terror or hate crimes, and if the general public is accepting of these imposed restrictions.

SOCIAL MEDIA ORGANIZATIONS' RESPONSE

With the government's hands largely tied with respect to preventing and removing terror propaganda , an answer must come from the private sector. In previous years, social media companies often held themselves as unadulterated protectors of free speech. Twitter even once promised that it would never censor terrorists on its platform. But today that landscape has changed dramatically as large social media platforms face increasing public pressure to curtail their role in acts of violence. Presently , these networks employ three primary methods to disrupt the distribution of terror propaganda. First, many of these companies employ thousands of human reviewers who can sift through flagged content and deem it unacceptable for violating terms and conditions that specify that calls to extremism are not tolerated. This flagged content often then falls into the second method which is called automated blacklisting (Leetaru, 2018). When content has been flagged as unacceptable, an electronic 'tag' marks it so that if the same content appears again on the platform (e.g., a viral terror video making the rounds on Facebook) it will be automatically blocked before it can be shared again. While this method proved to be more scalable than relying on expensive human workers, it is not as precise as it cannot detect new content nor intelligently determine whether or not content violates established rules. This brought about the need for the third category of mechanisms: artificial intelligence and machine learning algorithms. Companies

like Google have developed state-of-the-art software programs that can identify extremist messaging in foreign languages, pick up inflammatory terrorist speech amidst loud propaganda videos, and even use reverse image searching to identify terror organization symbols and references embedded in images (Leetaru, 2018). According to these companies' own data, "every single minute there are on average 510,000 comments and 136,000 photos shared on Facebook, 350,000 tweets posted on Twitter, and 300 hours of video uploaded to YouTube" (Macdonald, 2018). With this tremendous amount of content to sift through, many of these organizations have teamed up to share database information to help each other more quickly recognize terror-related content when terror groups attempt to shift social media platforms after getting banned on one of them (Macdonald, 2018).

The largest challenge to this now successful process is that terror groups are increasingly able to utilize the reach of these public media platforms while hosting their content on smaller sites through a method called outlinking. Put s imply, they can host their content on smaller platforms that lack the resources to effectively fight their messages and spread links to it through the major media outlets and these posts go unmolested as the links themselves possess no content that will be flagged by a blacklist or even artificial intelligence. Finally, once they have successfully recruited new members, they can utilize encrypted messaging sites like Telegram so that none of their conversations can be picked up by social media sites and handed over to authorities (Macdonald, 2018).

While private social media companies do not have the same legal obligation to protect free speech that the government does, they should nevertheless make careful considerations for what kind of speech they will target for removal. A net cast too narrowly will miss harmful content that can lead to violent radicalization, while a net cast too wide may lead to the removal of speech that is legal, even if undesirable. Recent conversations in the United States about this kind of censorship, which is often accused of being politically motivated even when companies claim it is done for harm-reduction reasons, have begun to push for the removal of Section 230 protections for social media companies from the federal Communications Decency Act. Some proponents of this action argue that social media companies are acting as publishers when they choose to censor speech based on political content rather than legality, and therefore should lose protections intended for websites that simply host third-party generated content. Others argue that social media companies are actually not doing enough to remove harmful content or prevent illegal actions on their platforms (Allyn, 2021). If social media companies veer too far one way or the other, they may either find themselves having to choose to not censor any content, or they may have to become something akin to regular publishers in order to avoid litigation due to content posted on their sites by third parties. The best option, it seems, would be to improve the precision of content moderation policies and capabilities to ensure that illegal content, including calls

to radicalization and extremist violence, is removed, while other protected speech, including political speech, is protected vigorously. By tiptoeing across this thin tightrope, social media companies may be able to strike a balance that preserves their Section 230 protections, allows for free speech on their platforms, and protects society-at-large from the dangers of virtual radicalization via social media.

SOCIETAL RESPONSE

Defining terrorism is difficult. Understanding exactly what constitutes this designation will always be a subject of debate as methods of attacks and the agendas behind them continue to change shape. But one piece of the puzzle that has remained constant is the audience. All terror attacks have an intended audience beyond the immediate victims that is meant to react in some way to the attack. That is what fundamentally sets terrorism apart from other means of violence like crime or war. Despite this key element of what makes terrorism, *terrorism*, there is a profoundly shocking lack of academic or even journalistic writing on what or how society itself should respond to these new kinds of attacks or try to prevent them. It is a fatal mistake to assume that only the government or large private entities are capable of having an impact on how and why terror occurs. Ultimately, terrorism's lasting effects take a toll on society as a whole and the effects of social media have only served to amplify its reach and lasting impact (Innes, 2015).

Whatever methods are taken to prevent terror messaging or recruitment, it must be remembered that the root of all terrorist activity is the impact it seeks to have on its audience. But if that audience doesn't give terror the time of day, then the terror might just go away. Violent acts may still occur, but it is likely that they will be far less frequent as the appeal that fame and importance have slowly drift away. If this country really wants to protect itself, it must start by changing the way this generation plays into the hands of the terrorists and teaching the next generation to do the same. The Christchurch attack cannot be ignored. It is a crystal-clear example of how modern society and its social media inundation have enabled and emboldened individual terrorists to act with shocking levels of sophistication to achieve their political aims. If its causes go ignored, our own nation and others like it may be doomed to repeat it. Ironically, perhaps, paying additional focus to this attack may finally help us understand what has gone so horribly wrong with the way our modern society fixates on these terror attacks and inadvertently elevates the political aims of the perpetrators by splashing their names, faces, and motivations across cable news and social media platforms alike. Preventing the next terrorist from ever self-radicalizing online is a noble goal, but it can only be achieved through a joint effort that stretches across society and unites it as a whole.

CONCLUSION

Social media was all fun and games (or perhaps cats and memes) until people started getting hurt. Society is beginning to reckon with the absolute power, both for good and for evil, that modern technology has brought about with instant unfiltered global communications. Like all other facets of society, terror organizations have latched onto the previously untapped abilities of these tools and utilized them for their own nefarious purposes. This study highlighted a number of important findings pertaining to this reality. First, social media has allowed for a reversal of the terror recruitment process. Now, vulnerable individuals can find their way to the propaganda of recruiters instead of the other way around. Second, social media expands the reach of these recruiters past geographic constraints. No longer must they worry about being caught during the process of crossing international borders, much less the expense of it all. Instead, they can access potential new members anywhere in the world, at any given time, at no cost. Third, social media can create a virtual community and echo chamber for radical beliefs. It allows for terror-minded groups and individuals to control the messaging that is bombarding isolated recruits such that they begin to internally embrace the group identity process and the confirmation bias that accompanies it. Finally, and most importantly, social media can suffice as a medium to fully radicalize an individual without the need for any direct contact by a radical group. This is a fundamental shift from what used to be theorized about what was required for the radicalization of new terrorists. While the group identity and isolation process is still important, it can be achieved solely through self-radicalization means online as demonstrated in the 2019 Christchurch terror attack. Counterterrorism efforts around the world must now ask if new measures are necessary to combat the process of social media radicalization and determine what research needs to be done accordingly. Finally, governments, social media companies, and society itself must all ask what responsibility falls on them to adapt to and ultimately prevent social media radicalization in the future.

WORKS CITED

Allyn, B. (2021). "As Trump Targets Twitter's Legal Shield, Experts Have a Warning" *NPR.* npr.org

Aly, A. (2017). "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization" *Taylor & Francis Group*

Australian Associated Press. (2019, 18 March). "Teenager Accused of Sharing Video of Christchurch Terror Attack Denied Bail" *AAP*. 9news.com.au

Behr, I. (2013). "Radicalization in the Digital Era" *RAND Corporation*

Berger, J.M. (2015, 27 Jan). "The Evolution of Terrorist Propoganda: The Paris Attack and Social Media" *Brookings.* brookings.edu

Bipartisan Policy Center. (2018, March). "Digital Counterterrorism: Fighting Jihadists Online" Bipartisanpolicy.org

Blaker, L. (2015). "The Islamic State's Use of Online Social Media" *Military Cyber Affairs: The Journal of the Military Cyber Professionals Association*

Bogost, I. (2019, 15 March). "Social Media are a Mass Shooter's Best Friend" *The Atlantic.* theatlantic.com

Gill, P. (2017). "Terrorist Use of the Internet by the Numbers" *Criminology and Public Policy*

Hamm, m. and Spaaj, R. (2015, Feb). "Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies" *National Criminal Justice Reference Service*

Haughom, J. (2016, 16 Nov). "Combatting Terrorism in a Digital Age: First Amendment Implications" *Freedom Forum Institute*. Freedomforuminstitute.org

Huey, L. (2015). "This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming" *Contemporary Voices: St Andrews Journal of International Relations*

Innes, M. (2015, March). “Security, Terrorism, and Social Media” *Economic and Social Research Council*. esrc.ukri.org

Isacson, Z. (2018, 2 Sept). “Combatting Terrorism Online: Possible Actors and their Roles” *Lawfare.* lawfareblog.com

Klausen, J. (2015). “Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq” *Taylor & Francis Group*

Koehler, D. (2014). “The Radical Online: Individual Radicalization Processes and the Role of the Internet” *Journal for Deradicalization*

Leetaru, K. (2018, 9 Oct). “Can We Finally Stop Terrorists from Exploiting Social Media?” *Forbes.* Forbes.com

Lieu, J. (2019, 15 March). “A Live Streamed Video of a Shooting Keeps Being Shared, Despite Pleas Not To” *Mashable.* mashable.com

Macdonald, S. (2018, 26 June). “How Tech Companies are Trying to Disrupt Terrorist Social Media Activity” *Scientific American.* Scientificamerican.com

Mann, A; Nguyen, K; Gregory, K. (2019, 23 March). “Christchurch Shooting Accused Brenton Tarrant Supports Australian Far-Right Figure Blaire Cottrell” *ABC.* abc.net.au

Ravndal, J. (2019, 16 March). “The Dark Web Enabled the Christchurch Killer” *Foreign Policy.* foreignpolicy.com

Smith, A. (2018, June). “How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us” *National Institute of Justice*

Smolan, R.; Erwitt, J. (2012). “The Human Face of Big Data” *Against All Odds Productions.*

United Nations Office on Drugs and Crime. (2012). “The use of the Internet for terrorist purposes”

Zaczek, Z. (2019, 23 March). “Australian white supremacist accused of killing 50

Muslims called far right nationalist Blair Cottrell 'Emperor' three years before mosque massacre - as it is revealed he was living off a $500,000 inheritance" *Daily Mail.* msn.com