Effective Counterterrorism:

Has Counterterrorism Policy Been Effective in Combating Racially and Ethnically Motivated Violent Violent Extremism in the 21st Century?

Sebastian Arnold Veron

California State Polytechnic University, Pomona

This study analyzes the effectiveness of counterterrorism policy by the United States to address the recent increased trend of alarming domestic attacks carried out by Racially and Ethnically Motivated Violent Extremism (REMVE). U.S. counterterrorism policies are closely analyzed to identify the most successful means of combating REMVE in the 21st century, as the threat landscape posed by REMVE has changed to encompass primarily white-identity terrorism and other types of right-wing extremist. Each of these counterterrorism policies are examined through an empirical case study, measuring the U.S. ability to effectively detect, disrupt, and dismantle REMVE networks and cells. The results from this study suggest a comprehensive multi-agency approach in coordination with domestic and international institutions must be taken in order to effectively combat the increased threat posed by REMVE in the 21st Century.

The origins of the word Terrorism come from the French revolutionary period of the eighteen-century known as the Reign of Terror or known more simply as the Terror. Meant to characterize the brutality of the state-sponsored attacks at the time against the civilian populations; however, terrorism itself has occurred throughout nearly all of human history. Currently, there is no established universal definition of terrorism regarding what constitutes a terrorist and the attacks they carry out. This becomes even more problematic with some states in the international system having more than one definition for defining terrorism, such as the United States of America (USA). However, three main widely accepted criteria must be established when classifying terrorism; the first is that the actors involved must be either subnational groups, individuals, or clandestine agents. Second is the targeting; the targets in nearly all instances of terrorism consist of civilian targets. Lastly, one of the most important aspects is the intentions or motivates behind the attacks must be politically motivated. The importance of understanding

Created by Sebastian Veron, Department of Political Science, California State Polytechnic University, Pomona. Correspondance concerning this research paper should be addressed to Sebastian Veron, Department of Political Science, California State Polytechnic University, Pomona. Email: saveron@cpp.edu

Undergraduate Journal of Political Science, Vol. 5, No. 1, Spring 2021. Pp. 193-208

how terrorism is classified is to distinguish between acts of terrorism and other kinds of crimes or causes of violence.

The past couple of decades has seen not just within the USA but across many different parts of the world a dramatic rise in a right-wing extremist ideology that has motivated various attacks and violent crimes against innocent civilians. However, a shift in how many of these right-winged extremist groups have chosen to organize themselves. Recently, there has been a notable trend in domestic terror groups to reduce the levels of their extremisms in the public's view to bring less attention from law enforcement agencies. These extremist groups' main focal points and principles have remained the same. Many of these right-wing domestic terror groups have maintained their underlining principles of racially motivated violence, anti-government, anti-Semitic, and anti-foreigner beliefs. Many of these hate-based extremist groups within the United States (US) have been able to operate and spread their radical ideologies with widespread protections as the result of constitutional protections of free speech, among other legal protections. One of the most significant threats to the USA today is the recent rise of Right Winged extremists, specifically, Racially and Ethnically Motivated Violent Extremist (REMVE).

As the US Intelligence Community (IC) has determined unanimously, the most significant national security threat currently being posed against the US is the continued rise of Right-wing domestic extremism. Since the 1990's these groups have attempted an increasing number of severe attacks, creating a significant potential for widespread casualties. In 1999 alone, two highly planned and organized significant attacks on the US had been prevented; however, this serves as a reminder of the gravity of the situation. Following the September 11th attacks against the US, the US had been caught off guard by one of the most significant intelligence failures to date. Many of the existing government agencies would find themselves quickly brought into the newly founded Department of Homeland Security (DHS) umbrella, whose new mission primarily focused on preventing future attacks through increased communication and intelligence sharing between the different intelligence agencies. However, the main types of terrorist threats that had become the focus of the US IC at the time had been foreign extremists and religious extremists, most specifically radical Islamic terrorist groups.

In the years following these destructive attacks against the US, many of the counterterrorism (CT) and foreign policy approaches the United States had taken had been seen to have mixed results, at times breaking domestic and international laws. Ultimately while the threat of foreign extremists still exists, it has become a lesser overall threat than the rising increase of REMVE actors. The result now has led many to question the US counterterrorism's effectiveness in preventing REMVE attacks. This thesis seeks to answer the question: Has Counterterrorism Policy Been Effective in Combating Racially and Ethnically Motivated Violent Extremism in the 21st Century? In the current political climate across the US, a prime example highlighting the importance of having effective strategy's in place to prevent attacks carried out by right-wing domestic extremist groups is the January 6th US Capitol riots in 2021. Many active members associated with REMVE groups were observed taking part in criminal acts at the US Capitol. As a result, I hypothesize that the US CT policy has not been able to effectively prevent attacks carried out by REMVE actors domestically within the United States.

LITERATURE REVIEW

The following review of literature is meant to provide an understanding of the current comprehension between terrorism, specifically REMVE actors, and how counterterrorism organizations have attempted to deter attacks by terrorists through their CT methods. The initial fundamental understanding is that there are no real significant differences between old terrorism and terrorism; instead, they are still fundamentally the same but utilize an increased amount of technology. Then moving to see how democratic states have shifted their approaches towards counterterrorism following the September 11th,

2001 attacks against the US, along with focusing on some of the possible driving factors behind an increase in right-wing domestic terror in the US. Next, the rise of different terrorist organizations to utilize various online methods in their organizations has led to different approaches being taken by counterterrorism agencies and the varying results and unexpected consequences that have emerged from it. Along with reviewing how in some cases, when attempting to deter terrorism activities, online counterterrorism policies have shifted towards preventing less likely possible attacks while also becoming more invasive in their intelligence gathering. Lastly, a game model is presented as an attempt to highlight some of the potential success of CT programs using technological advancements to deter possible terrorist attacks while also pointing out some of the current possible gaps in this approach.

The notion of there being a contrast between "New" terrorism and "Old" terrorism has been a considerable debate among many policymakers and academics; this has resulted in many rethinking how the two types of terrorism could be different. Recent scholars (Copeland, 2001) (Crenshaw, 2003) (Kalyvas, 2001) (Taylor, 2009) (Zhang, 2007) discuss how there is, in fact, no difference between the two forms of terrorism, explaining that the idea of new terrorism comes from insufficient historical knowledge along with a misinterpretation of contemporary terrorism. This argument establishes that contemporary terrorism remains still primarily based on political goals and views and is not, in contrast, a cultural phenomenon. It is then explained that terrorism has not changed to be fundamentally new since no difference has been established; instead, it has simply become elevated to a higher degree of intensity at times. Then by having distinguished between new and old terrorism, this would result in contradictions of information, unable to determine when the old terrorism would have ended, and the new terrorism would have started. As prior scholars have discussed, when examining possible contrast between new and old terrorism in its organizational structure, what is found is that there are vital issues when assuming the differences in the structural organization as being centralized and decentralized. This is given that there are many communication changes between new terrorist organizations, such as more online communication, which does not determine that the actual organizational structure of terrorist groups has fundamentally changed. Furthermore, (Copeland, 2001)(Crenshaw,2003) have discussed that even in old terrorism, there was not always a clear centralized organization, meaning that they had experienced fragmentation within their originations, similar to some terrorist organizations today operate independently of one another. The leading school of thought being offered by these scholars had been to show that no clear established difference can act as a distinguishing factor between terrorism as new vs. old terrorism, given that both sections have and continue to exhibit similar traits such as organization, violence, and having political motivations behind them.

As terrorism has continued to evolve, given changes in organization and attacks, the recent decade has also seen a considerable shift in CT among democratic states. Such changes could be seen through (Kurtulus, 2012) (Satana & Demirel-Pegg, T. 2020), in which different case studies of the US and Israel and the US and Turkey in CT are examined. Focusing on the new approaches taken in CT, such as partial religious bases, normalization of extra-judicial means through various means, and the increased practice of new, more lethal measures being taken by CT agencies that had been increasing civilian casualties. It is seen that (Kurtulus, 2012) discusses that the main reason behind an increase in lethal measures had been due to the hardening of traditional counterterrorism targets in combination with the increased usage of non-precision guided weapons, along with the issues over inadequate reliable intelligence sources. Other scholars such as (Entelis, J. P. 2005) have argued that many democratic states have been faced with having conducted a balancing act in their approaches towards CT to avoid adopting a more authoritarian position. Following the years post the September 11th, 2001 terrorist attacks, the CT strategy has changed dramatically. It has now resulted in an informal CT framework

utilizing private means to hold and interrogate suspected terrorists in a different framework from the normal state functions. This process has been made possible through the outsourcing of the roles of security to private organizations or overseas detention centers. Many previously mentioned scholars, such as (Kurtulus, 2012), note that such studies that examine terrorism and CT should be conducted together rather than separately.

The rise of domestic extremists within the US has raised the question of what has been the driving causes behind the radicalization of individuals among the far right on the political spectrum. As scholars such as (Frelich, 2009) (Adams, Roscigno 2005) (Piazza, 2017) have attempted to determine the different possibilities in driving factors, it can be agreed mainly that no one factor on its own appears to be a reliable driving cause. A recent case study by (Frelich, 2009) of possible factors behind the radicalization of individuals on the far right, had explored the organizational and recruitment changes that have been seen to have resulted in a much increase in higher recruitment numbers of individuals into these domestic right-wing terrorist organizations. Each of the different variables examined (Frelich, 2009) had centered mainly on the criminal and non-criminal involvement of these organizations, the various financial factors, and the overall political goals of each organization. What had been found was that there needed to have been more efforts towards offering law enforcement agencies a more comprehensive range of different kinds of policy implementations to deter these types of domestic right-wing terrorist organizations. While at the same time not focusing on any one factor in particular. The main focus from past scholars such as (Frelich, 2009) (Adams, Roscigno, 2005) (Piazza, 2017) has been focused on attempting to determine the driving factors that push individuals into radicalization. Factors such as wealth or social standing and others like it on their own had no significant impact in accurately determining if individuals would become more likely to become recruited into joining these types of domestic extremist terrorist organizations or become more willing to participate in acts of terrorism. Instead, it has been widely seen that there must be a more robust offering of various means towards effectively countering these types of domestic extremist terrorist organizations.

As there has been an increase in interactions among terrorist organizations online in an attempt to increase recruitment levels, there has also been a rising presence of online CT measures being taken (Enders, W., & Su, X. 2007). In the aftermath of the September 11th attacks, the US CT policy has taken on a more proactive position than responsive by having enacted the Patriot Act, which appeared to show a massive response towards law enforcement's approaches to CT online. Previous scholars such as (Jensen, T 2011) (Rehman, Nasir, Shahbaz 2017) (Bakali, 2019) have discussed the relationships between the online interactions of terrorist organizations and law enforcement agencies. In particular (Jensen, T 2011), a dynamic model of this relationship between the online interactions of terrorist organizations and law enforcement agencies, had highlighted how the optimal approaches towards CT given the consequence of an increased likelihood of higher recruitment rates among terrorist organizations. Having explained that given the increase of a CT presence, which has been seen to force many terrorist organizations to become more decentralized in their organization into smaller cells independent of one another. This, in turn, then leads to an increased likelihood of more minor scaled attacks taking place rather than more significant scaled attacks. As a result, this increases the probability of more minor scaled attacks being successful, creating a new cycle that would lead to higher recruitment levels. Ultimately (Jensen, T 2011) concludes that in the long term, the effects of increased recruitment levels among terrorist leads to increased CT, which deters large-scale attacks while at the same time increasing successful small-scale attacks leading to again more recruitment. The central relevance of these past scholars is that it helps to understand some of the unintended effects that have been seen as the result of CT approaches. It shows the effectiveness of increased CT presence while also showing some possible flaws when attempting to prevent small-scale attacks

and future recruitment rates.

The online presence of terrorists has taken a much more significant presence in recent years; however, how it is utilized has not been given as much attention for its possible dangers as the following section addresses. Research by (Argomaniz, J. 2015) examines the European Union's (EU's) CT response to terrorism operations online. Their findings showed that the EU's attempt to address the increase of online usage by terrorists had increased their communication infrastructure to prevent cyber attacks. Similar research in this field (Zimmermann, 2006) (Bendiek, 2006) (Routledge, Taylor, and Francis, 2006) has also stressed the importance of understanding the importance of increased CT activities online by state actors. Past studies such as (Argomaniz, J. 2015) have described how much of the effort made by the EU in regards to CT online has been drawn by the utilization of terrorist organizations' ability to raise funds online, communicate, and recruit and organization attacks online. While at the same time, the overall responses by state actors have overlooked this type of exploitation by terrorist organizations online and instead have shifted its main concerns towards having increased cyber defenses in place. This has highlighted how a result of the focus is on deterring cyber-attacks by terrorist organizations rather than distributing more resources towards what has been seen as being the other types of online usage by terrorists while on the internet. This has caused a far lesser amount of attention to be brought towards being able to address the issue effectively. Yet, at the same time, this has been highlighting the importance of such policies already in use that has been meant to deter online radicalization but have not accounted for the privacy rights of internet users.

With there having been much constant advancement in technologies and its easy, widespread, and affordable usage by many at an unprecedented scale, it has raised new questions on the effectiveness of new measures towards online CT programs. The increased technological uses such as social media have led to this becoming a new tool by both terrorist and counterterrorist agencies (Awan, 2017). The primary focus of these researchers has been to determine the viability of implementing an online focus CT radicalization program, such as (Aistrope, T. 2016) examining the state-run social media accounts to counter the increased presence of online activity by the terrorist organization previously AQ-Iraq, now more commonly known as ISIS. While the data analyzed had come from reviewing similar US Department of State (DOS) run programs that had been run throughout the previous decade. The findings revealed multiple shortcomings in the programs, which would have to be addressed to consider this method of counter-radicalization viable. Furthermore, a key focus had been on identifying the different shortcomings of how the government's credibility, especially in CT programs, can become quickly undermined when the same government's actions in foreign policy practices utilize practices that go against the interest of a state's CT policies.

When looking at the relation between technology and strategy in how terrorists have in the past used advancements in technology to increase their own goals and strategy, this relation has shown the changes in recent years. Previous research (Cornish, 2010) discussed how this relationship between technology and strategy has shifted, using the recent 2005 terrorist attacks in London and the response by the United Kingdom (UK) government—explaining how following the 2005 London attacks, the UK had adopted a national CT policy that utilized outdated assumptions from the relation between technology and strategy. This has resulted from having seen the main threat of terrorist attacks as coming from Chemical, Biological, Radiological, and Nuclear (CBRN) weapons (Mahan, 2013). What is seen through (Cornish, 2010) is that terrorists now utilize technology as a means to an end, not focusing on the sophistication of the technology. Instead, the main focus has shifted towards its effectiveness in carrying out their strategy as a whole. Discussing that while the UK has invested heavily into their CT strategy regarding spending and technological developments. The terrorist organizations that have been carrying out the

attacks may at times start to perceive a false sense of victory with each new attack if this relationship between technology and strategy is not effectively implemented. Lastly, it highlights that as the UK and other countries like it continue to develop and implement new advancements in technology in their CT strategies, it will not end terrorism; however, it would significantly increase the cost of terrorist activities making each attack less and less likelihood of being successful.

In an attempt to fill in the past gaps in CT literature, some scholars have conducted a game-theoretical model to determine the likelihood of a CT agency adopting new technological advances when being placed against an attacker. What is described by (Hunt, 2022) discusses the use of a binary choice defender representing a CT agency against a continuous choice attacker to determine the likelihood that a CT agency represented by the binary choice defender would decide to invest more heavily towards an increased level of effective technology in order to deter a terrorist attack represented by the continuous choice attacker. This case had also found that when taking into account the different risk attitudes of both the defender and the attacker, it showed that when the defender is taking on a more risk-averse position. It leads to no new adoption of technology, but in the cases in which the attacker is risk-averse, this leads to the defender adopting new technology, which then tends to be highly effective in deterring attacks. The research contributes to the field had been to help provide information for decisions making for when CT should adopt new technologies when provided with complete details. Some limitations that are addressed here are that other versions of this model would be needed to handle situations that lack complete information along with that much of the actual data on counterterrorism strategies' effectiveness has remained classified.

There has been an increased amount of research that has pointed toward reevaluating the means of CT policy. Research such as (De Lint, & Kassa, W. 2015) (Mueller, J., & Stewart, M. G. 2014) has suggested a change in the means of measuring CT policy as its overall ability to bring a more substantial level of unity and cooperation among the international system as a whole. Rather than measuring the effectiveness of preventing the attacks themselves, given the inability to accurately determine and calculate the prevention of attacks. (Van Dongen, 2011) (McCulloch & Pickering, S. 2009) It is seen that this suggests a more substantial focus be placed on ensuring that government organizations, both domestically and internationally, increase their focus on providing continued intelligence-sharing and improving the already existing international CT frameworks

The effectiveness of CT agencies moving towards increased technological deterrence can be seen as a possible solution towards deterring increased terrorist activities but still raises various issues and gaps that would have to be addressed before it could be seen as a practical approach. While some raise the concerns over intelligence gathering having become invasive and ineffective strategies in the ways CT programs have been carried out, there have been compelling examples of possible solutions towards minimizing the threat of terrorism and their ability to effectively use technology toward larger-scale attacks. In conclusion, it is seen that much of the current literature has focused heavily on addressing the different aspects surrounding terrorism and CT, with very few looking into how CT agencies have been impacted in their effectiveness when attempting to deter attacks.

METHODOLOGY

This thesis is meant to examine the current evolving threat landscape of the 21st Century in the USA as the result of increased right-wing extremism. The significance behind exploring the USA and the domestic terrorist groups and individuals that have been seen to be operating at an increasing scale. Had been centered around the unique challenges that the US faces, unlike many other western or democratic states, when attempting to deter domestic extremists. First is the constitutional protections that are in place in addition to the limitations of the federal government to conduct investigations until recently while also reviewing some of the potential invasive overreaches in surveillance. Secondly, given the significant role the US has played on

the international stage as a critical player in CT against many Foreign Terrorist Organizations (FTOs) while simultaneously appearing to be taking a much different approach towards being able to address the recent rise of domestic right-wing extremist. This then highlights how often it has been seen that the US has taken very tough approaches towards those that have been found to support ideologies linked to FTOs. While at the same time, seemingly unable to recognize the overlapping shared ideologies among domestic right-wing extremist ideologies in connection to foreign right-wing extremist ideologies. This has been seen that the US has been taking a much less aggressive approach in officially labeling domestic extremist groups as FTOs.

The US, while having experienced a number of both successes and failures throughout the 21st Century in the field of CT, has provided many other unique cases to examine. This is significant given that it offers a unique perspective into the known terrorist attacks that have been able to be carried out and also prevented in regards to seeing the possibility of different types of CT approaches by law enforcement to be taken. Given this, when attempting to determine the overall effectiveness of the US's ability to be able to actively identify, detect, and neutralize these growing threats, different kinds of REMVE actors are examined. This provides a deeper level of understanding of the US approaches to these types of terrorist networks in contrast to the same effective response as seen when attempting to deter other forms of terrorist attacks and organizations by FTOs.

In order to develop an understanding of the current threat landscape being posed by the increased number of REMVE actors against the USA, an analysis must be made focusing on the different aspects that have contributed to the spread of REMVE attacks in addition to some of the restrictions in place that have prevented the US from being able to effectively deter attacks from being carried out by REMVE actors. The analysis of individual REMVE terrorists and their connecting organizations has been meant to help identify critical points and trends that can be seen as being instrumental towards the spread of REMVE attacks being carried out domestically. Exploring the potential dangers that different types of REMVE actors have posed to the national security of the US due to their unique ability to communicate and assemble quickly. The importance of reviewing and examining the threats presented by REMVE actors is that in today's current polarized political climate within the US.

There has been a dramatic shift of the existing political parties amongst the right side, as there appears to have been a growing acceptance of radical ideology. These extremist views and trends have shown a new wave of radicalization that has become mainstream in its support and popularity among those on the right that have appeared to grow a new level of tolerance for an increased amount of political violence as a means to advance their political ideology. These types of disconnects from reality and the patterns of extremist ideologies by REMVE actors have not been anything new; these types of extremist ideologies and rhetoric have a long seeded history of violence across much of human history. Much of what appears REMVE actors has been rooted in similar ideologies of Ethnonationalism, believing that those who seem to not fit within the same ethnic in-group as you are then seen as an out-group or threat. As had been seen throughout the recent presidential elections, many of those that have become radicalized and have adopted extremist ideologies amongst the far-right have appeared to be emboldened and undeterred in taking on a more public stance in society rather than remaining along the fringes of society.

In addition, to finding potential shortcomings in the already existing CT frameworks in the US towards addressing domestic extremist actors and groups. Recognizing at the same time that this study is primarily limited in its ability to comprehensively analyze the trends of attacks, potential attacks, and the impacts they would have had, given that much of the information regarding terrorist attacks that have been prevented is still heavily classified by the US government for a number of national security concerns. Additionally, there are no current

existing databases of attacks that have been prevented, only attacks that have been carried out, and even then, the information becomes limited given the lack of information publicly accessible.

This thesis consists of a case study of the US responses to the recent increase in terrorist attacks. At the same time, taking into account a number of factors such as the legal restrictions of domestic CT approaches. In addition to reviewing the ideology components behind the radicalization of REMVE actors through a group-level analysis of different types of REMVE actors and their connections.

ANALYSIS

In order to understand the reality of the threat presented by REMVE actors and the ability of the US to implement effective measures of CT, it is crucial to focus on the historical concepts of the role of ideology and terrorism. The US, when approaching CT, concentrated on the connections behind the motivations of terrorist acts. One of these motivations for political violence is rooted deeply within extremist ideological ideas shared among the different individual actors involved in extremist groups. Foreign radical ideology has been a critical component in how the US government has chosen to categorize individuals and organizations as Foreign Terrorist Organizations (FTOs). This has been seen in a number of ways, first through the ways in which American citizens such as Jose Padilla, The San Bernardino Shooters, and The Boston Bombers have become radicalized by extremist groups such as Al Qaeda (AQ) or AQ Iraq later known as ISIS. Each of these cases is in which an American is caught either in the process of supporting through contributions or having taken part in an attack directly in an attack associated with an FTO or having been caught in the process of attempting to carry out an attack. During each of these incidents, either prior to an attack or in the aftermath that followed, both the federal and state agencies of law enforcement had conducted large-scale investigations and surveillance in order to determine the extent of the potential attack or to reveal any other potential coconspirators.

However, this appears to not always be the case however when approaching far-right ideology, with specific regard to prior surveillance of suspected terrorist individuals and their associates. Given that the US has not labeled many right-wing REMVE actors as being part of FTOs, this presents new challenges in preventing attacks. What is important to identify is that there appears to be a significant difference in the at the same time, one of the main ideologies that many of the growing right-winged REMVE actors have adopted, known as "The Great Replacement," is also a foreign ideology that was first established by the twentieth-century French nationalist author Maurice Barres. This ideology would become more widespread among REMVE actors under the recent French writer Renaud Camus who in 2011 had published the essay "The Great Replacement."

It is seen that many types of US-based REMVE actors are interconnected through these shared ideological beliefs. REMOVE groups such as the Proud Boys, the Attomwaffen Division, also known as the National Socialist Order, The Base, The III percenters, and the Rise Above Movement, also known as RAM; in addition, many others have each adopted ideologies rooted back to The Great Replacement. This also highlights how many of these REMVE groups share active networking and ideological ideas with other foreign-based REMVE groups, such as the Ukrainian-based Azov Battalion, Swedish-based Nordic Resistance Movement, and the UK-based Combat 18 extremist group, which most recently has been linked to the assassination of a German politician in recent years. Each of these groups, through their shared ideology, has found common ground with one another, creating a new threat that they pose not just within the US but also within the international system, given the potential dangers they pose. This radical ideology had been pushing the notions of the white race facing an external threat of replacement by different groups that have been viewed as outsiders consisting of immigrants and other types of minority groups. This is similar to the concepts found throughout many types of ethnic conflicts known as Ethnonationalism.

When attempting to establish effective means of CT activities and frameworks to be able to target domestic terrorist organizational networks and cells, a considerable challenge is raised. This challenge is the "rule of law." In the US, the constitution prevents the government from being able to easily and quickly label REMVE groups and actors as being FTOs, unlike how in other western nations, such as Canada or The UK, that isn't limited in the same ways. These western nations, following the recent increase in violence by REMVE actors associated with larger groups, have labeled US-based REMVE groups such as the Proud Boys, Atomwaffen, and the Base as being FTOs. In addition to this, the US constitution allows for these domestic extremist groups the ability and the freedoms to openly assemble and protest; however, again, during recent years, these groups have taken even more increasingly radical positions, with many armed while entering into different state capitol buildings across the US in addition to the US. Capital riots on January 6th, 2021.

In 1996, the US Congress, in response to major domestic bombing attacks during the 1990s, specifically the 1993 World Trade Center bombing and the 1995 Oklahoma City bombing (Mahan 2013, Pillar 2001), introduced new legislation known as The antiterrorism and Effective Death Penalty Act of 1996. This legislation had made it possible for specific acts of terrorism to be charged as federal crimes giving the federal government agencies a more comprehensive range of operations, with the possibility of the death penalty. This has, in turn, provided law enforcement agencies at the federal level with the ability to no longer be restricted by the statute of limitations. In addition, this would allow the US government to establish two significant CT policies. The first primary CT policy had been the ability to provide the US Secretary of State to establish a formal list of FTOs.

The ability to designate different groups as FTOs allows the second major policy. Second, it gave the US government the power to freeze and block the financial assets of anyone involved with FTOs. This allows for a much more effective means of disrupting the finances of terrorist organizations that have been listed as being an FTO. Those that may be in opposition to the labeling of certain REMVE actors and their organizations as being FTOs might also take the position that many left-wing groups, such as Black Lives Matter, also known as BLM, would also be required to be listed as FTO. The critical aspect, however, when listing groups as an FTO or a terrorist in general, refers back to fitting the current definitions of terrorism. The central element is proving the component of violence as a means of advancing a political goal.

Taking a look back at some of the US CT policy's in the past, many of them had been designed in response to fighting a new type of enemy in the aftermath of the September 11th, 2001 attacks on the US (Gottlieb, 2014) had shifted toward giving more power towards the executive branch in terms of heading the nation's war on terrorism. The official establishment of the DHS by the US Congress in 2005 had now given a nearly precedent amount of power under the executive branch. New types of changes to existing legislation now allowed for a broader range of government oversight in its ability to collect intelligence through surveillance. Such as the use of the Foreign Intelligence Surveillance Act (FISA) of 1978, now being used by the IC to issue FISA warrants through closed courts in order to conduct electronic monitoring of potential threats.

This would be most seen through the National Security Agency (NSA) under the directive of the US President through the use of executive orders to expand the NSA surveillance effort in coordination with the Patriot Act also passed by Congress. This massive expansion of the IC's ability to conduct surveillance had now allowed much of what had been previously considered off-limits as the result of the US constitution and other domestic laws to now be circumvented in the interest of national security. While the usage of presidential executive orders has not been a new concept when it has come to engaging in expanded acts of surveillance without other types of surveillance, it is seen that this latest expansion of the IC would become a massive invasion of privacy for everyday Americans as a violation

of the US Constitution. It is important to also note that the US has officially stopped these types of practices domestically; as the result of a later whistleblower, the usage of the executive orders has been seen to be a crucial part of many aspects of the current counterterrorism policies in the US.

While the Patriot Act had been in use, originally being passed in 2001 (Mahan, Griset 2013), it has consisted of a number of different types of provisions ranging in scale from extended types of wiretaps such as roving and sneak and peak style wiretaps meant to increase the amount of surveillance possible by law enforcement agencies. It also expanded the types of warrants that would now be made possible for use by the different members of the IC Additionally; the Patriot Act would allow for new existing wiretaps to be used for a much longer amount of time before becoming expired. Through the use of the Sunset provision, it would allow for each wiretap to be in use for a maximum of four years before ever having to be removed from whichever locations it had been in use for surveillance previously.

While the abilities of the different member of the IC had been expanded for a much easier and more extensive surveillance effort, there was also much more harsh criminal punishments attached to the act. The patriot act would now allow for increased sentencing laws for those suspected of having committed acts of terrorism; in addition, this would also be expanded towards anyone who had played a role in supporting these acts. The increase in criminal punishment, however, would play a minimal role in actually preventing acts of terror from occurring. Given that for a majority of REMVE actors who do not meet the current qualifications to be charged as a domestic terrorists, there is little to show that increased criminal charges would have an effect.

The 21st Century has brought many advancements to society, an essential aspect of which has been globalization and the increased advances in technology. The media has evolved over time, it has become much more accessible for individuals to not only have more manageable and more convenient access to a nearly infinite number of media sources, but also more and more individuals have become able to publish their own materials through social media platforms. There has also been an upward trend of increasing information and other forms of media that have been more based on gaining a larger audience. In contrast to media in the past that had been focused on providing accurate and reliable sources of information, today, it has been seen to be pushing away many from more credible sources of news media. Currently, with nearly every event being documented in one way or another, both domestic and foreign terrorist organizations have been able to convey their ideology through a variety of means, such as through the media (Wolfowicz, 2021). "Occasionally, exposure to these messages and their associated images may serve to attract new supporters and recruits, which is one of the main objectives of terrorists' use of the media," leaving many in the media networks with the dilemma of how much coverage of a terrorist attack to cover.

It has been seen that by covering the different kinds of extremist attacks that, the media are doing their jobs of keeping the public informed; however, there have been clear instances in which terrorists want the media to intentionally spread their manifestos and their reasons behind each attack such was the case of the Unabomber who had wanted his manifesto published in the media in exchange for a stop to the bombings. However, with the increased presence of internet-based social media platforms, the challenge becomes even more difficult. More recently, in 2019, the El Paso Shooter, twenty-one-year-old Patrick Wood Crusius, had written a manifesto consisting of anti-immigrant and anti-Hispanic views while also expressing his own white nationalist ideology. Prior to carrying out this attack, Crusius had published this manifesto online on a website known as 8chan, which was quickly picked up following the attack by media sources, law enforcement, and other REMVE actors. The ability to be able to upload their manifestos and ideology online has only strengthened their outreach; because of this, it is much easier for their network and following to grow more rapidly in far less amount of time. The media is always trying to do a balancing act

between the competing interests of three groups (Mahan, 2013). "These three interest groups—(1) journalists, (2) government authorities, and (3) terrorists—are competing for the attention and acceptance of the public." with each group having their own vested interest in getting the coverage that suits them the best. At the same time, while terrorists have been able to benefit from the increase of coverage by different aspects of the media, the utilization of the media available at a given time by terrorists is not new at all.

Terrorists have found ways to use each tool they had available to them to their advantage throughout most of history, (Wolfowicz, 2021)." Already in ancient times, terrorist groups leveraged media to promote their cause, first through graffiti, coins, and posters, and later with the advent of the printing press, which they leveraged to distribute propaganda and recruitment materials through pamphlets and literature" given that while modern-day media has been more readily available and widespread in being able to reach more people at a given time. Another central part of modern-day technology that has raised many concerns over its use by terrorists has been the internet. It is noted that terrorists have been able to utilize the internet in a nearly unprecedented way (Mahan, 2013). "Terrorists also use it to contact other terrorist cells and networks, both domestic and transnational connections, tap new sources of financial support, and plan attacks. They use the internet to conduct debates and settle disputes." The new easy access to an infinite number of ways to be in contact with one another, plan and coordinate attacks, and have access to finical funds has made the usage of the internet by terrorists more widespread.

Perfected initially by members of ISIS in their ability to utilize the internet for their own gains in networking and recruiting, a new trend can be seen in right-wing extremists adopting these same practices. It could be seen that many extremists use online chat rooms and encrypted servers to be able to communicate with each other online and spread more radical materials. Taking a look at the recent Charlottesville riot in the US in 2017 during the Unit the Right Rally, the coverage it had received (Rowley, 2018), journalists would discover a series of right-wing and neo-Nazi white supremacists that would be connected through online chat servers such as Discord and other online blogs in which communication and coordination of these groups could be seen networking with other white power groups that had been attending other white pride riots across the US during this time.

The Unit the Right Movement would be seen as a pivotal moment among many right-winged domestic terrorists; witnessing the lack of political backlash and rather a growing acceptance of those who support these types of radical ideologies, many of these groups would become emboldened. Additionally, a recent US-based neo-Nazi domestic terror group known as Atomwaffen Division, founded in 2015 by Adam Russel, a US national guardsman (Rowley, 2018), had been found to have many connections to multiple individuals that have taken part in acts of violence. Most notably, it is seen that the result of a multiple double homicides by Devons Arthur in 2017 while living with members of the Atomwaffen Division had brought an increased level of attention to the group as a whole (Rowley, 2018). This incident had led to law enforcement eventually finding massive amounts of evidence of online communications, weapons, explosives, and Nazi material, in addition to other extremist material. Later on, it would be seen that Russel, along with another member of the Atomwaffen Division, would be arrested following an Federal Bureau of Investigation (FBI) warrant for his arrest. His arrest would raise concerns over the potential attack that was prevented, given the types of weaponry and explosives found at the time of the arrest and their location being close to a nuclear power plant. However, the group as a whole would go on to have its members commit a number of other violent crimes motivated by their radical ideology.

Terrorist groups such as Attomwaffen Division have been seen to utilize the internet in different ways that best suit their own group's interest. The instance is that (Jacobson, 2010) had shown a pattern of a number of FTOs utilizing

the internet in a variety of ways to circumvent established frameworks of CT through the amenity of the internet. The use of the internet by a terrorist has been seen to target (Nations, 2012) " The Internet may be used not only as a means to publish extremist rhetoric and videos, but also a way to develop relationships with, and solicit support from, those most responsive to targeted propaganda." Those who are most responsive in society are who are most vulnerable or susceptible to the material being spread. The most significant usage of recruitment by terrorist groups online has been by ISIS; they have outmatched nearly all other terrorist groups through their online social media presence. In addition, it appears that many Americans who have become radicalized to join right-winged extremist groups have been the result of online interactions with extremist material.

The online campaign by terrorist groups online has been seen to have had an increase in recruitment, in particular within the groups of society that have been marginalized by society. Given that many terrorist networks today no longer operate with a clear command structure and instead operate in isolated cells or entirely on their own, there has been a drop in the more sophisticated coordinated attacks, yet there has still been a large number of unsophisticated random attacks that have been able to have significant impacts. With much of the extremist propaganda spread by terrorists still being able to be found online along with guides and instruction's on how to make homemade weapons and explosives, or the published manifestos, it has made the ability for those who become radicalized or inspired at home to carry out attacks on their own without the need for extensive training and travel. Past examples of those that have attempted to or have carried out attacks as the result of being influenced by online material have been the Pittsburgh synagogue shooter and the El Paso shooter. Another example would be Dylan Roof (Berman, 2021), who had been entirely self-radicalized online prior to committing a mass shooting against civilians who had been attending a historically African American church. Other shooters like this had taken inspiration from previous attackers creating a cycle of each attack, inspiring the next attacker, following information of the attack being available online.

At the same time, it is essential to understand the potential for REMVE actors to carry out attacks through other types of weapons, such as nuclear and biological weapons. While the likelihood of REMVE actors on their own being able to carry out attacks using these types of sophisticated weaponry is due to it requiring even more resources to obtain and develop the materials needed, along with extensive training that most terrorist groups and radicalized individuals do not have. In addition, most of these kinds of materials needed or the weapons themselves are oftentimes well regulated and heavily controlled, with some notable exceptions. Such as in the immediate aftermath of the Cold War in the Soviet Union and other third world countries that have access to nuclear materials in which, the existing regulations in these regions became difficult to fully monitor. This is not to say that the US does not also have the threat of terrorists taking advantage of the nuclear waste in the US (Mahan, 2013). "Nuclear waste and radioactive waste, including waste emanating from electric power generated at commercial nuclear plants and fissile materials at defense facilities, may take centuries to decay, posing major problems of waste disposal" the long life spans of these materials make it vastly challenging to store and transport them in secure areas for long periods of times.

At the same time, even with the threat of storing and transporting these kinds of materials, there have been very few examples of non-state actors have been able to capture or attack these materials in transit or storage. While also being aware of the threat of a terrorist obtaining nuclear materials is still possible as (Gottlieb, 2014) states, "No government or international organization has comprehensive knowledge of where all the nuclear stockpiles in the world are, what security measures are present at each location, and what kinds of threats target each site." With there being no universal set of regulations or oversight of nuclear materials around the world, it makes it a problematic effort to ensure that terrorists

do not obtain such materials. The threat that REMVE actors may pose in regards to being able to carry out attacks at such a large scale involving these types of weapons can be seen as being less likely. Given that much of the materials that are used in the development of these kinds of weapons are being easily traceable to the country of origin, it becomes even less likely to have state or rouge state actors sell these kinds of materials and weapons to non-state actors such as domestic terrorist group or individual REMVE actor given that should these weapons be used by a terrorist in any type of attack, it would be easy to identify the state actors that had supplied the weapons involved. Another means of high-tech attacks that have become apparent as the result of globalization is the possibility of cyber attacks by hackers (Mahan, 2013). "Although the threat is real, there have been no significant cyber attacks by terrorists on US government information systems, transportation systems, power grids, nuclear power plants, or other key infrastructure...Cyber attacks are common, but...primarily been conducted by non-terrorist hackers." As stated here, the number of possible targets for cyber attacks is vast, yet many of the known cyber attacks that have occurred have not been due to terrorism but instead have been by criminal hackers or even state hackers in some cases.

This is again key to understanding the US CT approaches, as with many resources being diverted into preventing large-scale cyber-attacks, there has been a much less significant effort in being able to monitor or prevent the online communications among domestic REMVE actors and groups between each other and in coordination with other foreign REMVE actors and groups. The majority of cyber attacks in these cases have frequently been more of harassment or espionage and have not been actual attacks on physical targets, an instance of hacking that took place by criminal hackers had been on the colonial pipeline, (Tom, 2021)" The hackers did not take control of the pipeline's operations, but Colonial shut it down to contain the damage." In this case, it was seen that criminal hackers who had targeted the pipeline had not intended to cause physical harm but instead had wanted an extortion payment. All of the ways mentioned above show possible high-tech methods of attack that are possible by terrorist organizations or individuals lone wolf style attackers and at the same time have demonstrated the likelihood that each kind of method has occurred, in contrast to the possible more widely available low tech methods of attacks.

Other kinds of weapons, such as explosives, have become common in low-tech attacks due to many of the terrorist sites that provide the guides to construct explosives can be found online and easily copied using materials found in stores and homes. Many of the bombers who have attempted to make their own homemade bombs have failed to detonate their explosives due to having made the bombs wrong or simply getting caught prior to setting off the attack, such as the Attomwaffen Division founder being caught with multiple homemade bombs and explosives, or times square bomber and others. The threat that these kinds of attackers create is still there, given how easy technology has made access to it. The use of low-tech attacks using technologies that have become widely available is seen to be much more common among terrorists today, especially among REMVE actors who oftentimes are limited in the types of materials and weapons they may have access to. Domestic extremists such as REMVE actors, in addition to FTOs, have been widely seen to no longer operate in set command structures such as the terrorist organizations throughout the second half of the 21st Century; this shows the increased dangers in a decentralized threat that operates within smaller groups often not coordinating with others.

CONCLUSION

The 2017 Charlottesville car-ramming, just to name one - these attacks had shown that domestic extremists who may lack the means to carry out more technologically sophisticated attacks are still able to carry out attacks by simply using a large vehicle against a crowd of people. As these attacks have become much more apparent against soft targets such as civilians, it has been seen that the US CT policies have

been at times effective in preventing larger-scale attacks by REMVE actors such as against Hard Targets, but there still appears to be a lack in the ability to protect civilians from REMVE actors. The rise of REMVE actors across the US has presented a significant national security threat to the US as it involves a variety of different aspects in being able to find solutions towards effectively deterring these types of attacks.

When reviewing some of the past existing CT approaches that have been taken by the US, it is seen that in response to the large-scale attacks of September 11th, 2001. The US had taken a massive and, in some cases, oversteps in their war against terrorism; while the usage of domestic surveillance had gone up exponentially, there had been little to suggest that these types of government surveillance had been effective in being able to deter acts of terror. While the use of the Patriot Act had been mainly meant to prevent acts of terrorism by FTOs, it also showed that in terms of also preventing domestic acts of terrorism by domestic extremists, it would have an even lesser impact. The results of the US government's approaches to preventing terrorism, however, can not be fully measured still, given that it is not currently possible to have an accurate assessment of how many domestic terrorist threats and attacks have been successfully prevented as the result of much of the presently existing data not being made available to the public. It is also worth noting that for many REMVE actors that have been successfully prevented from carrying out their attacks, it has been, in often cases, the result of the REMVE actor themselves bringing attention to their own operations.

This is not to suggest any faults of the existing CT policy, as there have been a number of potential attacks by REMVE actors that have been known to have been prevented. Additionally, there must be a realization that given the current changing threat environment that the US is facing as a result of the increased levels of domestic right-wing terrorism, there is a need for increased CT policies. There should be a broader push towards having an increased online CT approach; while increased surveillance has been seen to not always be the answer, attempts should be made to counter the massive amounts of extremist propaganda and disinformation that has been found online. While also being able to find ways of increased deradicalization programs created by the government in order to prevent an increased number of REMVE actors. In regards to CT, there have been many cases in which intelligence groups such as the FBI and the Central Intelligence Agency (CIA) have been able to prevent the spread of terrorist attacks or terrorists obtaining weapons of mass destruction. The FBI has prevented a handful of domestic terror attacks by militia groups, such as the preventing the attacks on police by the militia groups known as the arm the sword and the covenant, along with other attempts to incite violence during the previous 2020 US presidential elections. Such as the attempts made by right-wing militia groups attempting to kidnap and hold hostage state governors as a result of the previous US elections in 2020. In all, however, CT also runs into issues of being able to fully monitor the online activities of extremists given the legal limitations of surveillance along with the increasing encryption of online servers. As has been seen, there has been a dramatic increase in the number of ways that terrorist organizations and radicalized individuals have been able to use the internet, such as through encrypted web-based chat systems, the spreading of their own extremist materials online, the transnational connections, and the ability to conduct financial exchanges online. Finally, when attempting to answer the question of the effects of the US CT policy's ability to effectively prevent REMVE actors from carrying out acts of terrorism, there is no clear answer as to measuring counterterrorism in terms of preventing attacks; instead, it should be calculated on the ability of the US government to increase the existing framework of CT both on the domestic and international stage while ensuring to stay within its own legal framework.

REFERENCES

Adams, J., & Roscigno, V. J. (2005). White Supremacists, Oppositional Culture and the World Wide Web. Social Forces, 84(2), 759–778. https://doiorg.proxy.library.cpp.edu/10.1353/sof.2006.0001

Aistrope, T. (2016). Social media and counterterrorism strategy. Australian Journal of International Affairs, 70(2), 121–138. https://doi- org.proxy.library.cpp.edu/10.1080/10357718.2015.1113230

Argomaniz, J. (2015). European Union responses to terrorist use of the Internet. Cooperation and Conflict, 50(2), 250–268. http://www.jstor.org/stable/45084352

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. Society, 54(2), 138–149. https://doi-org.proxy.library.cpp.edu/10.1007/s12115-017-0114-0

Bakali, N. (2019). Challenging Terrorism as a Form of "Otherness": Exploring the Parallels between Far-right and Muslim Religious Extremism. Islamophobia Studies Journal, 5(1), 99–115. https://doi.org/10.13169/islastudj.5.1.0099

Berman, M. (2021, October 26). Prosecutors say Dylann Roof 'self-radicalized' online, wrote another manifesto in Jail. Retrieved May 3, 2022, from https://www.washingtonpost.com/news/post-nation/wp/2016/08/22/prosecutors-say-accused-charleston-church-gunman-self-radicalized-online/

Cornish, P. (2010). Technology, strategy and counterterrorism. International Affairs, 86(4), 875–888. https://doi-org.proxy.library.cpp.edu/10.1111/j.14682346.2010.00917.x

De Lint, & Kassa, W. (2015). Evaluating U.S. Counterterrorism Policy: Failure, Fraud, or Fruitful Spectacle? Critical Criminology (Richmond, B.C.), 23(3), 349–369.

Entelis, J. P. (2005). The Democratic Imperative vs. the Authoritarian Impulse: The Maghrib State between Transition and Terrorism. Middle East Journal, 59(4), 537–558. http://www.jstor.org/stable/4330183

Jacobson, M. (2010). Terrorist Financing and the Internet. Studies in Conflict & Terrorism, 33(4), 353–363.https://doiorg.proxy.library.cpp.edu/10.1080/10576101003587184

Jensen, T. (2011). Optimal counterterrorism and the recruitment effect of large terrorist attacks: A simple dynamic model. Journal of Theoretical Politics, 23(1), 69–86. https://doi.org/10.1177/0951629810384304

Jensen, T. (2016). National Responses to Transnational Terrorism: Intelligence and Counterterrorism Provision. Journal of Conflict Resolution, 60(3), 530–554. https://doi.org/10.1177/0022002714545221

Frelich, J. D., Chermak, S.M., & Caspi, D. (2009). Critical events in the life trajectories of domestic extremist white supremacist groups: A case study analysis of four violent organizations: Homeland Security and Terrorism. Criminology & Public Policy, 8(3), 497–530.

Gottlieb, S. (2014). Debating terrorism and counterterrorism: Conflicting perspectives on causes, contexts, and responses (Second ed.). Los Angeles: SAGE/CQ Press.

Mahan, S., & Griset, P. L. (2013). Terrorism in perspective (Third ed.). Thousand Oaks: Sage.s

McCulloch, J., & Pickering, S. (2009). Precrime and counterterrorism: Imagining future crime in the war on Terrorr. British Journal of Criminology, 49,628–645

Mueller, J., & Stewart, M. G. (2014). Evaluating counterterrorism spending. Journal of Economic Perspectives, 28(2), 237–248.

PILLAR, P. R. (2001). Terrorism and U.S. Foreign Policy. Brookings Institution Press. http://www.jstor.org/stable/10.7864/j.ctt1gpccnx

Piazza, J. A. (2017). The determinants of domestic right-wing terrorism in the USA: Economic grievance, societal change and political resentment. Conflict Management and Peace Science, 34(1), 52–80. https://doi.org/10.1177/0738894215570429

Rehman, F. U., Nasir, M., & Shahbaz, M. (2017). What have we learned? assessing the effectiveness of counterterrorism strategies in Pakistan. Economic Modelling, 64, 487–495. https://doi.org/10.1016/j.econmod.2017.02.028

Routledge, Taylor and Francis. (2006). Journal of policing, intelligence and counter terrorism.

Rowely, R, (2018) Documenting hate: New American Nazis. Retrieved May 2, 2022, from https://www.pbs.org/wgbh/frontline/film/documenting-hate-new-american-nazis/

Taylor. (2009). Is terrorism a group phenomenon? Aggression and Violent Behavior, 15(2), 121–129. https://doi.org/10.1016/j.avb.2009.09.001

Van Dongen, T. W. (2011). Break it down: An alternative approach to measuring effectiveness in coun-terterrorism. Journal of Applied Security Research, 6, 357–371.

Zhang. (2007). Beyond anti-terrorism: Metaphors as message strategy of post-September-11 U.S. public diplomacy. Public Relations Review, 33(1), 31–39. https://doi.org/10.1016/j.pubrev.2006.11.006