



April 2022

# Preventing Right-Wing Extremist Use of Social Media

Shivapriya Viswanathan

Master of Public Policy Candidate  
Frank Batten School of Leadership  
and Public Policy

Prepared for the United States Department  
of State, Bureau of Counterterrorism

## Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Acknowledgements, Disclaimer &amp; Honor Pledge.....</b>	<b>3</b>
<b>Introduction.....</b>	<b>5</b>
Problem Statement.....	5
Client Overview.....	6
<b>Background.....</b>	<b>7</b>
Impact of the Internet.....	7
Legal and Regulatory Environment.....	7
Comparisons to the Global Community.....	8
Consequences.....	8
<b>Existing Evidence.....</b>	<b>10</b>
Public-Private Partnerships.....	10
Digital Literacy Programs.....	11
Counter-Messaging Campaigns.....	12
<b>Alternatives.....</b>	<b>13</b>
Alternative 1: Takedown Legislation.....	13
Alternative 2: Digital Literacy Programming.....	13
Alternative 3: Counter-Messaging Campaign.....	14
<b>Criteria.....</b>	<b>15</b>
Cost-Effectiveness.....	15
Political Feasibility.....	15
Administrative Feasibility.....	15
Securing Rights.....	15
<b>Evaluation of Alternatives.....</b>	<b>16</b>
Evaluation of Alternative 1.....	16
Evaluation of Alternative 2.....	17
Evaluation of Alternative 3.....	19
<b>Outcomes Matrix.....</b>	<b>21</b>
<b>Recommendation.....</b>	<b>21</b>
<b>Implementation.....</b>	<b>22</b>
<b>Conclusion.....</b>	<b>24</b>
<b>Appendix.....</b>	<b>25</b>
<b>References.....</b>	<b>35</b>

## Acknowledgements

I would like to thank Oliver Wilcox and Irfan Saaed from the United States Department of State (DoS) Bureau of Counterterrorism for guiding me through this process and supporting me in tackling an emerging topic that aligns directly with my research interests. I would also like to thank Michael Darden and the entire RESOLVE Network team at the United States Institute of Peace for kindling my interest in peacebuilding and countering violent extremism. I would also like to thank them for taking the time to provide me with feedback through this process and always believing in my ability to succeed.

I am profoundly thankful to everyone at the Batten School from faculty to peers for equipping me with the skills to conduct policy analysis. I am extremely grateful to my APP advisors Professors James Wyckoff and Craig Volden for their invaluable insight and encouragement throughout this process regardless of how many times I met with them to ask questions or changed my problem statement. I would like to extend a special thanks to Professor Dan Player for being an invaluable support system both within and outside the classroom.

I am also grateful for my friends both within and outside of Batten for cheering me on throughout this process and providing me with constant and unconditional friendship. They ensured I balanced hard work with rest as I worked through this APP.

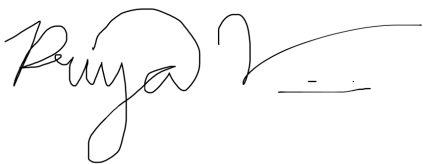
Finally, I would like to thank my parents, Balaji Viswanathan and Anu Krishnamurthy, for always believing in me and providing their unwavering support in all of my endeavors. This APP would not be possible without their love and constant sacrifice for me. I would also like to thank my younger brother Jayanth Viswanathan for being my biggest fan and always being a sounding board when I needed it most.

## Disclaimer

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

## Honor Pledge

On my honor as a student, I have neither given nor received unauthorized aid on this assignment.

A handwritten signature in black ink, appearing to read "Ranya V.", with a long horizontal flourish extending to the right.

## Executive Summary

The rapid growth of right-wing extremism (RWE) within the United States has been exacerbated by the use of large social media platforms. From the loss of life, to GDP impacts, to threats to democracy, RWE's ability to facilitate violence via social media poses a pressing problem to the United States.

This report will first describe the problem in greater detail and provide the necessary background to understand the context, causes, and consequences of RWE's use of social media. It will then include a brief analysis of existing literature that provides evidence to support potential policy alternatives to remedy this issue.

Following this description, the report provides and discusses three potential policy alternatives that the DoS could consider to prevent RWE's use of social media to facilitate violence:

1. Takedown Legislation
2. Digital Literacy Programming
3. Counter-messaging Campaign

These alternatives are then assessed across four criteria: cost-effectiveness, political feasibility, administrative feasibility, and securing rights. After analyzing each alternative based on these four criteria, the report recommends that the DoS implement a joint counter-messaging campaign with members of the Global Counterterrorism Forum as it performs well on both forms of feasibility and does not affect citizens' rights.

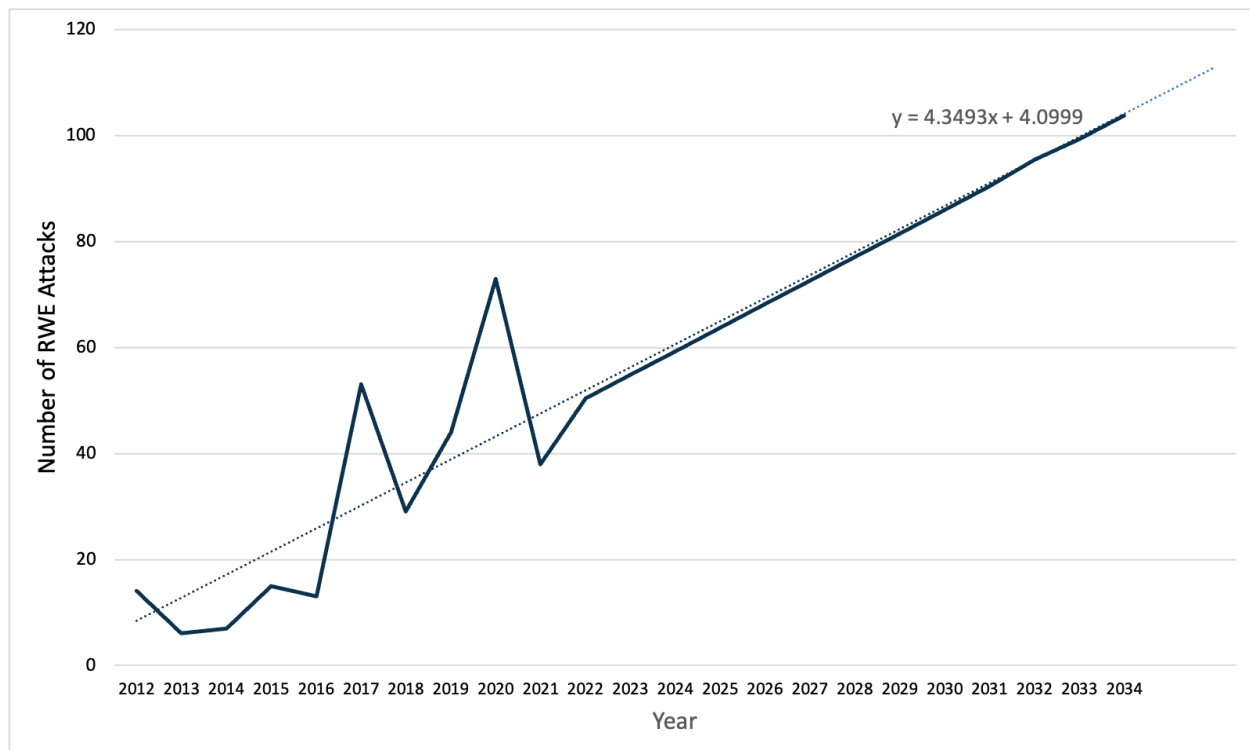
Finally, this report provides recommendations for implementation with a discussion of funding, potential first steps, ideal rollout method, and potential challenges. By implementing a joint counter-messaging campaign, the DoS will be able to prevent citizens' susceptibility to RWE content and misinformation online, thus preventing radicalization and acts of violence by RWEs.

# Introduction

## Problem Statement

***Too many right-wing extremists (RWEs) within the United States are committing acts of terrorism facilitated by large social media platforms.***<sup>1</sup> RWEs' online presence has been associated with numerous terrorist attacks including the January 6<sup>th</sup> insurrection, the August 2019 El Paso Walmart shooting, and the 2017 Charlottesville 'Unite the Right' rally (Conway et al., 2019). Furthermore, the prevalence of these right-wing attacks has grown at a greater rate than religious ones attributed to terrorist attacks like September 11, 2001 (*"The escalating terrorism problem in the United States"*, 2020). Therefore, experts have become increasingly concerned about the ability of social media to create more opportunities for right-wing extremism.

Figure 1. Projected number of RWE Attacks in the United States between 2023 and 2034<sup>2</sup>



Sources: (*"The escalating terrorism problem in the United States"*, 2020; Doxsee et al., 2022).

<sup>1</sup> Large social media platforms are any platforms that have more than 6.5 million registered users in the United States. The number of registered users used as a threshold to define a large social media platform was determined by scaling up the German threshold of 2 million to fit the United States population (*"Germany: Network enforcement act amended"*, 2021).

<sup>2</sup> Calculations for this forecast can be found in Appendix A.

## Client Overview

The United States DoS Bureau of Counterterrorism is responsible for assisting the United States in its efforts to promote national security by developing and implementing strategies to defeat terrorism abroad. Furthermore, they work in tandem with other organizations to also address terrorism within the United States. Since 2014, the Bureau has worked with its NATO counterparts to defeat ISIS through various efforts including military support, prevention, and humanitarian aid (“About us”, n.d.). However, the team is currently severely understaffed in both its racially and ethnically motivated violent extremism program as well as its team dedicated to the intersection of technology and counterterrorism. This project evolved from the Bureau’s need for greater research on the specific issue of RWE radicalization via online platforms due to its lack of resources. Literature has focused on this issue in Europe, particularly Germany, but there has not been much focus on the domestic aspect.

*Figure 2. Mission and Key Topics of U.S. DoS Bureau of Counterterrorism*



Sources: (“About us”, n.d).

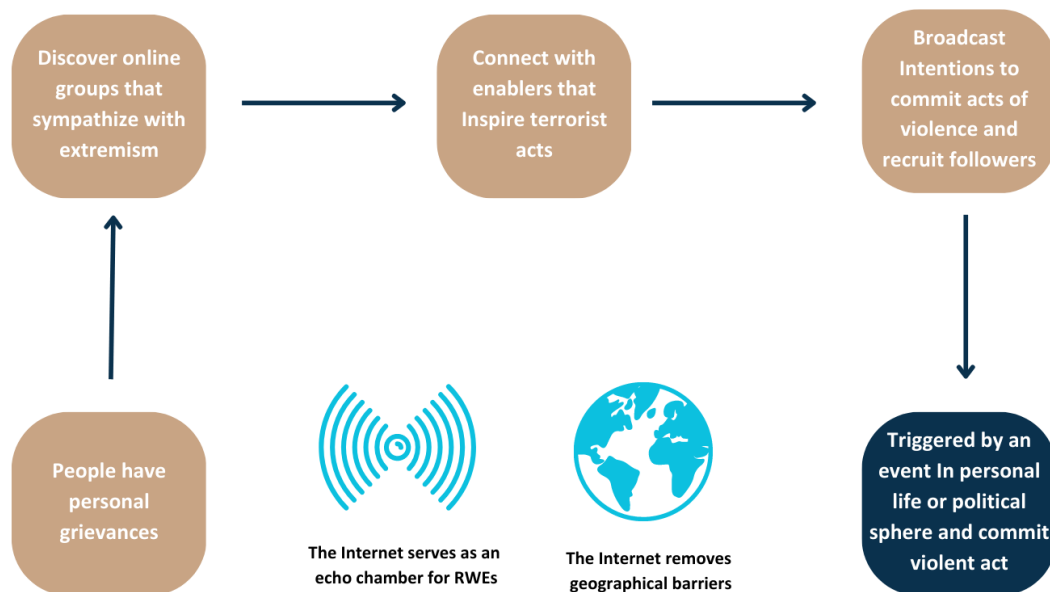
## Background

### Impact of the Internet

Since right-wing extremism's rise, numerous online platforms have been used as a hub for extremist activity. With the development of social media, extremists have been able to use the algorithms to their advantage to reach a wide audience that may have otherwise not been exposed to their content. This includes search engine optimization to get their content to the top of users' search results on Google. Social media platforms are not unfamiliar with extremist groups, and major platforms like Twitter have worked to keep jihadist content away from the masses. However, platforms have been far less effective in moderating RWE accounts which has allowed for the continued radicalization of individuals (Conway et al., 2019).

People are susceptible to radicalization for a wide variety of reasons and experts have developed numerous potential pathways, including traumatic experiences leading to the need to form relationships and address grievances, identity-seeking, material reward due to economic distress, and blatant recruitment (Smith, 2018). Although radicalization may not occur completely online, extremist use of the Internet creates more opportunities for, and accelerates, radicalization. This is because it enables people who may not have been otherwise connected due to a lack of physical contact to engage and formulate plans for potential violence. It also normalizes violent behavior by serving as an 'echo chamber' (von Behr et al., 2013).

Figure 3. Potential Radicalization Pathway via the Internet



Source: (Smith, 2018).

The interconnectedness of the Internet has also enabled extremists in foreign countries to influence Americans. The Department of Homeland Security has stated publicly that foreign actors can use online platforms to spread violent ideology as broadly as they can (*DHS strategic framework* 2019). There has been record of white supremacists traveling to foreign countries to continue to develop their networks,

and with the use of the Internet, it is far easier for them to do so without even leaving their homes (*White Supremacy Extremism* 2019).

## Legal and Regulatory Environment

Though there have been calls to address extremist content, there are many obstacles. One of the biggest regulatory challenges that the DoS and other governmental agencies must navigate is Section 230 of the Communications Decency Act (CDA 230). This section states that websites, such as social media sites, are immune from liability for the content generated by their users (*"The FCC's authority"*, 2020). Because of this, it is hard to convince social media sites to enact stricter mediation laws. The Department of Justice has indicated that it sees four major areas for reform, but so far, these amendments have not been made (*"Department of Justice's review"*, 2021).<sup>3</sup> Additionally, many prominent online sites, such as Telegram, are based in foreign countries, meaning the United States struggles to have jurisdiction over them.

Furthermore, currently, domestic terrorist organizations are not designated the way that foreign terrorist organizations are by the U.S. government which can make it harder to directly target them through legal action (*The rise of far-right extremism in the United States*, 2022).

## Comparisons to the Global Community

Right-wing extremism is not an issue contained to the United States. Europe has also become a victim of rising levels of RWE attacks. For example, in 2011, 77 people died in attacks conducted by RWEs in Oslo and Utoya. Of European Nations, RWE attacks seem to be most concentrated, and effective, in the United Kingdom. Additionally, networks of RWEs have been developed across Europe and this has been made easier through the use of the Internet (*The rise of far-right extremism in the United States* 2022).

---

<sup>3</sup> These areas include: incentivizing online platforms to address illicit content, clarifying federal government enforcement capabilities to address unlawful content, promoting competition, and promoting open discourse and greater transparency.



## Consequences

There are numerous costs associated with RWE attacks, particularly because of radicalization that occurs through active and passive social media use. These can be categorized into short and long-term costs that are both direct and indirect. It should be noted that costs are difficult to estimate for this issue so all numbers calculated are rough calculations.

*Figure 4. Total Costs to Society of RWE Use of Social Media*



In 2021, right-wing extremists were responsible for the deaths of 29 people in the United States (“*New ADL data*”, 2022). According to the Profiles of Individual Radicalization in the United States database, about 52.22% of extremists with successful terror plots included in the database used social media either passively or actively (Safer-Lichtenstein et al., 2018). Therefore, we can assume that social media use can be attributed to 15.14 deaths in 2021, which we can round to 15. Economists generally value the cost of a statistical life at \$10 million (Gonzalez & Malone, 2020). Therefore, the cost of the loss of human life due to right-wing terrorist attacks facilitated by social media in 2021 can be estimated to be around \$150 million.

There is not currently an extensive amount of data on the number of injuries, amount of property damage, and other economic costs that have occurred due to right-wing extremism. However, research suggests that of the total cost of terrorism, death accounts for 58.1%, property destruction accounts for 2.2%, injury accounts for 0.9%, and GDP loss accounts for 38.7% (Bardwell & Iqbal, 2020). Based on the aforementioned \$150 million cost due to death, this suggests that the cost of injury associated with social-media-facilitated RWE attacks was around \$5,700,000, the cost of property damage was around \$2,300,000, and the cost of GDP loss was around \$99,900,000.

One significant long-term cost is the impact on government spending to increase security processes to identify and prevent future attacks. At the current rate of terrorist attacks, research suggests that the approximate combination of direct government spending on counterterrorism and taxation as a result of this spending is about \$190 billion (Zycher, 2003). Going back to the analysis for the cost of human life, if 50% of all extremist-related deaths were due to right-wing extremist attacks and 52.22% of these attacks were facilitated by social media, then 26.11% of this aforementioned spending, or \$49.6 billion, is due to right-wing extremist attacks facilitated by social media (*"New ADL data"*, 2022). However, it should be recognized that there is no concrete data on how the current amount of defense spending is affecting the number of RWE attacks.

Another significant long-term cost is that of mental health illness after attacks have occurred. The rate of post-traumatic stress disorder (PTSD), for example, amongst direct victims of terrorist attacks is between 15 and 26 percent (Davis et al., 2022). Since data does not exist about the number of community members, this analysis will focus on direct family members of people who died in RWE attacks associated with social media use. In 2021, the average family had 3.13 persons (Duffin, 2022). If one died in an attack, that means that each victim had around 2.13 direct family members or 31.95 total people who lost someone in a social-media-facilitated RWE attack in 2021. This means between 4.79 and 8.31 people developed PTSD due to this issue. The annual cost of PTSD for a civilian is around \$18,640 annually. This translates to a total cost of between \$89,000 and \$155,000 due to PTSD caused by this issue. The actual cost of mental illness caused by such attacks is actually likely far higher since first responders and other community members are also affected, and other mental illnesses may also be caused by such attacks. A table of the short and long-term costs of this problem can be found in Appendix B.

## Existing Evidence

Much of the literature on the issue discusses research on potential methods to prevent right-wing extremist use of social media to influence acts of violent extremism. This summary of existing evidence largely focuses on best practices from other countries as suggested by countering violent extremism practitioners. It also draws on some quantitative studies that highlight the potential effects of the interventions on comparable issues. Though the quantitative evidence is not particularly strong, it does provide some confidence in interventions still being studied by experts.

### Public-Private Partnerships

Public-private partnerships between governments and technology companies can enable the restriction, removal, and prevention of extremist content online. The idea behind this strategy is that while governments themselves cannot necessarily remove extremist content from online platforms, by partnering with technology companies, they can develop norms and regulations to guide platforms in removing and moderating content.

Many countries have established such policies, the most prominent being Germany, which implemented its Network Enforcement Act (NetzDG) in 2017. This law requires large media platforms to remove “clearly illegal” content following user complaints with the threat of a fine for noncompliance. Assessment of the impact of this policy on content regulation on Twitter, Youtube, and Facebook indicated that throughout 2019, Youtube saw an increase in take-down rate by 2.5% and Twitter saw an increase by 6.9%. However, Facebook saw a reduction in the takedown rate from 25.5% to 13.3%. However, this study did not take into account any confounding factors that could be affecting takedown rates, including a lower-take-down rate in the pre-period than they reported (Park, 2020). Other sites have also implemented bans on certain types of content. For example, in 2015 Reddit imposed a ban on two significant subreddits due to harassment. Researchers analyzed the use of hate speech following this ban. The researchers used a matching and difference-in-difference model to conduct the analysis. By matching users of the banned subreddits to similar users in other subreddits the treatment users also engaged with, the researchers were able to see that twice the number of users subject to the ban became inactive compared to those not subject to it. To control for time-invariant confounding factors, the researchers also used a difference-in-difference method to observe the effects on the usage of hate speech. They found that after the ban, there was an 81-91% decrease in the use of hate words based on the type of content (Chandrasekharan et al., 2017). This suggests that partnerships with private companies may be effective in encouraging the removal of extremist content and continuing the reduction of extremist content. It should be considered, however, that Freedom of Speech is a huge tenet in the United States, which means that it may be more difficult for it to implement methods of content moderation.

However, as countering violent extremism experts have emphasized, these policies do not address social media platforms that focus on messaging as removal, and content mediation typically relies on static posts (*Countering online radicalisation A strategy for action* 2009). This is problematic since on many major platforms, such as Telegram, the main appeal is users’ ability to have unmonitored private

conversations with others (Walther & McCoy, 2021). Regulations developed via partnerships with social media platforms may still be useful if they rely on user reporting to identify extremist content (*Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies* 2021).

Finally, researchers have also pointed out that policies that come out of the aforementioned public-private partnerships can be ineffective because there is still not a universal definition of what constitutes “terrorist content” meaning companies may be confused by what content actually must be removed (Clifford, 2021).

## Digital Literacy Programs

Digital literacy programs have been suggested by many experts to be useful in preventing people from being drawn in by extremist messaging online. Though many experts suggest implementing such programs to counter right-wing extremism, there exists little concrete data on their efficacy for this specific use.

One research study observed students in classes that received digital literacy programming compared to students in classes that did not. Using questionnaires following the programming the researchers found that students who received digital literacy education saw an increase in awareness, defined by the researchers as knowledge about what extremist propaganda looks like. This increase was statistically significant with an average increase in awareness of 0.87 on a scale of 0-1 as opposed to a decrease in awareness of 0.48 for those that didn’t receive the programming (Schmitt et al., 2018). This suggests that digital literacy programs can effectively help people recognize extremist content online. However, this study did not randomly assign students to receive or not receive the programming meaning it is possible that other factors influenced this increased awareness. Furthermore, it only focused on youth, which is not the only target population. Finally, this study focuses on the impact of digital literacy programming on preventing susceptibility to Islamic extremist messaging, and effects may be different in response to exposure to right-wing extremist content.

There has been some research on the effect of digital literacy programs on people’s ability to identify misinformation. A 2020 study randomly exposed United States citizens to literacy programs that provide indicators of false news. They then surveyed those who did and did not get this intervention to estimate their accuracy in identifying false news. The study found that on a 4-point scale measuring accuracy, with 4 being the most inaccurate, there was a statistically significant decrease in inaccuracy by 0.2 points (Guess et al., 2020). However, this study does not focus on the efficacy of extremist messaging, meaning this evidence may not have useful implications for the use of such programming against right-wing extremist content online.

## Counter-Messaging Campaigns

Counter-messaging is often suggested as a solution to extremist content online when moderation is not an option. The idea behind this tactic is that it can prevent the efficacy of extremist propaganda online. There is a lack of quantitative research that supports the efficacy of counter-messaging in preventing extremist messaging from radicalizing others or facilitating violent behavior.

One report on counter-messaging campaigns described the impact of ExitUSA, which was a video campaign designed to counter right-wing extremism. Though the report lacked quantitative data supporting the impact of this program, qualitative evidence showed that this campaign generated discussion via comments, though 18% of these comments were negative. However, experts suggest that this indicates that this is a sign of progress because it demonstrates that the campaigns both reached the target audience and led to increased engagement. Additionally, at least eight people involved in right-wing organizations reached out to ExitUSA for help leaving the movements (Colliver & Davey, 2017). However, this data does not necessarily indicate a causal relationship and is highly speculative.

Despite the lack of concrete evidence supporting the efficacy of counter-messaging, experts have identified good practices for such programming. Many practitioners recommend that the messaging come from credible sources that will be seriously considered by target audiences. For example, they suggest that former members of right-wing extremist members be utilized in these campaigns as they are relatable to those who may be most susceptible (Macnair & Frank, 2017). Furthermore, they also suggest that civil society be engaged in counter-messaging campaigns because they can be effective in creating positive networks to combat extremist propaganda. Sweden has implemented this through its #IAmHere movement, which enables volunteers to inject facts into conversations identified to potentially be coming from extremists (*White Supremacy Extremism: The Transnational Rise of the Violent White Supremacist Movement* 2019). However, there is, once again, no concrete evidence to support these best practices.

## Alternatives

### Alternative 1: Takedown Legislation

Currently, many major social media websites claim they will take down illegal content and block accounts when they receive complaints. However, this has not been enough to prevent RWE content.

To address this the DoS could lobby for a new regulation based on Germany's Network Enforcement Act (NetzDG). The German NetzDG Act was implemented in 2017 and requires that social media companies with more than 2 million registered German users must take down "clearly illegal" content within 24 hours of receiving a user complaint. If they do not comply, they can be fined up to \$50 million. Furthermore, a 2021 amendment required that the complaint process be user-friendly and easy to access, that users be provided with an appeals process if their content or profile is flagged or removed, and that social media companies publish biannual transparency reports detailing how they have handled complaints they received (*"Germany: Network enforcement act amended", 2021*).

In the United States, this amendment would require that social media companies with more than 6.5 million registered users in the United States take down content within 24 hours of receiving a complaint if the content violates the platform's standards. The size of the platform was determined by scaling up Germany's threshold to account for the United States population. Violation of this policy would result in fines of up to \$50 million as determined by the Federal Trade Commission (FTC). Furthermore, this law would ensure that complaints be easy to submit and that users be provided with a clear process to seek redress if their content or profile is taken down. Additionally, platforms would be required to publish reports similar to those required under NetzDG biannually. Finally, to continue to protect platforms this amendment should reaffirm that the removal of some content due to this regulation does not then mean that the platform is liable for other content still published on the site (*"Department of Justice's review of Section 230", 2021*).

#### Alternative 1: Key Takeaways

1. Legislation that requires large platforms to address complaints within 24 hours
2. Regulated by FTC with potential fines for violations
3. Requires biannual reports on takedowns to be published

### Alternative 2: Digital Literacy Programming

Digital literacy programming targeted at preventing youth from being radicalized or believing misinformation is not widely distributed across the nation. To remedy this, the DoS could partner with STOMP Out Bullying, an NPO that partners with schools across the nation to prevent cyberbullying. This NPO already teaches solutions to respond to bullying and digital literacy training could be offered as part of its programming. This is in line with the organization's mission to prevent violence in schools (*About stomp out bullying*).

The digital literacy program could be based on Lewis University's How2INFORM (H2i) Educators Toolkit which is funded by a grant from the Department of Homeland Security. This program already has a plan for development and rollout that could be utilized by the NPO (*Application for Federal Assistance* 2022).

To fund spreading this programming to all of STOMP Out Bullying's partners across the United States, the NPO could apply for the DHS's Targeted Violence and Terrorism Prevention (TVTP) Grant Program. The grant has been prioritizing programs targeting online aspects of terrorism which makes it highly likely that they will receive it (*Targeted violence and terrorism prevention grant program*).

#### Alternative 2: Key Takeaways

1. Provides digital literacy programming to youth by partnering with STOMP Out Bullying
2. Based on Lewis University's How2INFORM Educator's Toolkit
3. Aims to prevent radicalization that occurs via social media

### Alternative 3: Counter-Messaging Campaign

Numerous organizations have implemented counter-messaging campaigns but the messaging is not consolidated and often does not target RWE. Therefore, the DoS's Office of Strategic Communications and Outreach could work with the Institute of Strategic Dialogue (ISD), the United States Institute of Peace (USIP), and other member think tanks of the Global Counterterrorism Forum (GCTF) to consolidate their current counter-narrative programs and use ongoing research on best practices to develop them further ("*GCTF - members and partners*"). These programs would specifically target RWE and expand ISD's Against Violent Extremism Network to include more former right-wing extremists in the campaigns ("*Against violent extremism (AVE) network*").

To do this, the Office would need to hire two more staff members to take on this new project and liaison with the organizations and other relevant bodies. Additionally, the Office could present its work at its annual conference that hosts youth and senior officials to promote awareness amongst the younger population. Finally, the Office would need to train members in search engine optimization (SEO) so that they can scale these campaigns to reach broad audiences without the use of advertising.

#### Alternative 3: Key Takeaways

1. Coordinates a counter-messaging campaign across members of GCTF
2. Establishes best practices for counter-messaging based on research
3. Utilizes search engine optimization to broaden reach

## Criteria

Each proposed alternative will be assessed on four criteria: cost-effectiveness, political feasibility, administrative feasibility, and securing rights.

### Cost-Effectiveness

Given that the negative impacts of successful plots are the greatest relative to radicalization, a reduction in successful plots will be used to measure efficacy. Effectiveness will project the expected reduction in the number of successful RWE plots that were facilitated via large social media platforms. Cost is measured by the monetary cost borne by the DoS to develop and implement each alternative. This will include salaries of staff, research and development cost, upkeep cost, and other spending.

Cost-Effectiveness is then the ratio of cost to effectiveness and represents the cost per attack reduced by the given alternative.

### Political Feasibility

This criterion indicates whether the DoS, Congress, and relevant partners would be willing to implement each alternative, and also considers potential pushback from social media companies. Political feasibility is measured on a scale of 1 to 3, with 1 indicating low political feasibility and 3 indicating high political feasibility.

### Administrative Feasibility

Administrative feasibility measures whether the DoS and relevant partners can implement each alternative in terms of staff, necessary research and materials, and other administrative factors. It further considers the difficulty of building the capability needed to implement each alternative. Administrative feasibility is measured on a scale of 1 to 3, with 1 indicating low administrative feasibility and 3 indicating high administrative feasibility.

### Securing Rights

This criterion will measure the degree to which each alternative secures existing freedoms and rights. In particular, it will consider freedom of speech protected under the First Amendment. It will be measured on a scale of increases, meaning even more flexibility is given to citizens, neutral, meaning that there is no change, and decreases, meaning more restrictions are placed on citizens.

### Weighting Considerations

Since securing rights is only a significant concern for one alternative, it is weighted lower than the other criteria at 10%. The other three criteria are all equally important and therefore each weighted at 30%.



## Evaluation of Alternatives

### Evaluation of Alternative 1

#### *Cost-Effectiveness*

##### Score – \$151,000

From Germany's NetzDG, Youtube saw an increase in takedown by 2.5% and Twitter saw an increase by 6.9%, therefore, the average increase in takedown rate is between 2.5% and 6.9% (Park, 2020). I will assume that it is around 4.7%. Additionally, a ban on offensive Reddit threads showed a 90% continued decrease in hate content across threads. This suggests that only 10% of users whose content or accounts were removed will move platforms. This suggests that effectiveness can be determined by multiplying the number of plots in a year by 0.047 (the increase in takedown rate) and then by the effectiveness in preventing movement across platforms (0.9). It should be noted that this Reddit study did not look at users' likelihood of changing platforms. Overall, this alternative is expected to prevent around 20 attacks over 11 years. Full calculations can be found in Appendix C.

In terms of costs, the FTC will need to hire additional personnel to monitor transparency reports submitted by companies. I assume that three additional personnel will be required. Each year, a GS-9 employee's salary increases based on the GS pay scale (*Washington DC pay locality - general schedule pay areas*). Additionally, benefits typically cost the government about 38% of an employee's annual salary. (*Federal Employee Benefits Summary*, 2023). Costs borne by social media companies are not included in this calculation as these are not paid by the government or its partners. However, they are considered in assessing political feasibility. Overall, this alternative is expected to cost around \$2.99 million across 11 years in 2023 dollars. Full calculations can be found in Appendix C.

#### *Political Feasibility*

##### Score – 1

Currently, two bills have been introduced in Congress that attempt to require social media sites to improve their regulation of potentially extremist content. The first was cosponsored by a Democrat and a Republican Senator and was referred to the Committee on Commerce, Science, and Transportation. This bill requires that interactive computer services report suspicious activity to assist with counterterrorism efforts. (*See Something, Say Something Online Act of 2023*). Though neither cosponsor sits on this committee, the introduction of this bill demonstrates support across the aisle for efforts to increase the takedown of RWE content. The second bill was introduced in the House by a Republican Representative and referred to the House Committee on Energy and Commerce. This bill attempts to limit the immunity of interactive computer services under CDA 230. However, this Representative does not sit on the committee that this bill was referred to (*CASE-IT Act*). The Department of Justice has also created a review of CDA 230 that recommends similar amendments as this alternative does. This suggests broader support for this alternative (*"Department of Justice's review of Section 230"*, 2021). However, because social media sites likely will have to hire personnel solely to comply with the regulations, they are likely to push back on this regulation. Large tech lobbying groups, namely the Computer and Communications Industry Association and NetChoice, will likely lead the push and have large pools of funding.

### *Administrative Feasibility*

#### Score – 3

The FTC will be the bureaucratic body in charge of implementing this legislation should it be passed. Since the Bureau of Consumer Protection already enforces similar policies, this would not require a large adaptation of the FTC's operating procedures. For example, the FTC imposed a \$5 billion penalty on Facebook (now Meta) in 2019 for violations of consumer privacy rights (*FTC imposes \$5 billion, 2019*).

### *Securing Rights*

#### Score – Decreases

This alternative does not require interactive computer services to take down content. Instead, it requires that they respond to complaints in a timely manner and assess them based on their own policies, making it content-neutral. Content-neutral regulations are not unconstitutional and still protect citizens' rights to free speech. However, experts have argued that regulation of interactive computer services can lead to "censorship creep" which could lead to protected speech being removed as well (Clifford, 2021).

## Evaluation of Alternative 2

### *Cost-Effectiveness*

#### Score – \$71,500

Critical media literacy programming has been shown to increase awareness of Islamist online propaganda by about 10% and likely would have similar effects on awareness of RWE content (Schmitt et al., 2018). I assume a 10% increase in awareness would lead to a 10% decrease in attacks assuming that all students have received digital literacy programming. The average age of a right-wing extremist is about 27 years old, and therefore effects are likely not going to be seen until the first group of high schoolers reaches around 24 years of age (seven years after the start of implementation) (*Theme report: What is the background of right-wing extremists in Norway?*, 2019). Therefore, this analysis uses a linear projection to estimate effectiveness between years 7 and 11 if the effect of the program grows to full effect by year 11. This analysis also provides cost-effectiveness assuming 50% efficacy with a sensitivity analysis conducted for 100% efficacy since all potential extremists likely won't have been exposed to this programming. Overall, this alternative is expected to prevent 7 attacks across 11 years at 50% efficacy. Full calculations can be found in Appendix D.

In terms of costs, Lewis University has budgeted \$2,349 for supplies and \$37,521 for a part-time principal investigator for their two-year program that targets all of Illinois (*Application for Federal Assistance 2022*). There are 10,103 total schools in Illinois (*Illinois schools*). STOMP Out Bullying currently partners with 45,000 schools, which is about 4.5 times more than H2i (STOMP Out Bullying, "Home"). This means their supply cost should be 4.5 times greater, which is \$10,570.50. Since this version of the alternative does not include travel it likely will be able to be fully developed and rolled out in 5 years. Therefore, after 5 years, an implementation plan will be in place and should be able to be integrated into the NPO's existing distribution model without additional help from a principal investigator. Additionally, the principal investigator of H2i was a part-time employee, but in this case, a full-time employee would be needed. I assume that this salary would be about double, which would mean a yearly salary of \$75,042. Additionally, benefits typically cost the government about 38% of an employee's annual salary (*Federal*

*Employee Benefits Summary, 2023*). The supply cost is broken down across the 10 years and the principal investigator's salary is no longer accounted for after 5 years. Overall, this alternative is expected to cost around \$354,000 across 11 years in 2023 dollars. Full calculations can be found in Appendix D.

#### *Political Feasibility*

##### Score – 1

This alternative requires DoS to work with another organization and therefore relies on both of their willingness to implement this alternative. Currently, STOMP Out Bullying's mission statement indicates that it "works to reduce and prevent bullying, cyberbullying, and other digital abuse, educates against homophobia, LGBTQIA+ discrimination, racism, and hatred, and deters violence in schools, online and in communities across the country" (STOMP Out Bullying, "Home"). Therefore, promoting digital literacy to prevent extremism seems in line with their organization's goals. Furthermore, the organization already has a bullying prevention toolkit they have made available to educators. However, this program may need to be phased out as not all schools that STOMP Out Bullying partners with will likely want to implement this training initially. Therefore, marketing it and encouraging schools to implement it may dissuade the organization from wanting to invest in this alternative.

#### *Administrative Feasibility*

##### Score – 1

The DoS would need to collaborate with the NPO and Lewis University outside to develop and disseminate a comprehensive digital literacy program. Because Lewis University has already partnered with DHS and has made many of its materials public, working with them to utilize the program they develop should be feasible. However, the DoS has never partnered with STOMP Out Bullying before, and facilitating a new relationship will likely require a lot of administrative work. Additionally, since the distribution channel already exists for STOMP Out Bullying's toolkit, they will likely be able to utilize that same process to disseminate the digital literacy toolkit as well. The DoS will have to hire a principal investigator to oversee development and implementation in the first few years. Given that it does not hold the same security as a full-time role within a specific Bureau, this may be challenging.

#### *Securing Rights*

##### Score – No Change

This alternative does not affect citizens' right to speech as it is not regulatory. Additionally, the aim of the program is not to teach students to censor their posts but rather to learn to identify extremist content online. Therefore, this alternative does not affect the rights of citizens.

## Evaluation of Alternative 3

#### *Cost-Effectiveness*

##### Score – \$230,000

Targeted counternarratives decrease internalization by 12.84% (Carthy & Sarma, 2021). Only 33.67% of RWEs conducted successful plots via passive social media use (Safer-Lichtenstein et al., 2018). This analysis assumes that if appropriate best practices are implemented, these studies will be fairly

representative of the effect the campaign will have. Assuming that within five years these counter-narrative campaigns will reach full effect, this analysis uses a projection to determine the impact if it grows linearly from 0 to a 4.3% reduction in attacks ( $.1284 * .3367$ ). It then assumes a stable impact from this point onward. Furthermore, this analysis provides cost-effectiveness assuming 50% efficacy with a sensitivity analysis conducted for 100% efficacy as well as it is unlikely that all RWEs will see a counter-narrative post. Overall, this alternative is expected to prevent 9 attacks across 11 years at 50% efficacy. Full calculations can be found in Appendix E.

Since most of these organizations already conduct counter-messaging campaigns, the only cost they need to account for is hiring two additional DoS employees. On average, the salary of a GS-9 employee is \$64,957 in year 0, and increases based on the GS pay scale (*Washington DC pay locality - general schedule pay areas*). Additionally, benefits typically cost the government about 38% of an employee's annual salary (*Federal Employee Benefits Summary*, 2023). Overall, this alternative is expected to cost around \$1.45 million across 11 years. Full calculations can be found in Appendix E.

#### *Political Feasibility*

##### Score – 3

This alternative requires DoS to work with another organization and therefore relies on both of their willingness to implement this alternative. All of the organizations this alternative proposes as partners are members of the Global Counterterrorism Forum (GCTF) and it is therefore not unreasonable for them to partner in other capacities as well (*"GCTF - members and partners"*). Furthermore, the DoS has worked with GCTF in the past and already has connections with them (*"About us"*, n.d). Finally, since these organizations have campaigns that they already run, it is clear they believe that they are important and effective, and would therefore be open to implementing this alternative.

#### *Administrative Feasibility*

##### Score – 3

To implement this alternative, the DoS would need to hire at least two more personnel. This may be somewhat difficult as hiring personnel requires the applicants to be able to obtain security clearances. However, given that the State Department hires yearly and many new graduates will be eligible for this position, it should not be a large burden. Additionally, the aforementioned organizations already have some form of counter-messaging occurring and therefore would not need to make large adjustments to their operating models to accommodate for this.

#### *Securing Rights*

##### Score – No Change

This alternative does not affect citizens' right to speech as it is not regulatory. Additionally, the aim of the program is not to censor posts but rather to provide more accurate information to the public. Therefore, this alternative does not affect the rights of citizens.

## Outcomes Matrix<sup>4</sup>

	Cost-Effectiveness (30%)	Political Feasibility (30%)	Administrative Feasibility (30%)	Securing Rights (10%)	Total
Alternative 1: Takedown Legislation	\$151,000 (2 points)	1 (1 point)	3 (3 points)	Decreases (1 point)	1.9
Alternative 2: Digital Literacy Programming	\$71,500 (3 points)	1 (1 point)	1 (1 point)	No Change (2 points)	1.7
Alternative 3: Counter-Messaging Campaign	\$230,000 (1 point)	3 (3 points)	3 (3 points)	No Change (2 points)	2.3

## Recommendation

I recommend that the DoS should implement a counter-messaging campaign alongside members of the GCTF as it has the highest total score compared to the other alternatives. This alternative is both highly politically and administratively feasible and would not affect the rights of citizens. Though it is more costly than the other alternatives, it remains the most likely to be implemented and works within the DoS's current capacities. Additionally, it has a higher effectiveness, in terms of reduction of attacks, than Alternative 2, which scores the highest on cost-effectiveness. Additionally, if it worked at 100% efficacy would be almost as effective in reducing attacks as Alternative 1 and be almost two times more cost-effective. This calculation can be found in Appendix E.

## Implementation

### Funding

The DoS should look to reallocate the budgets used by organizations already running counter-messaging campaigns to accommodate a new streamlined approach. Ideally, this new joint program would replace

<sup>4</sup> A scoring key and calculations for the total score can be found in Appendix F.

current RWE campaigns. Additionally, the NGOs could apply for the DHS's Targeted Violence and Terrorism Prevention (TVTP) Grant Program. The grant has been prioritizing programs targeting online aspects of terrorism which makes it highly likely that they will receive it (*Targeted violence and terrorism prevention grant program*).

## Initial Steps

The first step that the DoS needs to take to develop this campaign is to hire additional personnel within the Office of Strategic Communications. Since the security clearance process can take up to 120 days or longer, this should begin immediately to allow time for resume review and interviewing (*FAQs (frequently asked questions) - careers* 2022). From there, the Office should reach out to the United States Institute of Peace (USIP) as they already work closely on numerous projects. Specifically, the RESOLVE Network and the Public Affairs and Communications teams are involved with countering violent extremism and strategic communications and would be the most helpful in starting this project. Members of the DoS Bureau of Counterterrorism have funded past RESOLVE projects and maintain a relationship with many of the team members and should make initial contact before responsibility on to the Office for Strategic Communications. From there, the DoS and USIP can connect with members of the GCTF to further this initiative.

## Developing a Message

This initiative will require a compilation of best practices derived from the current counter-messaging campaigns run by GCTF member organizations. However, as a starting point, the DoS should consider that experts recommend that messaging come from credible sources that will be seriously considered by target audiences. For example, they suggest that former members of right-wing extremist members be utilized in these campaigns as they are relatable to those who may be most susceptible (Macnair & Frank, 2017). To implement this, the campaign could expand ISD's Against Violent Extremism Network to include more former right-wing extremists (*"Against violent extremism (AVE) network"*). Furthermore, they also suggest that civil society be engaged in counter-messaging campaigns because they can be effective in creating positive networks to combat extremist propaganda. Sweden has implemented this through its #IAmHere movement, which enables volunteers to inject facts into conversations identified to potentially be coming from extremists (*White Supremacy Extremism: The Transnational Rise of the Violent White Supremacist Movement* 2019).

## Rollout

Though it is ideal for these counter-messaging posts to be on all possible platforms, it would be most feasible to begin with one and then expand. Many successful campaigns have been run on Twitter, which provides a tried starting ground from which to expand (Silverman et al., 2016). Additionally, to maximize reach, the campaigns should utilize search engine optimization, which makes content appear higher and more often when keywords are searched (Google, *Search Engine Optimization (SEO) Starter Guide*).

## Challenges

The most significant challenge will be developing best practices for partner organizations to use when creating content. Though all of the organizations suggested as partners will likely be agreeable to improving their practices, developing these guidelines takes research and cooperation which can be difficult when they also have separate projects to run. Timely creation of these guides will therefore prove to be the most significant hurdle to implementation. However, many guides exist and the ISD has even already put one together that provides a significant starting point (Silverman et al., 2016).

## Conclusion

Right-wing extremism is a growing issue within the United States, with attacks quadrupling between 2016 and 2017 (Jones, 2022). Furthermore, over 50% of RWE attacks that have occurred have been facilitated by social media (Safer-Lichtenstein et al., 2018). Unfortunately, current practices have not been sufficient in preventing successful plots from being carried out with the help of online platforms. This report provided three potential alternatives to the status quo to combat this issue: takedown legislation, digital literacy programming, and counter-messaging campaigns. These alternatives were evaluated based on cost-effectiveness, political feasibility, administrative feasibility, and securing rights. Though counter-messaging campaigns are the least cost-effective, they are highly feasible and can be implemented with the fewest challenges.

The DoS should begin hiring personnel and reach out to GCTF member organizations to begin to develop a strategy for coordinated counter-messaging to begin implementing these campaigns.

## Appendix

### Appendix A: Status Quo and Projected Number of Attacks

The projected number of attacks between 2023 and 2034 was estimated by creating a linear forecast using data from 2012 through 2021. The expected number of attacks facilitated by social media was found by multiplying the projected number by .5222 (Doxsee et al., 2002; *“The escalating terrorism problem in the United States”*, 2020; Safer-Lichtenstein et al., 2018).

Year	Number of Attacks	Forecast	Number of attacks facilitated by social media
2012	14		7.3108
2013	6		3.1332
2014	7		3.6554
2015	15		7.833
2016	13		6.7886
2017	53		27.6766
2018	29		15.1438
2019	44		22.9768
2020	73		38.1206
2021	38		19.8436
2022		50.4629032	26.35172805
2023		54.9	28.66878
2024		59.3370968	30.98583195
2025		63.7741935	33.30288385
2026		68.2112903	35.61993579
2027		72.6483871	37.93698774
2028		77.0854839	40.25403969
2029		81.5225806	42.57109159
2030		85.9596774	44.88814354
2031		90.3967742	47.20519549
2032		95.4352	49.83626144
2033		99.2709677	51.83929933
2034		103.708065	54.15635154



## Appendix B: Costs to Society of RWE Use of Social Media

Cost Categories	Cost Description	Annual Cost (in 2021)
Short-Term	Loss of Life	\$150,000,000
	Injuries	\$5,700,000
	Property Damage	\$2,300,000
	GDP Loss	\$99,900,000
Long-Term	Government Spending and Taxes	\$49,600,000,000
	Mental Illness (PTSD)	\$89,000- \$155,000
Total	Total Short-Term	\$258,000,000
	Total Long-Term	~\$49,600,000,000

## Appendix C: Alternative 1 Cost-Effectiveness Assumptions and Calculations

### Cost Calculations with NPV Sensitivity Analysis ("Washington DC pay locality")

Year (starting 2023-2024)	Cost	Cost Breakdown
0	$\$64957 * 3 * 1.38 = \$268,921.28$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
1	$\$67122 * 3 * 1.38 = \$277,885.08$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
2	$\$69287 * 3 * 1.38 = \$286,848.18$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
3	$\$71452 * 3 * 1.38 = \$295,811.28$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
4	$\$71452 * 3 * 1.38 = \$295,811.28$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
5	$\$73617 * 3 * 1.38 = \$304,774.38$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
6	$\$73617 * 3 * 1.38 = \$304,774.38$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
7	$\$75782 * 3 * 1.38 = \$313,737.48$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
8	$\$75782 * 3 * 1.38 = \$313,737.48$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
9	$\$77947 * 3 * 1.38 = \$322,700.58$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
10	$\$77947 * 3 * 1.38 = \$322,700.58$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
11	$\$77947 * 3 * 1.38 = \$322,700.58$	Cost of 3 additional personnel at GS-9 + benefits (38% of salary)
NPV at 3%	\$2,994,278.38	
NPV at 7% (sensitivity analysis)	\$2,371,553.39	

### Effectiveness Calculations (Park, 2020)

Year (starting 2023-2024)	Effectiveness (reduction in successful plots)	Calculations
0	0	0
1	1.310700691	=30.98583195*0.047*0.9
2	1.408711987	=33.3028838457*0.047*0.9
3	1.506723284	=35.61993579*0.047*0.9
4	1.604734582	=37.93698774362*0.047*0.9
5	1.702745879	=40.25403969*0.047*0.9
6	1.800757174	=42.57109159*0.047*0.9
7	1.898768472	=44.88814354*0.047*0.9
8	1.996779769	=47.20519549*0.047*0.9
9	2.108073859	=49.83626144*0.047*0.9
10	2.192802362	=51.83929933*0.047*0.9
11	2.29081367	=54.15635154*0.047*0.9
Total	19.82	

\*Based upon status quo projections of the number of attacks found in Appendix A

\*Formula: (Projected number of attacks) \* (Average takedown rate) \* (% that don't move platforms)

### Cost Effectiveness with NPV Sensitivity Analysis

NPV	Cost-Effectiveness	Calculations
3%	\$151,061.30	=\$2,994,278.38 / 19.82
7%	\$119,644.83	=\$2,371,553.39 / 19.82

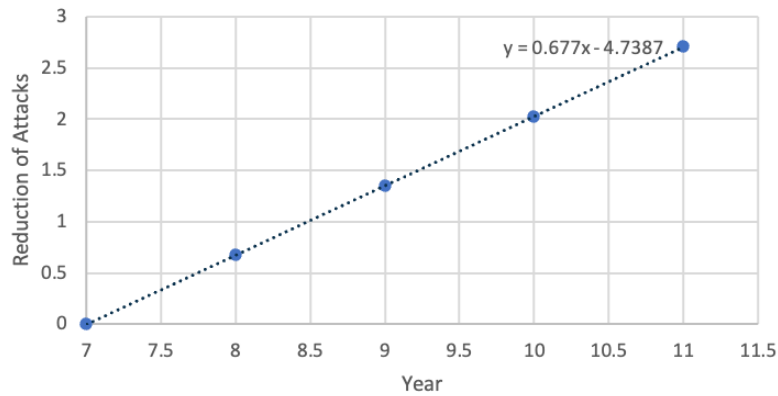
## Appendix D: Alternative 2 Cost-Effectiveness Assumptions and Calculations

### Cost Calculations with NPV Sensitivity Analysis (*Application for Federal Assistance 2022*)

Year (starting 2023-2024)	Cost	Cost Breakdown
0	$\$75,042.00 \times 1.38 = \$103,557.96$	Cost of PI salary during the development period + benefits (38% of salary)
1	$\$75042 \times 1.38 + 1097.55 = \$104,655.51$	Cost of PI salary + benefits + 1/10 supplies
2	$\$75042 \times 1.38 + 1097.55 = \$104,655.51$	Cost of PI salary + benefits + 1/10 supplies
3	$\$75042 \times 1.38 + 1097.55 = \$104,655.51$	Cost of PI salary + benefits + 1/10 supplies
4	$\$75042 \times 1.38 + 1097.55 = \$104,655.51$	Cost of PI salary + benefits + 1/10 supplies
5	$\$75042 \times 1.38 + 1097.55 = \$104,655.51$	Cost of PI salary + benefits + 1/10 supplies
6	\$1097.55	1/10 supplies
7	\$1097.55	1/10 supplies
8	\$1097.55	1/10 supplies
9	\$1097.55	1/10 supplies
10	\$1097.55	1/10 supplies
11	\$1097.55	1/10 supplies
NPV at 3%	\$484,124.57	
NPV at 7% (sensitivity analysis)	\$428,813.85	

\*Assumptions: The cost of the program will be 4.5 times as much as Lewis University's. The cost of supplies for Lewis University is \$2,349, so the cost to the DoS will be \$10,570.50.

### Projected Ramp-Up of Reduction of Attacks Between Year 7 and Year 11 (50% efficacy)

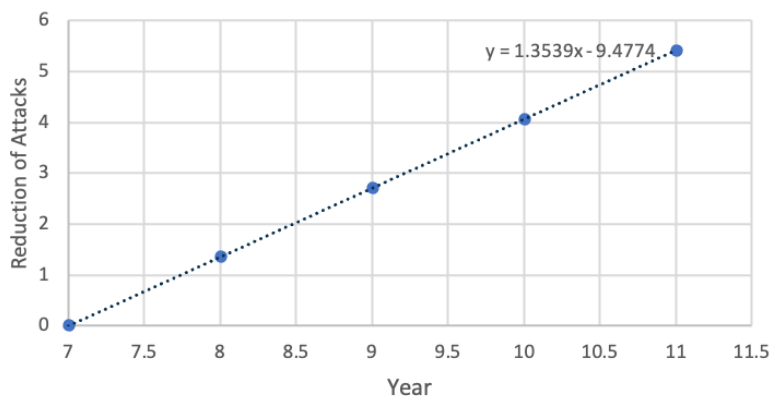


Assuming that the program will reach full 50% efficacy by year 11 but effects will be seen after year 7, this model uses a linear projection which yielded the equation shown above to determine what the reduction of attacks will be between year 7 and year 11. Reduction at year 11 was found by multiplying the projected number of attacks by 10% (this program should lead to 10% reduction) and then dividing this in half for 50% efficacy.

### Effectiveness Calculations at 50% Efficacy (Schmitt et al., 2018)

Year (starting 2023-2024)	Effectiveness (reduction in successful plots)	Calculations
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0.677	$=0.677(8) - 4.7387$
9	1.354	$=0.677(9) - 4.7387$
10	2.031	$=0.677(10) - 4.7387$
11	2.70781758	$=54.15635154*0.05$
Total	6.77	

**Projected Ramp-Up of Reduction of Attacks Between Year 7 and Year 11 (100% efficacy sensitivity analysis)**



Assuming that the program will reach full efficacy by year 11 but effects will be seen after year 7, this model uses a linear projection which yielded the equation shown above to determine what the reduction of attacks will be between year 7 and year 11. Reduction at year 11 was found by multiplying the projected number of attacks by 10% (this program should lead to 10% reduction).

**Effectiveness Calculations at 100% efficacy sensitivity analysis (Schmitt et al., 2018)**

Year (starting 2023-2024)	Effectiveness (reduction in successful plots)	Calculations
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	1.3539	=1.3539(8) - 9.4774
9	2.7078	=1.3539(9) - 9.4774
10	4.0617	=1.3539(10) - 9.4774
11	5.415635154	=54.15635154*0.1
Total	13.54	

**Cost Effectiveness 50% efficacy with NPV Sensitivity Analysis**

NPV	Cost-Effectiveness	Calculations
3%	\$71,512.20	=\$484,124.57 / 6.77
7%	\$63,342.01	=\$428,813.85 / 6.77

**Cost Effectiveness 100% efficacy with NPV Sensitivity Analysis**

NPV	Cost-Effectiveness	Calculations
3%	\$35,757.69	=\$484,124.57 / 13.54
7%	\$31,672.41	=\$428,813.85 / 13.54

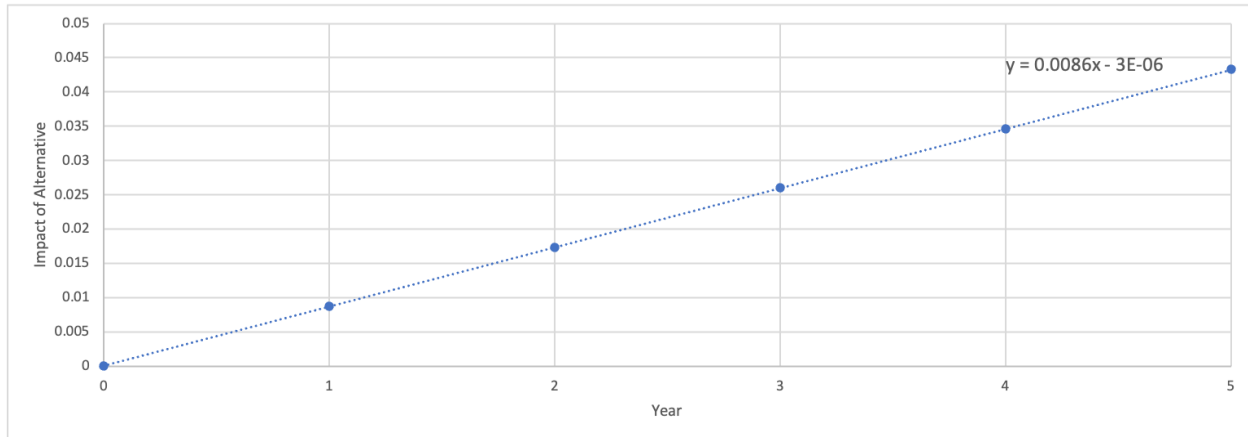
## Appendix E: Alternative 3 Cost-Effectiveness Assumptions and Calculations

### Cost Calculations with NPV Sensitivity Analysis ("Washington DC pay locality")

Year (starting 2023-2024)	Cost	Cost Breakdown
0	$\$64957 * 2 * 1.38 = \$179,281.32$	Cost of two additional personnel at GS-9 + benefits
1	$\$67122 * 2 * 1.38 = \$185,256.72$	Cost of two additional personnel at GS-9 + benefits
2	$\$69287 * 2 * 1.38 = \$191,232.12$	Cost of two additional personnel at GS-9 + benefits
3	$\$71452 * 2 * 1.38 = \$197,207.52$	Cost of two additional personnel at GS-9 + benefits
4	$\$71452 * 2 * 1.38 = \$197,207.52$	Cost of two additional personnel at GS-9 + benefits
5	$\$73617 * 2 * 1.38 = \$203,182.92$	Cost of two additional personnel at GS-9 + benefits
6	$\$73617 * 2 * 1.38 = \$203,182.92$	Cost of two additional personnel at GS-9 + benefits
7	$\$75782 * 2 * 1.38 = \$209,158.32$	Cost of two additional personnel at GS-9 + benefits
8	$\$75782 * 2 * 1.38 = \$209,158.32$	Cost of two additional personnel at GS-9 + benefits
9	$\$77947 * 2 * 1.38 = \$215,133.72$	Cost of two additional personnel at GS-9 + benefits
10	$\$77947 * 2 * 1.38 = \$215,133.72$	Cost of two additional personnel at GS-9 + benefits
11	$\$77947 * 2 * 1.38 = \$215,133.72$	Cost of two additional personnel at GS-9 + benefits
NPV at 3%	\$1,996,185.59	
NPV at 7% (sensitivity analysis)	\$1,581,035.60	



**Projected Growth of Impact of Alternative (Year 0 to Year 5)**



Assuming that this alternative will reach full impact in five years, this model uses a linear projection to estimate the growth in impact of alternative 3 from year 0 to year 5. The impact in year 5 was found by multiplying the effect of counternarratives on internalization (.1284) by the percent of RWEs that conduct successful plots and passively use social media (.3367) to get a total full impact of about 0.043 (Carthy & Sarma, 2021; Safer-Lichtenstein et al., 2018).

**Effectiveness Calculations at 50% Efficacy**

Year (starting 2023-2024)	Effectiveness (reduction in successful plots)	Calculations
0	0	0
1	0.133952061	= 0.00864602*30.98583195*.5
2	0.287803522	= 0.017284*33.30288385*.5
3	0.461822441	= 0.02593056*35.61993579*.5
4	0.655875889	= 0.03457712*37.93698774*.5
5	0.870136958	= 0.04323228*40.25403969*.5
6	0.920222676	= 0.04323228*42.57109159*.5
7	0.970308395	= 0.04323228*44.88814354*.5
8	1.020394114	= 0.04323228*47.20519549*.5
9	1.077267604	= 0.04323228*49.83626144*.5
10	1.120565552	= 0.04323228*51.83929933*.5
11	1.170651277	= 0.04323228*54.15635154*.5
Total	8.69	

**Effectiveness Calculations at 100% efficacy sensitivity analysis**

Year (starting 2023-2024)	Effectiveness (reduction in successful plots)	Calculations
0	0	0
1	0.267904123	= 0.00864602*30.98583195
2	0.575607044	= 0.017284*33.30288385
3	0.923644882	= 0.02593056*35.61993579
4	1.311751778	= 0.03457712*37.93698774
5	1.740273915	= 0.04323228*40.25403969
6	1.840445352	= 0.04323228*42.57109159
7	1.94061679	= 0.04323228*44.88814354
8	2.040788229	= 0.04323228*47.20519549
9	2.154535209	= 0.04323228*49.83626144
10	2.241131104	= 0.04323228*51.83929933
11	2.341302554	= 0.04323228*54.15635154
Total	17.38	

**Cost Effectiveness 50% efficacy with NPV Sensitivity Analysis**

NPV	Cost-Effectiveness	Calculations
3%	\$229,737.08	=\$1,996.185.59 / 8.69
7%	\$181,958.28	=\$1,581,035.60 / 8.69

**Cost Effectiveness 100% efficacy with NPV Sensitivity Analysis**

NPV	Cost-Effectiveness	Calculations
3%	\$114,868.54	=\$1,996.185.59 / 17.38
7%	\$90,979.14	=\$1,581,035.60 / 17.38

## Appendix F: Outcomes Scoring Key & Calculations

<b>Cost-Effectiveness (30%)</b>	<b>Highest Cost (1 point)</b>	<b>Middle Cost (2 points)</b>	<b>Lowest Cost (1 point)</b>
<b>Political Feasibility (30%)</b>	<b>1 (1 point)</b>	<b>2 (2 points)</b>	<b>3 (3 points)</b>
<b>Administrative Feasibility (30%)</b>	<b>1 (1 point)</b>	<b>2 (2 points)</b>	<b>3 (3 points)</b>
<b>Securing Rights (10%)</b>	<b>Decreases (1 point)</b>	<b>No Change (2 points)</b>	<b>Increases (3 points)</b>

### Scoring Calculations

Overall Formula:  $(0.3 \times \text{cost-effectiveness score}) + (0.3 \times \text{political feasibility score}) + (0.3 \times \text{administrative feasibility score}) + (0.1 \times \text{securing rights score})$

Alternative 1:  $(0.3 \times 2) + (0.3 \times 1) + (0.3 \times 3) + (0.1 \times 1) = 1.9$

Alternative 2:  $(0.3 \times 3) + (0.3 \times 1) + (0.3 \times 1) + (0.1 \times 2) = 1.7$

Alternative 3:  $(0.3 \times 1) + (0.3 \times 3) + (0.3 \times 3) + (0.1 \times 2) = 2.3$

## References

- American University. (2021, January). *Building Resilience & Confronting Risk in the COVID-19 Era*. Retrieved February 9, 2023, from [https://www.american.edu/centers/university-excellence/upload/splc\\_peril\\_covid\\_parents\\_guide.pdf](https://www.american.edu/centers/university-excellence/upload/splc_peril_covid_parents_guide.pdf)
- Anti-Defamation League. (2022, February 14). *New ADL data: Far-right extremists responsible for overwhelming majority of domestic extremist-related murders in 2021*. Retrieved October 13, 2022, from <https://www.adl.org/news/press-releases/new-adl-data-far-right-extremists-responsible-for-overwhelming-majority-of>
- Bardwell, H., & Iqbal, M. (2020). The economic impact of terrorism from 2000 to 2018. *Peace Economics, Peace Science and Public Policy*, 27(2), 227–261. <https://doi.org/10.1515/peps-2020-0031>
- Braddock, K., Hughes, B., Goldberg, B., & Miller-Idriss, C. (2022). Subversive online activity predicts susceptibility to persuasion by far-right extremist propaganda. *New Media & Society*. <https://doi.org/10.33767/osf.io/c734s>
- Bump, P. (2022, April 23). *The platform where the right-wing bubble is least likely to pop*. The Washington Post. Retrieved September 18, 2022, from <https://www.washingtonpost.com/politics/2022/04/23/telegram-platform-right-wing/>
- Carthy, S. L., & Sarma, K. M. (2021). Countering terrorist narratives: Assessing the efficacy and mechanisms of change in counter-narrative strategies. *Terrorism and Political Violence*, 1–25. <https://doi.org/10.1080/09546553.2021.1962308>
- CASE–IT Act (n.d.). bill. Retrieved March 2, 2023, from <https://www.congress.gov/bill/118th-congress/house-bill/573?q=%7B%22search%22%3A%5B%22communications+act%22%5D%7D&s=2&r=8>.
- Center for Strategic and International Studies. (2020, June 17). *The escalating terrorism problem in the United States*. Retrieved October 13, 2022, from <https://www.csis.org/analysis/escalating-terrorism-problem-united-states>
- Center for Strategic & International Studies. (2022, November 22). *The rise of far-right extremism in the United States*. Retrieved December 7, 2022, from <https://www.csis.org/analysis/rise-far-right-extremism-united-states>
- Chandrasekharan, E., Pavalanathan, U., Srinivasan, A., Glynn, A., Eisenstein, J., & Gilbert, E. (2017). You can't stay here. *Proceedings of the ACM on Human-Computer Interaction*, 1, 1–22. <https://doi.org/10.1145/3134666>
- Clifford, B. (2021, December). *Moderating extremism: The state of online terrorist content removal ...* Retrieved November 10, 2022, from <https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf>
- Colliver, C., & Davey, J. (2017). Cross-Spectrum Counter Violent Extremism: Prevention and Intervention Models. In *Digitale Medien und politischweltanschaulicher Extremismus im Jugendalter*. essay, Deutsches Jugendinstitut . Retrieved from

- [https://www.dji.de/fileadmin/user\\_upload/bibs2017/Digitale\\_Medien.AFS.Band.13.pdf#page=166](https://www.dji.de/fileadmin/user_upload/bibs2017/Digitale_Medien.AFS.Band.13.pdf#page=166).
- Conway, M., Scrivens, R., & Macnair, L. (2019). *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends*. <https://doi.org/10.19165/2019.3.12>
- Davis, L. L., Schein, J., Cloutier, M., Gagnon-Sanschagrin, P., Maitland, J., Urganus, A., Guerin, A., Lefebvre, P., & Houle, C. R. (2022). The economic burden of posttraumatic stress disorder in the United States from a societal perspective. *The Journal of Clinical Psychiatry*, 83(3). <https://doi.org/10.4088/jcp.21m14116>.
- Department of Homeland Security . (n.d.). *Targeted violence and terrorism prevention grant program*. Retrieved March 2, 2023, from <https://www.dhs.gov/tvtpgrants>
- Department of Justice's review of Section 230 of the communications decency act of 1996*. The United States Department of Justice. (2021, January 20). Retrieved February 9, 2023, from <https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996>
- DHS strategic framework for countering terrorism and targeted violence*. DHS Strategic Framework for Countering Terrorism and Targeted Violence | Homeland Security. (2019, September). Retrieved November 3, 2022, from <https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence>.
- Doxsee, C., Jones, S. G., Thompson, J., Halstead, K., & Hwang, G. (2022, May 17). *Pushed to extremes: Domestic terrorism amid polarization and protest*. Retrieved March 2, 2023, from <https://www.csis.org/analysis/pushed-extremes-domestic-terrorism-amid-polarization-and-protest#:~:text=The%20total%20number%20of%20domestic,percent%20from%20the%20prior%20year>
- Duffin, E. (2022, September 30). *Average family size in the U.S. 1960-2021*. Statista. Retrieved October 13, 2022, from <https://www.statista.com/statistics/183657/average-size-of-a-family-in-the-us/#:~:text=As%20of%202021%2C%20the%20U.S.,18%20living%20in%20the%20household>
- FederalPay. (n.d.). *Washington DC pay locality - general schedule pay areas*. Retrieved March 2, 2023, from <https://www.federalpay.org/gs/locality/washington-dc>
- Federal Trade Commission. (2019, July 24). *FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook*. Retrieved March 16, 2023, from <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>
- Food Safety and Inspection Service. (2023, February 28). *Federal Employee Benefits Summary*. Retrieved April 25, 2023, from <https://www.fsis.usda.gov/careers/incentives/federal-employee-benefits-summary>
- Galston, W. A., & Kamarck, E. (2022, January 4). *Is democracy failing and putting our economic system at risk?* Retrieved November 3, 2022, from <https://www.brookings.edu/research/is-democracy-failing-and-putting-our-economic-system-at-risk/>

*Germany: Flawed social media law*. Human Rights Watch. (2018, February 14). Retrieved September 18, 2022, from <https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law>

*Germany: Network enforcement act amended to better fight online hate speech*. The Library of Congress. (2021). Retrieved February 9, 2023, from <https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/>

Global Counterterrorism Forum. (n.d.). *GCTF - members and partners*. Retrieved February 9, 2023, from <https://www.thegctf.org/About-us/Members-and-partners>

Gonzalez, S., & Malone, K. (2020, April 15). *Lives vs. the economy*. NPR. Retrieved December 7, 2022, from <https://www.npr.org/2020/04/15/835571843/episode-991-lives-vs-the-economy>

Google. (n.d.). *Search Engine Optimization (SEO) Starter Guide*. Retrieved March 19, 2023, from <https://developers.google.com/search/docs/fundamentals/seo-starter-guide>

Great Schools. (n.d.). *Illinois schools*. Retrieved March 2, 2023, from <https://www.greatschools.org/illinois/>

Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences*, 117(27), 15536–15545. <https://doi.org/10.1073/pnas.1920498117>

Indah, K. (2022, September 29). *How many people use telegram in 2022?* EarthWeb. Retrieved October 13, 2022, from <https://earthweb.com/how-many-people-use-telegram/>

Institute for Strategic Dialogue. (n.d.). *Against violent extremism (AVE) network*. Retrieved February 9, 2023, from <https://www.isdglobal.org/against-violent-extremism-ave/>

International Centre for the Study of Radicalisation and Political Violence . (2009). *Countering online radicalisation A strategy for action*. Retrieved November 10, 2022, from <https://icsr.info/wp-content/uploads/2010/03/ICSR-Report-The-Challenge-of-Online-Radicalisation-A-Strategy-for-Action.pdf>

iThrive Games. (2021, October 1). *ITHRIVE games, Middlebury Institute of International Studies awarded DHS grant for new simulation game*. Retrieved February 9, 2023, from <https://ithrivegames.org/newsroom/blog/countering-radicalization-with-play-dhs-grant/>

Jones, S. G. (2022, September 16). *The rise of far-right extremism in the United States*. Retrieved September 18, 2022, from <https://www.csis.org/analysis/rise-far-right-extremism-united-states>

Koetsier, J. (2021, December 27). *Top 10 most downloaded apps and games of 2021: Tiktok, telegram big winners*. Forbes. Retrieved September 18, 2022, from <https://www.forbes.com/sites/johnkoetsier/2021/12/27/top-10-most-downloaded-apps-and-games-of-2021-tiktok-telegram-big-winners/?sh=3fbf3a983a1f>

Lewis University . (2022). *Application for Federal Assistance*. Retrieved March 2, 2023, from [https://www.cisa.gov/sites/default/files/2023-02/DHS%20Form%20SF315\\_7-31-2023.pdf](https://www.cisa.gov/sites/default/files/2023-02/DHS%20Form%20SF315_7-31-2023.pdf)

Liang, C. S., & Cross, M. J. (2020). White Crusade: How to Prevent Right-Wing Extremists from Exploiting the Internet. *Geneva Center for Security Policy* , (11).

Macnair, L., & Frank, R. (2017). Voices Against Extremism:A case study of a community-based CVE counter-narrative campaign. *Journal for Deradicalization*.

- Mattheis, A. A. (2022). Atomwaffen division and its affiliates on telegram: Variations, practices, and Interconnections. *RESOLVE Network*. <https://doi.org/10.37805/remve2022.1>
- Mccabe, D. (2023, January 19). *Supreme Court poised to reconsider key tenets of online speech*. The New York Times. Retrieved March 2, 2023, from <https://www.nytimes.com/2023/01/19/technology/supreme-court-online-free-speech-social-media.html>
- Park, J. (2020). *The public-private partnerships' impact on transparency and effectiveness in the Eu internet content regulation: The Case of "Network Enforcement Act (NetzDG)" in Germany* (thesis). Schriftenreihe für Public und Nonprofit Management. Retrieved from <https://doi.org/10.25932/publishup-48718>.
- Pew Research Center. (2021, April 7). *Internet/broadband fact sheet*. Retrieved September 18, 2022, from <https://www.pewresearch.org/internet/fact-sheet/internet-broadband/>
- Politiets Sikkerhetstjeneste. (2019, April 4). *Theme report: What is the background of right- wing extremists in Norway?* Retrieved March 2, 2023, from [https://www.politietstryggingsteneste.no/globalassets/artikler/utgivelser/theme-report\\_-what-is-the-background-of-rightwing-extremists-in-norway.pdf](https://www.politietstryggingsteneste.no/globalassets/artikler/utgivelser/theme-report_-what-is-the-background-of-rightwing-extremists-in-norway.pdf)
- Robinson, M. M. (2022). *Social media recruitment and online propaganda by extremist groups* (thesis).
- Safer-Lichtenstein, A., LaFree, G., Jensen, M., & James, P. (2018). *Use of social media by US extremists* . Retrieved October 14, 2022, from [https://www.start.umd.edu/pubs/START\\_PIRUS\\_UseOfSocialMediaByUSExtremists\\_ResearchBrief\\_July2018.pdf](https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf)
- Schmitt, J. B., Rieger, D., Ernst, J., & Roth, H.-J. (2018). Critical Media Literacy and Islamist Online Propaganda: The Feasibility, Applicability and Impact of Three Learning Arrangements. *International Journal of Conflict and Violence*, 12. <https://doi.org/10.4119/UNIBI/ijcv.642>
- See Something, Say Something Online Act of 2023 (n.d.). bill. Retrieved March 2, 2023, from <https://www.congress.gov/bill/118th-congress/senate-bill/147/text?s=2&r=1&q=%7B%22search%22%3A%5B%22communications+act%22%5D%7D>
- Silverman, T., Stewary, C. J., Amanullah, Z., & Birdwell, J. (2016). *The impact of counter-narratives - ISD*. Retrieved March 20, 2023, from [http://www.isdglobal.org/wp-content/uploads/2016/08/Impact-of-Counter-Narratives\\_ONLINE.pdf](http://www.isdglobal.org/wp-content/uploads/2016/08/Impact-of-Counter-Narratives_ONLINE.pdf)
- Smith, A. G. (2018). How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us. *National Institute of Justice*.
- STOMP Out Bullying™. (n.d.). *About stomp out bullying*. Retrieved February 9, 2023, from <https://www.stompoutbullying.org/about>
- STOMP Out Bullying. (n.d.). *Home*. Retrieved March 2, 2023, from <https://www.stompoutbullying.org/>
- Targeted violence and terrorism prevention grant program*. Targeted Violence and Terrorism Prevention Grant Program | Homeland Security. (n.d.). Retrieved February 9, 2023, from <https://www.dhs.gov/tvtpgrants>
- The FCC's authority to interpret Section 230 of the Communications Act*. Federal Communications Commission. (2020, October 21). Retrieved September 18, 2022, from

- <https://www.fcc.gov/news-events/blog/2020/10/21/fccs-authority-interpret-section-230-communications-act>
- The Soufan Center. (2019, September). *White Supremacy Extremism: The Transnational Rise of the Violent White Supremacist Movement*. Retrieved November 10, 2022, from <https://thesoufancenter.org/wp-content/uploads/2019/09/Report-by-The-Soufan-Center-White-Supremacy-Extremism-The-Transnational-Rise-of-The-Violent-White-Supremacist-Movement.pdf>
- Tech Against Terrorism. (2021). *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*. Retrieved November 10, 2022, from <https://www.techagainstterrorism.org/>
- Telegram APIs. (n.d.). *End-to-end encryption, secret chats*. Retrieved November 10, 2022, from <https://core.telegram.org/api/end-to-end>
- Twitter. (n.d.). *United States - Twitter Transparency Center*. Retrieved March 2, 2023, from <https://transparency.twitter.com/en/reports/countries/us.html#2021-jul-dec>
- United Nations Office on Drugs and Crime. (2018, July). *Counter-terrorism module 2 key issues: Radicalization & Violent extremism*. E4J University Module Series: Counter-Terrorism. Retrieved October 13, 2022, from <https://www.unodc.org/e4j/zh/terrorism/module-2/key-issues/radicalization-violent-extremism.html>
- U.S. Department of State. (n.d.). *About Us – Bureau of Counterterrorism - United States Department of State*. U.S. Department of State. Retrieved September 18, 2022, from <https://www.state.gov/about-us-bureau-of-counterterrorism/>
- U.S. Department of State. (2022, August 9). *FAQs (frequently asked questions) - careers*. U.S. Department of State. Retrieved March 19, 2023, from <https://careers.state.gov/faqs/>
- von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism*. RAND.
- Walther, S., & McCoy, A. (2021). US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism. *Perspectives on Terrorism*, 15(2), 100–124. <https://www.jstor.org/stable/27007298>
- Zycher, B. (2003). *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*. RAND Corporation. Retrieved from [https://www.rand.org/pubs/monograph\\_reports/MR1693.html](https://www.rand.org/pubs/monograph_reports/MR1693.html)