

THE DIGITAL BATTLEFIELD: HOW ON-LINE
TERRORISTS USE THE INTERNET AND ON-
LINE NETWORKS FOR RECRUITMENT AND
RADICALIZATION

HEARING

BEFORE THE

SUBCOMMITTEE ON
COUNTERTERRORISM,
LAW ENFORCEMENT, AND
INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MARCH 4, 2025

Serial No. 119-5

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

60-837 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi, <i>Ranking Member</i>
CLAY HIGGINS, Louisiana	ERIC SWALWELL, California
MICHAEL GUEST, Mississippi	J. LUIS CORREA, California
CARLOS A. GIMENEZ, Florida	SHRI THANEDAR, Michigan
AUGUST PFLUGER, Texas	SETH MAGAZINER, Rhode Island
ANDREW R. GARBARINO, New York	DANIEL S. GOLDMAN, New York
MARJORIE TAYLOR GREENE, Georgia	DELIA C. RAMIREZ, Illinois
TONY GONZALES, Texas	TIMOTHY M. KENNEDY, New York
MORGAN LUTTRELL, Texas	LAMONICA MCIVER, New Jersey
DALE W. STRONG, Alabama	JULIE JOHNSON, Texas, <i>Vice Ranking Member</i>
JOSH BRECHEEN, Oklahoma	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
ELIJAH CRANE, Arizona	NELLIE POU, New Jersey
ANDREW OGLES, Tennessee	SYLVESTER TURNER, Texas
SHERI BIGGS, South Carolina	VACANT
GABE EVANS, Colorado	VACANT
RYAN MACKENZIE, Pennsylvania	
BRAD KNOTT, North Carolina	

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

AUGUST PFLUGER, Texas, *Chairman*

MARJORIE TAYLOR GREENE, Georgia	SETH MAGAZINER, Rhode Island, <i>Ranking Member</i>
TONY GONZALES, Texas	J. LUIS CORREA, California
MORGAN LUTTRELL, Texas	DANIEL S. GOLDMAN, New York
GABE EVANS, Colorado	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
RYAN MACKENZIE, Pennsylvania	NELLIE POU, New Jersey
MARK E. GREEN, MD, Tennessee (<i>ex officio</i>)	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)

MICHAEL KOREN, *Subcommittee Staff Director*
BRITTANY CARR, *Minority Subcommittee Staff Director*

CONTENTS

	Page
STATEMENTS	
The Honorable August Pfluger, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence:	
Oral Statement	1
Prepared Statement	3
The Honorable Seth Magaziner, a Representative in Congress From the State of Rhode Island, and Ranking Member, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence:	
Oral Statement	5
Prepared Statement	6
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Prepared Statement	7
WITNESSES	
Mr. Daveed Gartenstein-Ross, Ph.D., Senior Advisor on Asymmetric Warfare, Foundation for Defense of Democracies:	
Oral Statement	9
Prepared Statement	10
Mr. Aaron Zelin, Ph.D., Senior Research Fellow, The Washington Institute for Near East Policy:	
Oral Statement	22
Prepared Statement	24
Mr. Daniel Flesch, Senior Policy Analyst, Middle East and North Africa, Allison Center for National Security, The Heritage Foundation:	
Oral Statement	29
Prepared Statement	30
Mr. Kurt Braddock, Ph.D., Assistant Professor, Public Communication, American University:	
Oral Statement	34
Prepared Statement	36

THE DIGITAL BATTLEFIELD: HOW ON-LINE TERRORISTS USE THE INTERNET AND ON- LINE NETWORKS FOR RECRUITMENT AND RADICALIZATION

Tuesday, March 4, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM,
LAW ENFORCEMENT, AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:14 p.m., at Room 310, Cannon House Office Building, Hon. August Pfluger [Chairman of the subcommittee] presiding.

Present: Representatives Pfluger, Greene, Luttrell, Magaziner, Correa, Goldman, and Pou.

Also present: Representative Crane.

Mr. PFLUGER. The Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence will come to order. Without objection, this committee may recess at any point. Without objection, the gentleman from Arizona, Mr. Eli Crane, is permitted to sit on the dais and ask questions of witnesses.

The purpose of this hearing is to identify how foreign terrorist organizations, like ISIS and other nefarious actors, use the internet, on-line networks, and generative AI to recruit and radicalize individuals to commit violence and terrorist acts. This hearing will also explore policy solutions to ensure law enforcement agencies have the necessary tools and training to combat these threats. I now recognize myself for an opening statement.

Good afternoon. Welcome to the first Counterterrorism and Intelligence Subcommittee hearing of the 119th Congress. I would like to begin by welcoming all the Members here today. I would also like to take a second to welcome several new Members to the committee: Representatives Gabe Evans, Ryan Mackenzie, Nellie Pou, and Pablo José Hernández. These Members will be coming in after the vote series has just ended.

But last Congress, this subcommittee held various hearings on pressing national security issues. Those national security threats range from vulnerabilities posed by transnational criminal organizations and known or suspected terrorists at our Southern Border to the threats posed by the Chinese Communist Party and the Iranian regime to U.S. homeland security. We will continue to work on those issues and expand our scope to include new and emerging threats.

This subcommittee also conducted critical oversight on important DHS entities, such as the Office of Intelligence and Analysis, and the ramifications of policy decisions made by the Biden administration, such as our Nation's withdrawal from Afghanistan. Our Nation faces many challenges and this subcommittee must examine these threats through a clear and objective lens. Since 9/11 and the formation of this committee, this subcommittee has worked tirelessly to ensure that our Nation understands the threats that face the United States and that our law enforcement agencies have the proper tools to safeguard our country and the American people. As Chairman of this subcommittee, I am committed to working with everyone on this committee to advance these goals.

Unfortunately, we did begin this year with a sober reminder that the same ideology that radicalized 19 individuals to hijack commercial airliners and fly them into the World Trade Center, the Pentagon, and in Shanksville, Pennsylvania, drove an individual to commit a heinous ISIS-inspired terror attack that killed 14 people and injured dozens more on Bourbon Street in New Orleans, Louisiana. Our thoughts and prayers are with all of those affected by this tragedy.

Since the terror attack, the Nation has learned more about that particular perpetrator's background. The individual, Shamsud-Din Jabbar, is believed to have self-radicalized on-line through various propaganda channels affiliated with ISIS. The FBI has also confirmed that Jabbar's on-line search history indicated he conducted extensive research into the terror attacks that took place last year at a German Christmas market and that he pledged his support to ISIS on his personal on-line media accounts, including Facebook.

The case related to Jabbar is not an isolated incident of an individual within the United States becoming radicalized on-line by a foreign terrorist organization. On-line radicalization is a significant terrorism threat that our Nation currently faces. In fact, the Ranking Member and myself have agreed that this would be the first hearing in a bipartisan way that we want to tackle this issue. I hope everyone knows that we have worked together on this and I hope that we can focus and hone in on these particular issues right here in a bipartisan way.

But at a recent Homeland Security and Government Affairs Committee hearing, former FBI Director Wray highlighted the severity of the threat when he stated, "The greatest terrorism threat to our homeland is posed by lone actors or small cells of individuals who typically radicalize to violence on-line and who primarily use easily accessible weapons to attack soft targets."

To provide greater context, between April 2021 and January 2025, there were over 50 indictments against individuals who have worked to provide material support or carry out an attack on behalf of foreign terrorist organizations like ISIS, al-Qaeda, and Hezbollah. Almost all of these individuals have been radicalized by terrorist media propagations.

Americans' ability to access propaganda from foreign terrorist organizations is easier than ever. Groups like al-Qaeda, ISIS, and Boko Haram are disseminating their propaganda at lightning speed across the globe on platforms such as Telegram and Redz. Hamas, Hezbollah, and other Iranian proxies have utilized TikTok

and other platforms to spread propaganda in the West related to Israel's war with Hamas in hopes of radicalizing individuals to join their quest to launch a global intifada.

We saw this hateful propaganda mold the actions of radicalized protesters at Columbia University and other colleges across the United States. Another stark example of on-line radicalization was seen last year when thousands of Americans went on TikTok and attempted to rationalize Osama Bin Laden's letter to America and victim blame our Nation for the atrocities that took place on 9/11. Moreover, we have now seen an increase in juvenile home-grown violent extremists inspired by foreign terrorist organizations' media being shared on youth-oriented platforms. For instance, a 16-year-old in Las Vegas, Nevada, was arrested after threatening a lone-wolf terrorist attack in support of ISIS and possessing components and instructions to build a bomb. He wrote in a chat room that he would be starting lone-wolf operations in Las Vegas against the enemies of Allah.

There is no doubt that ISIS actively looks to inspire younger individuals and frequently produces media tailored at juveniles because they think they are more susceptible to terrorist ideologies and more accessible due to their on-line presence on a range of platforms. We must acknowledge and confront this urgent threat head-on or we risk having another incident like we did in New Orleans.

I hope today's discussion is the first of many productive conversations on the enduring terrorism threats our Nation faces and how this subcommittee can find legislative solutions to overcome these challenges. I also hope that while we may disagree here in a partisan way on some of the things that have happened in the last couple of years, I hope that we can really focus and limit blame, that we can take the context and the facts. I hope that the Ranking Member knows that I took seriously his inputs to having this hearing, to holding this hearing, to focusing on this not just as a sign of goodwill, but also as a sign that this committee, of all the committees in Congress, that this committee right here was formed after the worst terrorist attack in our country, and that the sole reason we have this committee is to ensure that the oversight of those entrusted with national security, of homeland security, do it correctly.

[The statement of Chairman Pfluger follows:]

STATEMENT OF CHAIRMAN AUGUST PFLUGER

MARCH 4, 2025

Good afternoon, and welcome to the first Counterterrorism and Intelligence Subcommittee hearing of the 119th Congress.

I want to begin by welcoming all the Members here today. I'd also like to take a second to welcome several new Members to the committee. Representatives Gabe Evans, Ryan Mackenzie, Nellie Pou, and Pablo José Hernández.

Last Congress, this subcommittee held various hearings on pressing national security issues.

Those national security threats ranged from the vulnerabilities posed by transnational criminal organizations and known or suspected terrorists at our Southern Border to the threats posed by the Chinese Communist Party and the Iranian regime to U.S. homeland security.

We will continue to work on those issues and expand our scope to include new and emerging threats.

This subcommittee also conducted critical oversight work on important DHS entities, such as DHS's Office of Intelligence and Analysis, and the ramifications of policy decisions made by the Biden administration, such as our Nation's withdrawal from Afghanistan.

Our Nation faces many challenges, and this subcommittee must examine these threats through a clear and objective lens.

Since 9/11 and the formation of this committee, this subcommittee has worked tirelessly to ensure that our Nation understands the threats that face the United States and that our law enforcement agencies have the proper tools to safeguard our country and the American people.

As Chairman of this subcommittee, I am committed to working with everyone to advance these goals.

Unfortunately, we began this year with a sober reminder that the same ideology that radicalized 19 individuals to hijack commercial airliners and fly them into the World Trade Center, the Pentagon, and Shanksville, Pennsylvania, drove an individual to commit a heinous ISIS-inspired terror attack that killed 14 people and injured dozens more on Bourbon Street in New Orleans, Louisiana.

Our thoughts and prayers are with all of those affected by this tragedy.

Since the New Orleans terror attack, the Nation has learned more about the perpetrator's background.

The individual, Shamsud-Din Jabbar, is believed to have self-radicalized on-line through various propaganda channels affiliated with ISIS.

The FBI has also confirmed that Jabbar's on-line search history indicated he conducted extensive research into the terror attacks that took place last year at a German Christmas market and that he pledged his support for ISIS on his personal Facebook account.

The case related to Jabbar is not an isolated incident of an individual within the United States becoming radicalized on-line by a foreign terrorist organization.

On-line radicalization is a significant terrorism threat our Nation currently faces.

At a recent Homeland Security and Government Affairs Committee hearing, former FBI Director Wray highlighted the severity of this threat when he stated: "[t]he greatest terrorism threat to our homeland is posed by lone actors or small cells of individuals who typically radicalize to violence on-line, and who primarily use easily accessible weapons to attack soft targets."

To provide greater context, between April 2021 and January 2025, there were over 50 indictments against individuals who have worked to provide material support or carry out an attack on behalf of foreign terrorist organizations like ISIS, al-Qaeda, and Hezbollah.

Almost all of these individuals had been radicalized by terrorist media propaganda.

Americans' ability to access propaganda from foreign terrorist organizations is easier than ever.

Groups like al-Qaeda, ISIS, and Boko Haram are disseminating their propaganda at lightning speed across the globe on platforms, such as Telegram and Redz.

Hamas, Hezbollah, and other Iranian proxies have utilized TikTok and other platforms to spread propaganda in the West related to Israel's war with Hamas in hopes of radicalizing individuals to join their quest to launch a global intifada.

We saw this hateful propaganda mold the actions of radicalized protesters at Columbia University and other colleges across the United States.

Another stark example of on-line radicalization was seen last year when thousands of Americans went on TikTok and attempted to rationalize Osama bin Laden's letter to America and victim-blame our Nation for the atrocities that took place on 9/11.

Moreover, we have now seen an increase in juvenile home-grown violent extremists inspired by foreign terrorist organizations' media being shared on youth-oriented platforms.

For instance, a 16-year-old in Las Vegas, Nevada, was arrested after threatening a lone-wolf terrorist attack in support of ISIS and possessing components and instructions to build a bomb. He wrote in a chatroom that he would be "starting lone-wolf operations in Las Vegas against enemies of Allah."

There is no doubt that ISIS actively looks to inspire younger individuals and frequently produces media tailored at juveniles because they think they are more susceptible to terrorist ideologies and more accessible due to their on-line presence on a range of platforms.

We must acknowledge and confront this urgent threat head-on, or we risk having another terrorist attack like New Orleans take place here in the United States.

I hope today's discussion is the first of many productive conversations on the enduring terrorism threats our Nation faces and how this subcommittee can find legislative solutions to overcome these challenges.

I thank our distinguished panel for their testimony today.

With that, I yield to the gentleman from Rhode Island, Ranking Member Magaziner, for his opening statement.

Mr. PFLUGER. With that, I thank our distinguished panel. I will introduce you shortly. I would like to yield to the gentleman from Rhode Island, my friend and the Ranking Member, Mr. Magaziner, for his opening statement.

Mr. MAGAZINER. I thank Chairman Pfluger for his kindness and also for having this hearing today. I think it is appropriate that this is our first hearing in this subcommittee of the new Congress. It is a topic I have been interested in addressing for some time and I know that he is very interested in it as well, because increasingly, on-line radicalization is one of the largest threats that we face to the homeland. I want to thank our witnesses for being here as well.

On New Year's Day, 14 innocent people lost their lives and more than 50 were injured when a terrorist drove a pickup truck into a crowd on Bourbon Street in New Orleans. In their investigation after the attack, the FBI found that the attacker had been radicalized on-line through information about ISIS and engagement with ISIS content. According to the Department of Homeland Security's Office of Intelligence and Analysis, since August 2023, so just a year-and-a-half, law enforcement has disrupted 5 plots in which juveniles were radicalized by foreign terrorist organizations on-line and mobilized to plan terror attacks. Five times in just the last 5 years—sorry, just the last year-and-a-half.

While foreign terrorist organizations like ISIS and al-Qaeda exploit the internet to spread propaganda, they, unfortunately, are not the only bad actors who use on-line platforms to inspire individuals to violence. In September, the Justice Department indicted 2 individuals who are leaders of the so-called Terrorgram Collective and a domestic neo-fascist terrorist organization that used the Telegram platform to plot the murder of Federal officials, including a U.S. senator, U.S. district court judge, and a U.S. attorney, who they considered to be "enemies of the white race." Terrorgram provided guidance and instructions for terror attacks, encouraging the use of bombs to attack critical infrastructure, such as government buildings and energy facilities as well.

In December 2023, the FBI arrested an Arizona man for using social media to incite a religiously-motivated terror attack in Australia, an ambush shooting that killed 6 people, including 2 police officers. This individual and his wife and brother were motivated by an extreme religious ideology and attacked and killed victims simply for being law enforcement officers. We also know that on-line radicalization played a key role in the white supremacist extremist attack in Buffalo in 2022 when an 18-year-old terrorist killed 10 people, all of whom were African American. An investigative report by the Office of the New York State Attorney General found that this individual learned about the so-called Great Replacement Theory via memes, an ideology that he himself cited as the basis for his racist terror attack.

So these are just a few examples of domestic violent extremists' use of the internet and digital content for recruitment and

radicalization. Of course, foreign terrorist organizations, as has been noted, are using the same exact strategies, unfortunately, often to lethal effect.

Congress is not powerless to stop this. Social media companies and gaming companies can and should moderate violent extremist content on-line with proper consideration for protected speech. They should also cooperate with law enforcement investigations.

To be clear, American citizens have a First Amendment right to hold and espouse extreme ideologies. However, there is no First Amendment right to plot acts of violence. There is no First Amendment right to recruit others into committing acts of violence. Foreign terrorists have no First Amendment rights of any sort. So social media companies and gaming companies are in no way compelled to allow terrorists or criminals to use their platforms to incite violence. In fact, they should face consequences if they knowingly do so. That is something that Congress needs to act on.

I worked with Ranking Member Thompson to request that the Government Accountability Office examine how social media and gaming companies report and mitigate on-line content that promote violent extremism, and the extent to which the FBI and DHS have developed goals and strategies for sharing information on the threat of violent extremism on social media and gaming companies. The GAO produced its findings in January 2024, which included neither—but neither DHS nor FBI have developed such a strategy. They must do so, and the strategy must be comprehensive to include all forms of on-line radicalization and incitement of violence, whatever the ideology behind it may be.

It is my hope that this subcommittee will continue today's conversation with today's experts, but also with representatives of the social media and on-line gaming industries and the relevant law enforcement agencies so that we can explore real answers, including legislative solutions, in combating on-line radicalization.

I thank the Chairman again for his bipartisan approach to this topic. I am excited to work together on it and I yield back.

[The statement of Ranking Member Magaziner follows:]

STATEMENT OF RANKING MEMBER SETH MAGAZINER

MARCH 4, 2025

On New Year's Day, 14 innocent people lost their lives and over 50 were injured when a terrorist drove a pickup truck into a crowd on Bourbon Street in New Orleans. In their investigation after the attack, the FBI found that the attacker had been radicalized on-line through information about ISIS and engagement with ISIS content.

According to the Department of Homeland Security's Office of Intelligence and Analysis, since August 2023, law enforcement has disrupted 5 plots in which juveniles were radicalized by foreign terrorist organizations on-line and mobilized to plan terror attacks. While foreign terrorist organizations like ISIS and al-Qaeda exploit the internet to spread propaganda, they unfortunately aren't the only bad actors who use on-line platforms to inspire individuals to violence.

In September, the Justice Department indicted Dallas Humber and Matthew Allison, 2 leaders of the Terrorgram Collective—a far-right, neo-fascist terrorist organization—that used the Telegram platform to plot the murder of Federal officials such as a U.S. Senator, a U.S. district court judge, and a U.S. attorney who they considered enemies of the white race. Terrorgram provided guidance and instructions for terrorist attacks encouraging the use of bombs to attack critical infrastructure such as government buildings and energy facilities.

In December 2023, the FBI arrested an Arizona man for using social media to incite a “religiously-motivated terrorist attack,” in Australia—an ambush shooting that killed 6 people including 2 police officers. Gareth Train, his brother Nathaniel Train and Nathaniel’s wife Stacey Train, motivated by a Christian extremist ideology—attacked and killed the victims simply for being law enforcement officers.

We also know that on-line radicalization played a key role in the white supremacist extremist attack in Buffalo in 2022, when an 18-year-old terrorist killed 10 people—all of whom were African American. An investigative report by the Office of the New York State Attorney General found that the Buffalo terrorist learned about the so-called “Great Replacement Theory” via memes—an ideology he cited as the basis for his racist terrorist attack.

These are just a few examples of domestic violent extremists’ use of the internet and digital content for recruitment and radicalization. Congress is not powerless to stop this.

Social media companies can and should moderate violent extremist content on-line with proper consideration for protected speech. They should also cooperate with law enforcement investigations.

To be clear: American citizens have a first amendment right to hold and espouse extreme ideologies.

However:

- There is no first amendment right to plot acts of violence
- There is no first amendment right to recruit others to commit acts of violence
- Foreign terrorists have no first amendment rights of any sort
- And social media companies are in no way compelled to allow terrorists or criminals to use their platforms.

In fact, they should face consequences if they knowingly do so, and that is something that Congress needs to act on.

I worked with Ranking Member Thompson to request that the Government Accountability Office (GAO) examine how social media and gaming companies report mitigating on-line content that promotes domestic violent extremism and the extent to which the FBI and DHS have developed goals and strategies for sharing information on the threat of domestic violent extremists with social media and gaming companies.

GAO produced its findings in January 2024, which included that neither DHS or FBI have developed such a strategy. They must do so, and the strategy must be comprehensive to include all forms of on-line radicalization, any incitement of violence, whatever the ideology behind it may be. It is my recommendation that the subcommittee continue today’s conversation with both representatives from the social media and gaming industry and the agencies so that we can explore real answers in combating on-line radicalization.

Mr. PFLUGER. I thank the Ranking Member. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 4, 2025

Terrorists’ use of on-line platforms to spread ideology, recruit members, and plan attacks is not novel. Neither is it new that individuals with extreme views seek out virtual communities of like-minded people and use the internet to express grievances and plan and live-stream attacks.

Nearly 10 years ago, minutes prior to a failed terrorist attack at the Curtis Culwell Center in Garland, Texas, one of the perpetrators posted a tweet with the hashtag #texasattack. One month following that attack, 9 African-American parishioners at Mother Emanuel in South Carolina were killed by a white-supremacist terrorist who self-radicalized on-line.

Next week will mark 5 years since a terrorist live-streamed on Facebook the attacks in which he heinously murdered 51 people at mosques in Christchurch, New Zealand. Unfortunately, the list of examples where extremism on-line and real-world violence converge goes on and on.

Although extremists have recently migrated to encrypted platforms, they largely use the same social media platforms as the average internet user. Research indicates that up to a third of internet users experience hate speech on-line.

The data is even more grim when it comes to on-line multiplayer games. According to a NYU study on extremists’ exploitation of gaming platforms, 41 percent of

survey respondents came across statements portraying a particular ethnic, gender, or religious group as inferior.

People encountered statements that included support for reprehensible ideas such as: violence against women is justified, a particular race or ethnicity should be expelled or eliminated, and using violence is justified or necessary to achieve a political aim.

A separate study by ADL found that 75 percent of teens and pre-teens experienced harassment in on-line multiplayer games in 2023 and that women and Black or African American gamers were the most harassed because of their identity.

This problem will only become more acute as the current owner of X, Elon Musk, is an extremist himself who has created an environment on his platform where pro-Nazi accounts that share Hitler speeches flourish.

Moreover, Musk profits from this kind of hateful content. The Center for Countering Digital Hate found that X “stands to make up to \$19 million a year from ads on just 10 toxic reinstated accounts,” and that accounts spewing hateful anti-LGBTQ rhetoric generate up to \$6.4 million per year for X in ad revenue.

Musk will not adopt any counter-extremist content policies or measures because that would affect his bottom line—never mind the fact that he also holds the keys to the Federal Government and will block any engagement between Government and industry on the issue.

Nevertheless, Committee Democrats will continue to examine the threats posed by on-line radicalization and engage the willing and socially responsible on-line and gaming platforms on solutions.

Mr. PFLUGER. I am pleased to have 4 distinguished witnesses before us today on this very important topic, some of whom have testified before this committee multiple times. I ask that our panel of witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. PFLUGER. Thank you. Let the record reflect that the witnesses have answered in the affirmative.

I will now formally introduce our panel of witnesses, starting with Dr. Daveed Gartenstein-Ross serves as a senior advisor on asymmetric warfare at the Foundation for Defense of Democracies. He is also the founder and chief executive officer of Valens Global. Welcome.

I would like to introduce now Dr. Aaron Zelin, who currently serves as a senior research fellow at the Washington Institute where he directs the Islamic State Worldwide Activity Map Project. I am also a graduate. As a fellow of the Washington Institute, it is good to see you.

I would like to introduce Mr. Daniel Flesch, who serves as a senior policy analyst for Middle East and North Africa at the Heritage Foundation. He previously served as an IDF paratrooper. Welcome.

Last, Dr. Kurt Braddock is an assistant professor of public communication in the School of Communication at American University. His research focuses on the strategies used by violent extremist groups to recruit and radicalize individuals targeted by propaganda. I thank everyone for being here. Thank you for your expertise. Thank you for your time.

We will now go to your opening statements. I know you have submitted written statements and if you would be so kind to summarize that at the 5-minute mark you will see the timer that counts down on that.

With that, Dr. Gartenstein-Ross, you are recognized for your opening statement.

**STATEMENT OF DAVEED GARTENSTEIN-ROSS, PH.D., SENIOR
ADVISOR ON ASYMMETRIC WARFARE, FOUNDATION FOR DE-
FENSE OF DEMOCRACIES**

Mr. GARTENSTEIN-ROSS. Thank you. Chairman Pfluger, Ranking Member Magaziner, distinguished Members of the subcommittee, on behalf of the Foundation for Defense of Democracies, thank you for the opportunity to testify on the important topic that the subcommittee is addressing today.

In my written testimony, I discuss what my colleagues at Valens Global and I call composite violent extremism, or CoVE. It describes individuals who blend elements from multiple ideologies, grievances, and sentiments without adhering to a single well-defined belief system. CoVE was not created by the on-line space. Ideologically-fluid extremists have existed for decades, but CoVE's increasing prevalence is tied to the digital age. The internet has transformed how violent extremist beliefs form, spread, and evolve.

We've seen this before. Technological shifts have repeatedly reshaped terrorism and we are now living through the next great technological shift, one that is more momentous than the advent of the internet itself. This shift is the rapid development of artificial intelligence, especially generative AI.

In 2018, I wrote an article titled "Terrorists are Going to Use Artificial Intelligence." At the time the idea was debated, but from our vantage point today, it's not a prediction. It's happening. We have seen a recurring pattern in terrorists employing new technologies. Terrorists first fail with a new technology, often giving way to iterative experimentation, adaptation, and eventual success. Social media, encryption, and drones all followed this trajectory, where initial crude attempts evolved into sophisticated applications, forcing governments to scramble for countermeasures. I call this pattern the violent non-state actor technology adoption curve, a consistent cycle in which terrorists initially struggle with new tools, but grow more adept at using them over time. We have seen this cycle unfold time and again. AI is not an exception. It is the next phase.

Terrorists don't need cutting-edge AI research labs to weaponize artificial intelligence. They only need access to the same widely-available AI tools that businesses and individuals are already using. As AI becomes more powerful, it will lower barriers to entry even further.

These are not hypothetical threats for the distant future. They are real today. Bad actors are already experimenting with AI to illustrate ways that AI and large language models can influence terrorist operations, there's propaganda and psychological warfare. AI can generate hyper-personalized extremist content, create deepfake recruitment videos, and use generative AI in recruitment agents that engage recruits dynamically. There's training and operational planning. Large language models can generate tactical handbooks, simulate security vulnerabilities, and coach extremists step by step through attack planning.

Some may assume that safeguards will prevent AI from being exploited. They won't. Large language models are already easy to jail-break, that is to manipulate into bypassing built-in safeguards against generating prohibited or harmful conduct. Even platforms

with thoughtful built-in restrictions can be manipulated. I don't want to explain the tactics to do so openly in this hearing, but I would be happy to generate basic jailbreaking techniques to any member who is interested.

Also, terrorists don't need ChatGPT. Other models, like China's DeepSeek, have fewer safeguards and are easier to weaponize. Governments and tech companies cannot rely on safety filters alone. A reactive approach is a losing strategy.

In the over 20 years that I have worked on counterterrorism, one pattern has been painfully clear: we are too often reactive rather than proactive. The same failure of imagination that the 9/11 Commission warned of is still at play. If we fail to recognize how AI will reshape terrorism and extremism, we risk being blindsided in ways that could dwarf the digital era mistakes of the past. That's why legislative efforts, such as the Gen AI Terrorism Threat Assessment Act are important. This bill would ensure that DHS conducts regular assessments of how terrorist organizations use encrypted, cloud-based communication platforms.

We need to monitor these trends rather than react when it's too late. If we aren't tracking how terrorists adapt to the technologies that are reshaping the world we will always be behind. We should act before the next breakthrough becomes the next disaster.

Again, I appreciate the opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Gartenstein-Ross follows:]

PREPARED STATEMENT OF DAVEED GARTENSTEIN-ROSS

MARCH 4, 2025

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee, on behalf of the Foundation for Defense of Democracies, I am honored to appear before you to discuss the important topic of the digital battlefield, exploring how terrorists use the internet.

This testimony will focus on an important trend in on-line radicalization that my colleagues and I have been tracking for several years, which we refer to as composite violent extremism (CoVE). Composite violent extremism describes cases where individuals engage in or support acts of terrorism or targeted violence despite adhering to a mixture of ideological beliefs, grievances, and prejudices that do not fit neatly into traditional categories of extremism. Unlike conventional ideological radicalization, where individuals are drawn into well-defined extremist movements, CoVE involves the blending of disparate ideological elements, often shaped by on-line environments, personal grievances, and cultural influences.

Understanding composite violent extremism is important because its growing prevalence presents new challenges for counterterrorism efforts, law enforcement, and policy makers—and because it provides new opportunities for violent extremists. Traditional frameworks for identifying and countering violent extremism often rely on clear ideological categories, yet instances of composite violent extremism do not fit neatly into these classifications. Extremists increasingly draw from multiple, sometimes contradictory, ideological sources.

This testimony will proceed in two major parts. First, it explains the concept of composite violent extremism in greater detail, outlining its defining characteristics and how it differs from traditional forms of ideological radicalization. Second, the testimony will explore the specific challenges that CoVE presents for terrorism prevention efforts. Understanding these dynamics is essential for developing more effective strategies to counter evolving threats in the digital battlefield.

In April 2022, Frank James opened fire on a New York subway train during rush hour, injuring 29 people. James's voluminous on-line writings left authorities, experts, and the media scratching their heads about his motives. Some reports called him a black nationalist, while others pointed to more disparate racist and misogyny-

nist ideas. James expressed hatred toward white people, Jews, and Latinos as well as anti-American sentiments and political grievances—none of which amounted to a coherent ideology or aligned with any distinct ideological movement. Complicating matters, James also struggled with mental illness.

Was James's shooting spree an act of violent extremism? If so, what kind? Scholars and practitioners have grappled with the increasing prominence of attackers like James who are ideologically idiosyncratic or even incoherent. In Congressional testimony from 2022, for example, FBI Director Christopher Wray spotlighted extremists who hold a “weird hodgepodge blend of ideologies,” noting that this trend is producing challenges in “trying to unpack what are often sort-of incoherent belief systems, combined with kind-of personal grievances.” Indeed, it can be difficult to unpack such belief systems because practitioners have often lacked the conceptual tools necessary to comprehend extremists who defy neat categorization.

FBI Director Wray described this phenomenon as “salad bar” extremism.¹ For well over half a decade, researchers have been trying to explain this phenomenon, employing terms like “ideological convergence,” “fused extremism,” “hybrid ideologies,” “fringe fluidity,” “ideology a la carte,” and “choose your own adventure” extremism—all of which have slightly different meanings and some of which only loosely relate to the FBI's concept of salad bar extremism.² Indeed, cases that fit the so-called salad bar paradigm (for which I offer an alternative terminology and concrete ways to understand) are challenging to conceptualize and categorize in large part because it can be difficult to discern motives amid complex interplays of disparate beliefs, interests, prejudices, grievances, and personal risk factors. This testimony thus explains the concept of composite violent extremism (CoVE).³

The increased prominence of these attacks that challenge established categories of violent extremism are of clear interest to this subcommittee. My contribution today is to offer a conceptualization of these vexing varieties of violent extremism and offer potential explanations for their apparently increased frequency.

BACKGROUND

In recent years, governments have begun expanding the scope of counterterrorism and prevention efforts to address ideologically ambiguous cases. DHS's 2019 Strategic Framework for Countering Terrorism and Targeted Violence (the CTTV framework) and the United Kingdom's mixed, unstable, and unclear (MUU) classification enable discussion of traditional terrorism alongside cases where an attacker lacks a clearly discernible ideology but where the intent and tactics resemble terrorism.

¹ FBI Director Christopher A. Wray, “A Review of the President's Fiscal Year 2023 Funding Request for the Federal Bureau of Investigation,” Testimony Before the Senate Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies, May 25, 2022. (<https://www.appropriations.senate.gov/hearings/a-review-of-the-presidents-fiscal-year-2023-funding-request-for-the-federal-bureau-of-investigation>); FBI Director Christopher A. Wray, “Threats to the Homeland,” Testimony Before the Senate Homeland Security and Government Affairs Committee, September 24, 2020. (<https://www.hsgac.senate.gov/hearings/--14-2020-threats-to-the-homeland>).

² See Julien Bellaiche, “Connecting the Fringes: Neo-Nazi Glorification of Salafi-Jihadi Representations Online,” Global Network on Extremism and Terrorism, August 24, 2021. (<https://gnet-research.org/2021/08/24/connecting-the-fringes-neo-nazi-glorification-of-salafi-jihadi-representations-on-line>); Ariel Koch, “The ONA Network and the Transnationalization of Neo-Nazi-Satanism,” *Studies in Conflict & Terrorism*, January 12, 2022, pages 1,172–1,199. (<https://www.tandfon-line.com/doi/full/10.1080/1057610X.2021.2024944>); Jesse J. Norris, “Idiosyncratic Terrorism: Disaggregating an Undertheorized Concept,” *Perspectives on Terrorism*, Volume 14, Number 3, June 2020. (<https://www.jstor.org/stable/26918296>); Milo Comerford and Sasha Havlicek, “Mainstreamed Extremism and the Future of Prevention” (London: Institute for Strategic Dialogue, 2021). (<https://www.isdglobal.org/wp-content/uploads/2021/10/ISD-Mainstreamed-extremism-and-the-future-of-prevention-3.pdf>); Daveed Gartenstein-Ross and Madeleine Blackman, “Fluidity of the Fringes: Prior Extremist Involvement as a Radicalization Pathway,” *Studies in Conflict & Terrorism*, January 7, 2019, pages 555–578. (<https://www.tandfon-line.com/doi/full/10.1080/1057610X.2018.1531545>); Paige Pascarelli, “Ideology a la Carte: Why Lone Actor Terrorists Choose and Fuse Ideologies,” *Lawfare*, October 2, 2016. (<https://www.lawfareblog.com/ideology-%C3%A0-la-carte-why-lone-actor-terrorists-choose-and-fuse-ideologies>); Kurt Braddock, Brian Hughes, and Cynthia Miller-Idriss, “The Post-9/11 Fight Against Extremism Must Take On Propagandists' Tricks, Not Just Ideology,” *MarketWatch*, September 11, 2021. (<https://www.marketwatch.com/story/the-post-9-11-fight-against-extremism-must-expand-to-attitudinal-inoculation-11631285779>).

³ I would like to acknowledge the work of 3 colleagues with whom I developed the concept of CoVE: Emelie Chace-Donahue, Madison Urban, and Andrew Zammit. See Daveed Gartenstein-Ross, Andrew Zammit, Emelie Chace-Donahue & Madison Urban, “Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism,” *Studies in Conflict & Terrorism*, March 29, 2023. (<https://www.tandfon-line.com/doi/full/10.1080/1057610X.2023.2194133>).

Coupling terrorism with this more ambiguously motivated violence is in part intended to strengthen prevention efforts. As DHS's strategy stated, these phenomena "overlap, intersect, and interact as problems" and thus "necessitate a shared set of solutions."⁴

DHS's 2019 CTTV framework was the first time a department-level U.S. strategy recognized terrorism and targeted violence within the same threat landscape. According to the framework, "targeted violence refers to any incident of violence in which a known or knowable attacker selects a particular target prior to the violent attack" (though it is worth noting that the framework also recommends the promulgation of an updated definition of the phenomenon of targeted violence).⁵ The CTTV framework goes on to note that "unlike terrorism, targeted violence includes attacks otherwise lacking a clearly discernible political, ideological, or religious motivation, but that are of such severity and magnitude as to suggest an intent to inflict a degree of mass injury, destruction, or death commensurate with known terrorist tactics."⁶

The U.K.'s Prevent Programme addresses traditional terrorism but goes a step beyond the CTTV framework by creating a specific category for less clearly discernible ideologies. The Prevent Programme includes the MUU classification for individuals referred to the program whose ideology or motivations challenge traditional categorizations.⁷ According to the program, MUU applies to cases "where the ideology presented involves a combination of elements from multiple ideologies (mixed), shifts between different ideologies (unstable), or where the individual does not present a coherent ideology yet may still be vulnerable to being drawn into terrorism (unclear)."⁸

Australian authorities have similarly demonstrated concern about ideologically unclear attacks, as shown by the proliferation of fixated threat assessment centers within State police counterterrorism functions. Fixated threat assessment centers aim to protect the public from individuals with an "obsessive preoccupation with a person or some idiosyncratic cause, which is pursued to a pathological degree" that can result in violence.⁹ These centers were not initially viewed as having a counterterrorism function, as they were largely concerned with individuals who were "fixated on a highly personal cause or grievance" rather than being ideologically motivated.¹⁰ The United Kingdom established a Fixated Threat Assessment Centre (FTAC) in 2006 due to persistent threats to the Royal Family from unstable individuals. This FTAC remained largely separate from the country's counterterrorism efforts. Australia's adoption of fixated threat assessment centers, which began with the establishment of a center in Queensland in 2013, was initially modeled on the United Kingdom's approach but increasingly came to involve a more explicit counterterrorism role.¹¹ For example, in 2017 both the New South Wales Police and Victoria Police established fixated threat assessment centers within their counterterrorism commands, showing that Australian counterterrorism approaches were broadening beyond a concern over individuals with clear ideological motivations.¹² In this way, the recognition that counterterrorism tools were relevant in this par-

⁴U.S. Department of Homeland Security, Strategic Framework for Countering Terrorism and Targeted Violence, September 2019, page 11. (https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf).

⁵Ibid., page 4.

⁶Ibid.

⁷Mark Townsend, "Anti-Terrorism Programme Must Keep Focus on Far Right, Say Experts," Guardian (UK), May 22, 2022. (<https://www.theguardian.com/uk-news/2022/may/22/anti-terrorism-programme-must-keep-focus-on-far-right-say-experts>)

⁸United Kingdom Home Office, "User Guide to: Individuals Referred to and Supported Through the Prevent Programme, England and Wales," December 5, 2024. (<https://www.gov.uk/government/publications/user-guide-to-individuals-referred-to-and-supported-through-the-prevent-programme-england-and-wales/user-guide-to-individuals-referred-to-and-supported-through-the-prevent-programme-england-and-wales>).

⁹Michele T. Pathé, Timothy Lowry, Debbie J. Haworth, Danae M. Webster, Melodie J. Mulder, Paul Winterbourne, and Colin J. Briggs, "Assessing and Managing the Threat Posed by Fixated Persons in Australia," The Journal of Forensic Psychiatry & Psychology, Volume 26, Number 4, May 5, 2015, pages 425–438. (<https://www.tandfon-line.com/doi/full/10.1080/14789949.2015.1037332>).

¹⁰Ibid., page 426.

¹¹Ibid., pages 425–438.

¹²Paul Farrell, "NSW Police Establish 'Fixated Persons' Unit to Help Counter Lone Wolf Terror Attacks," The Guardian (UK), April 25, 2017. (<https://www.theguardian.com/australia-news/2017/apr/26/nsw-police-establish-fixated-persons-unit-to-help-counter-lone-wolf-terror-attacks>); Premier of Victoria, "New Threat Assessment Centre to Keep Victorians Safe," October 3, 2017. (<https://www.premier.vic.gov.au/new-threat-assessment-centre-to-keep-victorians-safe>)

allel context resembles the U.S. Department of Homeland Security’s inclusion of targeted violence in the CTTV framework.

These policy and operational frameworks are significant steps, but more attention needs to be paid to understanding trends and common characteristics within targeted violence, MUU, and fixated threats. The CoVE framework, which I will now explain, accomplishes this. In 2022–23, I worked with a team of highly competent researchers—with the principal contributors being Emelie Chace-Donahue, Madison Urban, and Andrew Zammit—to better understand how cases like these fit within the violent extremism landscape. This team sought to develop a new conceptual framework with a clear overarching concept and a typology of subordinate concepts that disaggregated the different forms of violent extremism being observed. We sought to engage in a careful process of conceptualization, which began by identifying 94 cases of interest through existing datasets of violent extremists and mass shooters (including PIRUS and The Violence Project) along with less structured searches through Google. I will now outline our overarching conclusions.¹³

COMPOSITE VIOLENT EXTREMISM AND ITS SUBORDINATE CATEGORIES

The framework’s overarching concept is composite violent extremism, or CoVE. Composite, a term denoting something made up of various parts or elements, encompasses the concept of an amalgamated extremist outlook at the broadest level. The three subordinate categories in the typology demonstrate the different types of amalgamation that composite violent extremism covers. However, it is important to clarify what the concept of composite violent extremism does not cover.

At one end of a spectrum, composite violent extremism does not encompass violent extremists who possess a discernible ideology that is not combined with other sentiments or cooperation with adherents of other ideologies. This means the concept does not cover the phenomenon of fringe fluidity, wherein an extremist switches in full from one ideology to another. It also means the concept potentially does not cover cases that would be examples of unstable under the MUU criteria, unless the ideological shifts did not encompass the wholesale adoption of new ideology but instead involved amalgamation in some form.

At the other end, composite violent extremism does not cover violent actors who do not remotely demonstrate any ideological adherence, which meant that many mass shooters are excluded. The purpose of developing the overarching concept was to capture the apparent new paradigm of violent extremism that has clashed with existing categories used by scholars and practitioners, not to simply broaden the concept of violent extremism so much that it would encompass all mass killers with multiple non-ideological grievances or motivations. The concept is therefore deliberately described as composite violent extremism rather than composite violence.

Within this conception of composite violent extremism are 3 distinct categories based on levels of ideological discernibility and the centrality of beliefs to an individual’s worldview. Rather than attempting to categorize based on motive—which can be especially difficult to discern for extremists swayed by multiple beliefs—the CoVE framework categorizes based on expressed or exhibited beliefs that appear to influence an individual’s worldview and outlook. Many of the cases our team analyzed did not exhibit clear motives.

The categories of the typology are thus based on whether the individual expresses or exhibits easily discernible ideologies and the level to which expressed beliefs appear to be central to the individual’s worldview. Inferences about how central the beliefs expressed by an individual are to their worldview depend on factors such as the extent to which an individual expresses the belief (e.g., posting about it on-line once versus repeatedly), whether the individual is connected to groups or movements sharing the belief, whether their chosen target aligns with the belief, and whether the individual self-identifies as an adherent of the belief. Though categorizing in this way still involves a significant amount of subjectivity, we assess this process as a clear and rigorous way to discuss cases with high levels of ambiguity that might otherwise be left under-examined and uncategorized.

One reason that a level of subjectivity invariably remains in play is that the concepts used to develop these categories are themselves contested. This is most evident with the concept of ideology itself, which is “infamous for its superfluity of

¹³I believe that methodological explanations are out of place in Congressional testimony. For those who are interested in our methodological approach, see Daveed Gartenstein-Ross, Andrew Zammit, Emelie Chace-Donahue & Madison Urban, “Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism,” *Studies in Conflict & Terrorism*, March 29, 2023, pages 5–7. (<https://www.tandfon-line.com/doi/full/10.1080/1057610X.2023.2194133>).

meanings.”¹⁴ For the CoVE framework, ideology is defined as a set of beliefs that form a coherent outlook. This includes clearly-defined and discernible ideologies (e.g., neo-Nazism, jihadism) or any prejudice (e.g., racism, extreme misogyny) that shapes a worldview or lifestyle. In some cases, a subculture interest (e.g., extreme violence, “Columbiners”) can function as an ideology when it rises to the level of fixation and clearly shapes an individual’s behavioral patterns, worldview, and identity.¹⁵ Functional ideologies were only evident in roughly 10 percent of cases in the dataset. This is an unconventional definition of ideology, aimed at highlighting the reality that there are traditional ideologies as well as functional ideologies.

The CoVE framework also relies on specific definitions for sentiments, prejudices, grievances, subcultures, and fixations, as these terms are central to the defining requirements of the 4 categories of composite violent extremism. A sentiment refers to an expressed prejudice, grievance, or subculture interest. A prejudice refers to a distinct negative opinion that is expressed toward some defined outgroup. A grievance refers to a real or imagined wrong or other cause for complaint or protest, especially unfair treatment. A subculture refers to a community, often on-line, centered around a particular aesthetic or shared interest at odds with accepted norms (e.g., glorification of mass violence, Satanism). And a fixation refers to an obsessive interest in or feeling about someone or something.

With these underlying definitions provided, I will now elaborate on the different types of composite violent extremism. As I noted earlier, the 3 categories are ambiguous, mixed, and fused. The ambiguous category applies to cases where the perpetrator does not exhibit an easily discernible ideology based on existing buckets (e.g., anti-government extremism), but rather an amalgamation of sentiments. The mixed category applies to persons who appear to hold multiple easily discernible ideologies, potentially alongside other sentiments. The fused category applies to persons who appear to hold a core ideology but also exhibit other sentiments that make the case difficult to neatly categorize using existing buckets.

Ambiguous

This category applies to violent extremists whose worldview does not appear to be influenced by any clearly discernible ideologies, but rather by an amalgamation of prejudices, grievances, and subcultures that may undergird various extremist ideologies (e.g., misogyny, racism, antisemitism, conspiracy theories, or mass violence). This includes individuals who express some level of support for an ideology (e.g., posting Nazi symbols) alongside other prejudices that make it difficult or impossible to discern a central belief system.

One example is an August 2022 attack in Bend, Oregon. Ethan Miller—who opened fire in a grocery store, killing 2 people before taking his own life—exhibited a range of racist and misogynistic prejudices alongside other extreme sentiments. His journal and social media exhibited racist terms (against white people, black people, Jews, Asians, and Latinos) and expressions of hatred for “EVERYONE & EVERYTHING.” Though Miller rejected being labeled an incel (involuntary celibate), his writings exhibited hatred and threats toward women and an unfulfilled desire for a partner common among incel communities. Miller also railed against the government, police, religion, and technology. He claimed inspiration from the 1999 Columbine school shooting.¹⁶ The dizzying array of sentiments expressed by Miller, which resembled multiple ideologies but never amounted to coherent expressions of these ideologies, places him in the ambiguous category.

Another example of composite violent extremism that fits within the ambiguous category is Nikolas Cruz. On February 14, 2018, Cruz carried out a shooting at Marjory Stoneman Douglas High in Parkland, Florida, killing 14 students and 3 staff.¹⁷ Cruz’s worldview appears to have been influenced by a blend of prejudices, including

¹⁴Jonathan Leader Maynard, “Ideology and Armed Conflict,” *Journal of Peace Research* 56, Volume 56, Issue 5, April 8, 2019, page 637. (<https://journals.sagepub.com/doi/10.1177/0022343319826629>).

¹⁵“Columbiners” refers to the subcultures that display an obsession with the 1999 Columbine High School shooting in Littleton, Colorado. Columbiners generally evince a fixation with shooters Eric Harris and Dylan Klebold, expressing admiration for their actions and, at times, a desire to emulate them. See: Manny Fernandez, Julie Turkewitz, and Jess Bidgood, “For ‘Columbiners,’ School Shootings Have a Deadly Allure,” *The New York Times*, May 30, 2018. (<https://www.nytimes.com/2018/05/30/us/school-shootings-columbine.html>).

¹⁶“Oregon Safeway Shooter Claimed Inspiration from Columbine, Expressed Harsh Resentment Toward Women,” SITE Intelligence Group, August 29, 2022; Jessica McBride, “Ethan Miller, Bend Safeway Shooter: 5 Fast Facts You Need to Know,” *Heavy*, August 29, 2022. (<https://heavy.com/news/ethan-miller-bend-safeway-shooter>).

¹⁷Paul Murphy, “Exclusive: Group Chat Messages Show School Shooter Obsessed with Race, Violence and Guns,” *CNN*, February 18, 2018. (<https://www.cnn.com/2018/02/16/us/exclusive-school-shooter-instagram-group>).

racism and antisemitism (he posted repeatedly about his hatred for black people, Jews, Latinos, and Asians), Nazism and white supremacy (he had swastikas carved into his gun magazines and content on his phone referencing the KKK), Satanism (his backpack and photos found on his cell phone depicted the Satanist reference “666”), and a general interest in mass violence.¹⁸ Cruz read extensively about acts of mass violence, including the 2016 jihadist shooting at the Pulse nightclub in Orlando, the 2014 incel killings in Isla Vista, the 2012 Aurora movie theater shooting, and the 1999 Columbine attack.¹⁹ The sum of Cruz’s expressed sentiments does not point to a coherent ideology. Instead, his worldview appears to center around an amalgamation of prejudices and a general interest in violence.

Violent extremists who fit the ambiguous category can be identified by their expression (through their social media profiles, writings, and other sources) of an amalgamation of disparate prejudices, ideas, or grievances without a clearly discernible ideology. They often exhibit elements of an ideology but only inconsistently and interspersed with a variety of other beliefs or grievances, and their belief systems lack structure and consistency. Cruz, for example, lacked ideological consistency, piecing together disparate ideas—a determination supported by a court psychologist’s later findings.

Mixed

This category applies to violent extremists whose worldview appears to be influenced by multiple distinct and discernible ideologies alongside other prejudices, grievances, or subcultures. This includes individuals who adhere to multiple discernible ideologies or a combination of traditional and functional ideologies. Three individuals across 3 countries represent examples of the mixed category of composite violent extremism.

In April 2021, French authorities arrested 18-year-old Leila B. for plotting a terrorist attack targeting a church in Montpellier on Easter weekend.²⁰ During a search of her residence, authorities found material for constructing explosive devices and a journal filled with sketches of symbols associated with jihadism (e.g., a depiction of an ISIS member holding a decapitated head) and neo-Nazism (e.g., swastikas and depictions of Nazi soldiers), alongside other evidence that she was connected online with both ideological movements.²¹ She also exhibited a fixation on mass violence: She was obsessed with gore, Columbine, and serial killers.²²

¹⁸Ibid.; Law & Crime Network, Twitter, July 6, 2022. (<https://twitter.com/LawCrimeNetwork/status/1544716552641122308>); Marjory Stoneman Douglas Public Safety Commission, “Cruz Cell Phone Content and Internet Searches,” School Shooters.info, November 8, 2018. (<https://schoolshooters.info/sites/default/files/Cruz-Cell-Phone-Content-and-Internet-Searches.pdf>).

¹⁹Broward Sheriff’s Office, “Case Supplemental Report,” School Shooters.info, August 9, 2018. (https://schoolshooters.info/sites/default/files/Broward_Sheriffs_Office_Documents.pdf); Marjory Stoneman Douglas Public Safety Commission, “Cruz Cell Phone Content and Internet Searches,” School Shooters.info, November 8, 2018. (<https://schoolshooters.info/sites/default/files/Cruz-Cell-Phone-Content-and-Internet-Searches.pdf>); Terry Spencer, “Parkland School Shooter’s Swastika Carvings Are Focus of U.S. Court Fight,” The Times of Israel (Israel), July 7, 2022. (<https://www.timesofisrael.com/parkland-school-shooters-swastika-carvings-are-focus-of-court-fight/>); Gregory Richter and Ariana Richter, “The Incel Killer and the Threat to the Campus Community,” Security Magazine, March 12, 2019. (<https://www.securitymagazine.com/articles/89962-the-incel-killer-and-the-threat-to-the-campus-community>).

²⁰“Suspect Arrested Over Easter Linked to French Church Plot,” Associated Press, April 8, 2021. (<https://apnews.com/article/arrests-terrorism-europe-france-02d562667268b2f0158df8714fe423eb>); Jérémie Pham-Lê, “Je Voulais Mettre Cette Bombe dans l’Eglise: Révélation sur L’Adolescente de Béziers qui Projetait un Attentat [‘I wanted to put this bomb in the church’: revelations about the teenager from Béziers who planned an attack],” Le Parisien (France), April 17, 2021. (<https://www.leparisien.fr/faits-divers/je-voulais-mettre-cette-bombe-dans-leglise-revelations-sur-ladolescente-de-beziers-qui-projetait-un-attentat-17-04-2021-TH7TMLMZB5DXX-BQH5K7V7PTD54.php>).

²¹“Enquête pour ‘Association de Malfaiteurs Terroriste’ à Béziers : La Suspecte Mise en Examen et Ecrouée [Investigation for ‘terrorist criminal association’ in Béziers: the suspect indicted and imprisoned],” Le Monde (France), April 8, 2021. (https://www.lemonde.fr/societe/article/2021/04/08/enquete-pour-association-de-malfaiteurs-terroriste-a-beziers-des-elements-de-radicalisation-retrouves-chez-l-une-des-suspectes_6076012_3224.html); Pham-Lê, “Je Voulais Mettre Cette Bombe dans l’Eglise,”; Ronan Folgoas and Jérémie Pham-Lê, “‘Je Veux Faire Pire Que Columbine’: le Projetée Tuerie de Masse d’un Adorateur d’Hitler Déjoué par la DGSI [‘I want to do worse than Columbine’: the mass murder plan of a Hitler worshiper foiled by the DGSI],” Le Parisien (France), October 2, 2021. (<https://www.leparisien.fr/faits-divers/je-veux-faire-pire-que-columbine-le-projet-de-tuerie-de-masse-dun-normand-adorateur-dhitler-dejoue-par-la-dgsi-02-10-2021-KPUTTZCGGV-B5HKN4PYGAUWFT5M.php>).

²²Pham-Lê, “Je Voulais Mettre Cette Bombe dans l’Eglise.” Leila B.’s outlook appears to be based on a mix of ideologies blended with a general fixation on mass violence.

Andrea Cavalleri, arrested by Italian authorities in January 2021, also exhibited an interest in violent subcultures, writing about the “pleasure” he would feel carrying out a school shooting.²³ He was arrested for allegedly establishing and serving as the leader of a neo-Nazi organization “with the aim of recruiting volunteers and planning extreme and violent acts for subversive purposes . . . inspired by the American supremacist group Atomwaffen Division and the Nazi Waffen-SS.”²⁴ Beyond his evident adherence to neo-Nazi beliefs, Cavalleri was also a self-declared incel and stated his desire to carry out an attack motivated by this identity. At one point he wrote to a friend: “We will be the first Italian incels to take action.”²⁵ Cavalleri’s self-identification as an incel and his neo-Nazi ideology, along with attributing a desire to commit violence based on both, places him in the mixed category.

Finally, in October 2014, Zale Thompson attacked a group of NYPD officers with a hatchet, wounding 2 of them before being killed by police. The NYPD described the sentiments that Thompson expressed on social media as “anti-Western, anti-government, and in some cases anti-White,” and the FBI said he sought “inspiration from foreign terrorist sources like ISIS, but there is also evidence he was focused on black separatist ideology.”²⁶ Our analysis indicates that his outlook was influenced by two distinct and easily discernible ideologies: jihadism (he viewed extensive ISIS and al-Qaeda propaganda and posted on social media about jihadism) and black separatism (he had loose connections to black nationalist groups and advocated for black revolt).²⁷ Drawing heavily from these two ideological frameworks places him in the mixed category.

Violent extremists in this category can be identified by their expressions of multiple distinct and easily discernible ideologies through their behaviors (e.g., school behavioral records or arrests), writings (e.g., social media posts, manifestos), or personal belongings (e.g., books, flags). Leila B.’s inclusion in mixed was primarily due to her behaviors and active communication with members of the Atomwaffen group as well as ISIS. Another marker that an individual fits this category includes an expressed desire to attack based on different beliefs, such as Cavalleri stating he would like to be an incel attacker while also planning violence with neo-Nazis. Unlike Cavalleri, Thompson did not explicitly self-identify with both ideologies that we attributed to him, but his social media profile and writings exhibited adherence to multiple distinct ideologies.

²³ Paolo Frosina, “Il Delirio del Suprematista di Savona: ‘Hitler Come Cristo Guida Luce’. La Missione di una Guerra la Razziale ‘Contro Negri E Degenerati’ [The delirium of the supremacist from Savona: ‘Hitler as Christ guides light’. The mission of a racial war ‘against negroes and degenerates’],” *Il Fatto Quotidiano* (Italy), January 23, 2021. (<https://www.ilfattoquotidiano.it/2021/01/23/il-delirio-del-suprematista-di-savona-hitler-come-cristo-guida-luce-la-missione-di-una-guerra-la-razziale-contro-negri-e-degenerati/6075257>).

²⁴ Ministry of the Interior of Italy, Polizia di Stato, Press Release, “Terrorismo: Arrestato 22enne Suprematista e Negazionista [Terrorism: 22-year-old arrested for supremacist propaganda],” January 22, 2021. (<https://www.italypress.com/terrorismo-arrestato-un-22enne-per-propaganda-suprematista>).

²⁵ Francesco Marone, “Black Sun: A Case of Radicalization Between Neo-Nazism and Incel Ideology,” Italian Institute for International Political Studies (Italy), January 27, 2021. (<https://www.ispion-line.it/en/publicazione/black-sun-case-radicalization-between-neo-nazism-and-incel-ideology-29063>).

²⁶ “Transcript: Mayor de Blasio and Commissioner Bratton Provide an Update on the Assault of Two Police Officers,” NYC.gov, October 24, 2014. (<https://www1.nyc.gov/office-of-the-mayor/news/897-14/transcript-mayor-de-blasio-commissioner-bratton-provide-update-the-assault-two-police>); Jonathan Dienst, “Hatchet Attack on NYPD Officers Was ‘Act of Terror’: FBI Director,” NBC New York, November 17, 2014. (<https://www.nbcnewyork.com/news/local/hatchet-attack-nypd-officers-act-of-terror-fbi-director-james-comey/844450>).

²⁷ Alexandra Klausner, Kieran Corcoran, David Martosko, and Sophie Jane Evans, “Armed and Radicalized: Ranting ‘Self-Proclaimed Convert’ New York Hatchet Attacker was a ‘Terrorist’, Say Police,” *Daily Mail* (UK), October 24, 2014. (<https://www.dailymail.co.uk/news/article-2806731/Was-terror-attack-Police-probe-extremist-links-on-line-rants-New-York-hatchet-attacker-emerge-shot-dead-attack-group-cops-Queens.html>); “Terror Connection Not Ruled Out in Hatchet Attack, Police Say,” *Fox News*, November 21, 2015. (<https://www.foxnews.com/us/terror-connection-not-ruled-out-in-hatchet-attack-police-say>); “Black Identity Extremists Likely Motivated to Target Law Enforcement Officers,” FBI, August 3, 2017. (<https://privacysos.org/wp-content/uploads/2017/10/FBI-BlackIdentityExtremists.pdf>); Michael Schwirtz and William K. Rashbaum, “Attacker With Hatchet is Said to Have Grown Radical on His Own,” *The New York Times*, October 24, 2014. (<https://www.nytimes.com/2014/10/25/nyregion/man-who-attacked-police-with-hatchet-ranted-about-us-officials-say.html>); Priscilla DeGregory, Kevin Sheehan, and Kirstan Conley, “Black Panther Hails Ax Attack on Cops,” *New York Post*, October 27, 2014. (<https://nypost.com/2014/10/27/new-black-panther-group-hails-ax-attacker>).

Fused

This category applies to violent extremists whose worldview is based on one clearly discernible ideology, but who appear to fuse this core ideology with other distinct prejudices or grievances. In cases that fit this category, there are clear indications of a core ideology but the presence of other sentiments complicates what might otherwise be clean bucketing (e.g., the individual's on-line footprint points to a single ideology but also contains references to other distinct sentiments).

In 2019, authorities in the United Kingdom arrested Jack Reed for planning a terrorist attack.²⁸ He reportedly wrote a manifesto with a list of targets to attack, including schools, pubs, council buildings, post offices, and a synagogue.²⁹ Reed fundamentally embraced neo-Nazi ideology. His journal contained Nazi symbols and admiration for Hitler and he initially came to authorities' attention when he expressed support for the British neo-Nazi group National Action.³⁰ However, Reed's core neo-Nazi outlook appeared to be infused with Satanism (he described his Satanic beliefs on an on-line forum, calling himself an "immoral individual," and also had references in his journal to the esoteric Satanist group Order of Nine Angles) and mass violence (he reportedly expressed admiration for murderers Ian Brady and Charles Manson, and repeatedly visited websites related to the Columbine attack).³¹ Though it is clear that Reed fits the neo-Nazi label, his interests in Satanism and mass violence complicate the picture—possibly explaining why some of the targets on his list did not appear to have connections to his neo-Nazi beliefs.

Scott Beierle carried out a November 2018 shooting at a yoga studio in Tallahassee, Florida, killing 2 women and injuring 5 before killing himself. The U.S. Secret Service's National Threat Assessment Center used Beierle as a case study on misogynistic extremism, citing notes he left before the attack, his history of sexual harassment, and the content of the music he produced as evidence that incel and misogynistic beliefs fueled his worldview.³² In other words, extreme misogyny was Beierle's core ideology, as it was fundamental to his identity and worldview. However, Beierle also exhibited racism and white supremacist prejudices. The National Threat Assessment Center reported that he "openly admired Hitler and Aryan Nations" and that "other members of on-line social networks referred to him as a Nazi." A few of Beierle's song lyrics and descriptions also reveal racist and white supremacist sentiments (one titled "To Arms!" calls for people to take up arms to defend the homeland from immigrants).³³ While Beierle exhibited extreme misogyny as a core ideology, categorizing him solely as such would be inaccurate.

Deciding whether a case of violent extremism fits within the fused category depends on whether the extremists demonstrate a primary fixation on one ideological framework or belief that dictates their behaviors, writings, or personal belongings while still exhibiting some level of adherence to other sentiments. The fused category, as opposed to ambiguous or mixed, is for individuals whose worldview is primarily centered around one idea. For Beierle, his history of sexual harassment, attack target selection, and lyrics evidenced that extreme misogyny was central to his worldview even though he also expressed racist sentiments. In the case of Reed, his writings and admiration for Nazism were clearly central but he nonetheless also exhibited some behavior, writing, or personal belongings that suggests an interest or less central belief in Satanism. This category primarily exists to allow for nuance in evaluating attackers who are more complex upon closer examination than they appear on the surface.

²⁸ Lizzie Dearden, "One of UK's Youngest Terror Plotters Named After Losing Anonymity Battle," *The Independent* (UK), January 11, 2021. (<https://www.the-independent.com/news/uk/crime/neo-nazi-terror-plot-durham-jack-reed-b1785650.html>)

²⁹ Faye Brown, "Terrifying Drawings Found in Bedroom of Neo-Nazi, 16, Convicted of Terrorism," *Metro* (UK), November 20, 2019. (<https://metro.co.uk/2019/11/20/terrifying-drawings-found-bedroom-neo-nazi-16-convicted-terrorism-11189596>).

³⁰ *Ibid.*

³¹ Daniel De Simone, "Durham Teen Neo-Nazi Became 'Living Dead,'" *BBC* (UK), November 22, 2019, (<https://www.bbc.com/news/uk-england-tyne-50397477>); Brown, "Terrifying Drawings Found in Bedroom of Neo-Nazi."

³² National Threat Assessment Center, "Hot Yoga Tallahassee: A Case Study of Misogynistic Extremism" (Washington: U.S. Secret Service, March 2021). (https://www.secretservice.gov/sites/default/files/reports/2022-03/NTAC%20Case%20Study%20-%20Hot%20Yoga%20Tallahassee_0.pdf).

³³ See, for example, Scott Beierle, "American Whore," archived November 4, 2018. (https://web.archive.org/web/20181104002705mp_/https://pathofdefiance.com/american-whore); Scott Beierle, "I'm Dreaming . . .," archived November 4, 2018. (https://web.archive.org/web/20181104002542mp_/https://pathofdefiance.com/4-i-m-dreaming); Scott Beierle, "American Burden," archived November 4, 2018. (https://web.archive.org/web/20181104001746mp_/https://pathofdefiance.com/8-american-burden); Scott Beierle, "To Arms!" archived November 4, 2018. (<https://web.archive.org/web/20181104000923/https://pathofdefiance.com/to-arms>).

TOWARD EXPLANATIONS OF COMPOSITE VIOLENT EXTREMISM

The CoVE framework helps to both identify and disaggregate various acts of violent extremism that have challenged traditional categories in recent years. The apparently increased frequency of such incidents has gained attention from scholars and practitioners, prompting debate and the introduction of new policy frameworks in multiple countries. Why is this occurring?

The Information Environment and On-line Space

I believe that the information environment and on-line space is critical and relevant to the present hearing. Much of the current literature on the phenomenon we are referring to as CoVE highlights the importance of the information environment. As Jakob Guhl, Moustafa Ayad, and Julia Ebner note, multiple ideological trends have been “converging into ideologically elastic on-line subcultures.”³⁴ Cynthia Miller-Idriss and Brian Hughes argue that “material infrastructure enables the muddling of ideological rationales. . . . The infrastructure of digital communication technology, at both engineering and design levels, makes motley ideological blends increasingly common.”³⁵ There is an intuitive logic to this, as today’s information environment—which broadly refers to the full spectrum of actors and systems that produce, share, and use information—is widely understood to play some role in reshaping people’s beliefs and behaviors. The information environment is particularly impacted by on-line spaces (e.g., the internet and social media), which are quickly becoming the primary means by which people communicate and consume information. A 2021 Pew Research survey revealed that 86 percent of American adults get their news from digital devices, about half of whom read their news on social media.³⁶ The CoVE cases in the dataset had extensive on-line footprints and social media activity (on platforms like Facebook and YouTube) related to their beliefs, but not necessarily to a greater degree than the general population.

Social psychology research indicates that social media enables individuals to strategically “connect with like-minded others and distance themselves from people with conflicting belief sets.”³⁷ This would suggest that social media tends to be a place where people confine themselves to narrow viewpoints, rather than being exposed to a range of beliefs. But it is also true that people consume information in the current information environment like drinking from a firehose. The proliferation of news sites, social media platforms, and other on-line information channels readily available to internet users makes it easier than ever to passively consume and be shaped by vast amounts of information from a multitude of on-line actors and communities simultaneously. Though someone might join a certain on-line channel intentionally—based on their preexisting interests and proclivities—that person might just as easily stumble upon a forum or thread that piques a new interest. In some cases, it is possible to observe in retrospect how the on-line space creates an environment where worldviews are formed in both intentional and haphazard ways that produce idiosyncratic beliefs.

Lindsay Souvannarath—who plotted with a co-conspirator in 2015 to carry out a shooting at a mall in Halifax, Canada—described her radicalization process in a podcast interview, noting that it happened “by chance” through on-line communities. By her own account, Souvannarath became a National Socialist after she joined an on-line art community and connected with an artist who happened to be a National Socialist. Through this relationship, she gained exposure to the broader neo-Nazi community and came to accept this belief system.³⁸ Similarly, she initially became obsessed with Columbine because of on-line research she conducted for a short story she was writing. She wanted the story to include a shooting, and her research ex-

³⁴ Jakob Guhl, Moustafa Ayad, and Julia Ebner, “From The Vicious Cycle To Ideological Convergence,” VoxPol (Ireland), January 26, 2022. (<https://www.voxpol.eu/from-the-vicious-cycle-to-ideological-convergence>).

³⁵ Cynthia Miller-Idriss and Brian Hughes, “Blurry Ideologies and Strange Coalitions: The Evolving Landscape of Domestic Extremism,” Lawfare, December 19, 2021. (<https://www.lawfareblog.com/blurry-ideologies-and-strange-coalitions-evolving-landscape-domestic-extremism>).

³⁶ Elisa Shearer, “More than Eight-In-Ten Americans Get News from Digital Devices,” Pew Research, January 12, 2021. (<https://www.pewresearch.org/short-reads/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices>).

³⁷ Adrian Lüders, Alejandro Dinkelberg, and Michael Quayle, “Becoming ‘Us’ in Digital Spaces: How Online Users Creatively and Strategically Exploit Social Media Affordances to Build up Social Identity,” *Acta Psychologica*, Volume 228, August 2022. (<https://www.sciencedirect.com/science/article/pii/S0001691822001585?via%3Dihub>).

³⁸ Jordan Bonaparte, Interview with Lindsay Souvannarath, “The Story of Lindsay Souvannarath: Life Before Choosing Death,” Night Time, February 7, 2019. (<https://www.nighttimepodcast.com/episodes/lindsay-souvannarath-2>).

posed her to Columbine subcultures, where she built friendships and gained exposure to the writings of Eric Harris and Dylan Klebold.³⁹

These on-line influences culminated in an attack plan that exhibited elements of both Nazi ideology and a fixation with Columbine. Souvannarath and her co-conspirator, whom she met on-line, targeted a mall in “a protest against capitalism, against consumerism, against greed” in the vein of their National Socialist beliefs, and planned to end the attack “just like Columbine” by shooting themselves on the count of 3.⁴⁰ Fortunately, the attack was thwarted by the Canadian Border Services Agency when Souvannarath attempted to cross from the United States into Canada to carry out the plot.⁴¹

Lindsay Souvannarath’s case highlights how individuals can be drawn into certain beliefs based on the networks and subcultures they choose to engage with on-line, but people can also be shaped by the information they consume exogenous to their own actions. The information environment—social media and news media in particular—is rife with information intentionally produced and disseminated to subtly influence people’s beliefs and behaviors without their knowledge. Foreign adversaries—both state and non-state—are known to manipulate the information environment to exacerbate and exploit political, ideological, and other divides in American society. Adversaries benefit from advancing any narrative that challenges the status quo while driving further polarization. This type of “hostile social manipulation” or “virtual societal warfare” may generally lend itself to individuals being influenced by an amalgamation of inputs and narratives designed to stoke chaos and a sense of urgency to act.⁴²

Violence & Nihilism

Individuals primarily oriented toward violence could be attaching themselves to a range of beliefs that provide ideological frameworks or justifications for violence. Indeed, many of the cases we observed exhibited distinct interests in mass violence. Many extremists in the dataset extensively glorified mass violence and mass attackers, most commonly Eric Harris and Dylan Klebold (perpetrators of the 1999 Columbine shooting), Elliot Rodger (perpetrator of 2014 Isla Vista shootings), Timothy McVeigh (perpetrator of the 1995 Oklahoma City bombing), and Dylann Roof (perpetrator of the 2015 Charleston church shooting). At times, the relationship between an interest in violence and an ideology was symbiotic. Leila B., for example, told investigators that she adhered to jihadism and neo-Nazism to “justify” her “fascination with violent death.”⁴³ Still, this explanation raises further questions about whether and why individuals primarily oriented toward violence are a new or rising phenomenon, and whether this is novel to CoVE cases.

It is also possible that within the broader violent extremism ecosystem, violence and nihilism are becoming more central than ideology. Today’s violent extremists may be coalescing more around opposition to the current system by adopting any violent anti-status quo belief, and less around specific desired ideological outcomes. And, with the proliferation of existential threats and cynicism about the ability of any extant political system to deal with them, the reasons for the growth in nihilism are clear enough. From this vantage point, destroying the current system is of foremost importance, while determining what will replace it may be secondary or even

³⁹ Ibid.

⁴⁰ Jordan Bonaparte, Interview with Lindsay Souvannarath, “The Story of Lindsay Souvannarath_3 Lindsay, James, and the Valentine’s Day Massacre,” Night Time, February 15, 2019. (<https://www.nighttimepodcast.com/episodes/lindsay-souvannarath-3>).

⁴¹ The Canadian Border Services Agency detained Souvannarath based on an anonymous tip and lack of return ticket and luggage. See: Mack Lamoureux, “The Woman Who Plotted a Valentine’s Mass Murder Shares How the Internet Radicalized Her,” Vice, February 21, 2019. (<https://www.vice.com/en/article/eve54j/the-woman-who-plotted-a-valentines-mass-murder-shares-how-the-internet-radicalized-her>).

⁴² Michael Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica: RAND Corporation, 2019). (https://www.rand.org/pubs/research_reports/RR2713.html); Michael J. Mazarr, Ryan Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment* (Santa Monica: RAND Corporation, 2019). (https://www.rand.org/pubs/research_reports/RR2714.html).

⁴³ Jérémie Pham-Lê, “Je Voulais Mettre Cette Bombe dans l’Eglise’: Révélation sur l’Adolescente de Béziers qui Projetait un Attentat [‘I wanted to put this bomb in the church’: revelations about the teenager from Béziers who planned an attack],” *Le Parisien* (France), April 17, 2021, (<https://www.leparisien.fr/faits-divers/je-voulais-mettre-cette-bombe-dans-leglise-revelations-sur-l-adolescente-de-beziers-qui-projetait-un-attentat-17-04-2021-TH7TMLMZB5DXX-BQHSK7V7PTD54.php>).

irrelevant. Driven by a sense of urgency for change, violent extremists may be drawn to a range of belief systems that present perceived possibilities of success.

This explanation requires more study, but one case that illustrates the point is the Order of Nine Angles (O9A) and Ethan Melzer. O9A has a complex and often deliberately obscurantist belief system, but it can be understood as advocating for the destruction of Western society by any means necessary, encouraging adherents to bolster or even collaborate with movements like jihadism and neo-Nazism.⁴⁴ Melzer, a self-proclaimed O9A adherent, was involved in neo-Nazi channels on-line while plotting what he believed would be a jihadist attack against a U.S. military convoy in Turkey. He believed that this attack would draw the United States into another prolonged conflict and thus contribute to the collapse of the current U.S. political and social system. Further, a coalescence around nihilism and anti-status quo aesthetics could also explain why some factions of the white supremacist movement have adopted Satanism, which on its surface has little overlap with white supremacism.

Decentralization & Ideological Fragmentation

The on-line space is also contributing to the formation of decentralized extremist movements and networks, which may in turn decrease the ideological singularity and purity that comes with centralized command in an organized off-line group.⁴⁵ In the context of ever-evolving on-line movements and subcultures, it could be increasingly difficult for groups to maintain control or influence over ideology. Again, this is apparent in the white supremacist movement, where groups like Atomwaffen and National Action became fractured over the adoption of subcultures like Satanism that spread through the movement on-line.⁴⁶

Google's tech incubator Jigsaw, which conducts research on issues related to violent extremism, touched on this move away from formal groups to decentralized on-line networks in the February 2021 issue of its magazine *The Current*. Based on interviews with former extremists, the magazine discusses how on-line networks enable individuals to join the white supremacist movement without exclusively adopting the ideology. Jigsaw theorizes that "the internet lowers barriers for those curious about a supremacist idea to anonymously learn about it, lurk in supremacist spaces on-line, and eventually interact with others as part of loose, informal networks." One result is that this "enables supremacists to pick and choose which aspects of supremacist ideology resonate and engage selectively with those ideals . . . supremacists no longer have to find a group with which they fit; there is less friction to joining the distributed movement because they can retain idiosyncratic beliefs."⁴⁷

Terrorism experts have also discussed the importance of this shift and its impact on ideology and beliefs. In July 2020, Colin Clarke and Bruce Hoffman wrote an analysis of the "next American terrorist," emphasizing increasing decentralization and ideological fragmentation. Writing that "bureaucratic organizations with hierarchical leadership structures and clearly-defined objectives have been supplanted by loosely networked movements with amorphous goals that exist across the ideological spectrum," they suggest that "a confluence of ideological affinities is more powerful in inspiring and provoking violence than the hierarchical terrorist organizational structures of the past."⁴⁸ Ideological fragmentation seems like a natural extension of this decentralization and may play some role in how individuals come to adopt composite beliefs.

⁴⁴ Daveed Gartenstein-Ross and Emelie Chace-Donahue, "The Order of Nine Angles: Cosmology, Practice & Movement" (forthcoming in *Studies in Conflict & Terrorism*).

⁴⁵ Cynthia Miller-Idriss and Brian Hughes, "Blurry Ideologies and Strange Coalitions: The Evolving Landscape of Domestic Extremism," *Lawfare*, December 19, 2021. (<https://www.lawfareblog.com/blurry-ideologies-and-strange-coalitions-evolving-landscape-domestic-extremism>).

⁴⁶ Kelly Weill, "Satanism Drama is Tearing Apart the Murderous Neo-Nazi Group Atomwaffen," *The Daily Beast*, March 21, 2018, (<https://www.thedailybeast.com/satanism-drama-is-tearing-apart-the-murderous-neo-nazi-group-atomwaffen>); "Neo-Nazis Denounce Occultists Associated with Terror Plot, Favor Optics-Friendly Groups," *SITE Intelligence Group*, June 25, 2020; Lizzie Dearden, "Student Who Founded Neo-Nazi Terrorist Groups Convicted of Terror Offences," *The Independent* (UK), July 11, 2021. (<https://www.independent.co.uk/news/uk/crime/andrew-dymock-srn-sonnenkrieg-nazi-b1864321.html>).

⁴⁷ "Global, Connected and Decentralized," *The Current* 2 (2021). (<https://medium.com/jigsaw/global-connected-and-decentralized-41e496b44daf>).

⁴⁸ Bruce Hoffman, "The Next American Terrorist," *Cipher Brief*, July 2, 2020. (<https://www.thecipherbrief.com/article/united-states/the-next-american-terrorist>).

IMPLICATIONS FOR PREVENTION

The rise of composite violent extremism (CoVE) presents a unique set of challenges for terrorism prevention efforts. Traditional counterterrorism strategies were largely designed to address violent extremism rooted in well-defined ideological movements. Prevention frameworks were built on the premise that extremist beliefs and pathways to radicalization followed a structured, identifiable trajectory. CoVE disrupts these assumptions.

Prevention efforts can be broadly categorized into 3 levels:

1. *Publicly-Focused Initiatives.*—Awareness campaigns, media literacy programs, and efforts to promote critical thinking and community resilience.
2. *Community-Based Approaches.*—Collaboration with local leaders and organizations to monitor risk factors and conduct early interventions.
3. *Targeted Interventions.*—Focused efforts on individuals at risk of carrying out violence, including deradicalization, mentorship programs, and law enforcement action.

While these categories remain useful, CoVE presents distinct challenges that require adaptation:

1. *Distinguishing Genuine Threats.*—A core difficulty in countering CoVE is separating real threats from noise in an information space saturated with irony, trolling, and shock value content. Short-form media—including tweets, memes, TikTok, and YouTube shorts—has reshaped how extremists express their beliefs. While traditional extremists often articulate a coherent ideological framework, composite extremists may express disjointed and contradictory beliefs that nonetheless reinforce their intent to commit violence.

Practitioners must recognize that, despite their contradictions, composite violent extremists do have belief systems. Their worldviews, while fragmented, still have patterns, boundaries, and contours that can be analyzed. A critical challenge is determining when an individual's extreme expressions, even if incoherent, signal an intent to act. The failure to address this ambiguity can result in real threats being dismissed as unserious or performative.

2. *Avoiding Counterproductive Engagement.*—Prevention measures could backfire if they trigger unexpected grievances hidden in the complex worldviews of people at risk of succumbing to composite violent extremists. In targeted interventions, this uncertainty makes selecting a credible intervener—someone seen as trustworthy, competent, or impartial—more complex than it is for traditional ideological terrorists.

In an age of polarization, institutional efforts to inoculate against extremism (e.g., messaging campaigns) can themselves provoke grievances. Similar issues crop up in direct communication with composite violent extremists, such as one-on-one interventions. Misrepresenting a composite worldview with an imprecise blanket term like “white supremacism” could potentially undermine the trust necessary for effective deradicalization. After all, one aspect of building trust in the deradicalization context is providing individuals with the confidence that important aspects of their former extremist worldview are understood by the intervenors with whom they interact. The potential for misunderstandings in this regard is even greater in the context of CoVE.

3. *Tracking the Evolution of Fringe Beliefs.*—Many ideologies that today seem well-defined began as loose collections of grievances and subcultures. The incel (involuntary celibate) movement, for example, evolved from disparate on-line spaces into a structured belief system with its own terminology, grievances, and moral framework. Understanding when composite worldviews harden into new ideological movements is important for anticipating emerging threats.

Practitioners should track when composite violent extremists begin coalescing around shared narratives and self-reinforcing communities. While some CoVE cases may remain fragmented and individualized, others may lay the foundation for the next generation of extremist movements. Recognizing these patterns early is thus vital.

FINE-TUNING PREVENTION STRATEGIES

The challenges presented by CoVE do not necessitate a wholesale reinvention of terrorism prevention. The existing toolkit remains valuable, but fine-tuning is necessary to account for the ideological fluidity, digital dynamics, and radicalization pathways unique to CoVE.

Prevention must remain adaptive, nuanced, and aware of the changing nature of extremism. Addressing composite violent extremism requires refining intervention strategies, ensuring that risk assessments account for ideological ambiguity, and enhancing efforts to track how radical beliefs take shape in the digital era. By doing

so, we can build a more resilient system capable of identifying threats earlier, engaging at-risk individuals effectively, and preventing future attacks.

Mr. PFLUGER. Thank you very much.

The Chair now recognizes Dr. Zelin for his opening statement.

STATEMENT OF AARON ZELIN, PH.D., SENIOR RESEARCH FELLOW, THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY

Mr. ZELIN. Thank you, Chairman Pfluger, it's a great honor to do a hearing with you once again, Ranking Member Magaziner, and the distinguished Members of the subcommittee for giving me this opportunity to testify today on how terrorists use the internet today.

This is an important topic in light of the recent New Orleans attack. On that day, Shamsud-Din Jabbar was killed in a shootout with police after driving his Ford pickup truck with an Islamic State flag through a New Year's crowd on Bourbon Street, killing 14 and injuring 57. Prior to that attack, last October, he recorded a video of the French Quarter using his Meta smart glasses. Jabbar also expressed support for IS in videos posted to Facebook, researched the December 2016 car attack at the Christmas market in Germany, and pledged allegiance to the group before his deadly attack.

The following week, the Islamic State wrote an editorial in its weekly newsletter titled "We Were There," where it gloated over Jabbar's attack. It highlighted the group's influence and incitement capabilities and the piece also boasted that the perpetrator used American technology, referring to the Meta smart glasses. The piece concluded by once again urging Muslims in both Europe and the United States to carry out more terrorist attacks, highlighting how IS uses one attack to push yet another.

Jabbar's attack also falls in line with the Islamic State's instructional attack planning. In particular, in mid-November 2016, in IS English language magazine at the time called *Rumiyah*, it released an article titled "Just Terror Tactics," that discussed the use of pickup trucks, renting a vehicle if you did not have one, targeting pedestrian streets, and using a secondary weapon, among other things. In this case, Jabbar placed 2 coolers with explosive devices at 2 other locations in the city's French Quarter, and thankfully they didn't explode, also.

Finally, the article tells prospective attackers to find an appropriate way for announcing one's allegiance to the caliphate, and in this way we saw this with the Facebook post, as well as him using the ISIS flag on the car during the attack. This all shows that while this attack occurred in 2025, in many ways examples and guidance literature from almost a decade ago now that remains accessible on-line has a long shelf life, and not enough is still being done to make sure that potential attackers do not have access to such content on-line.

Beyond traditional propaganda efforts to recruit and incite, there are more recent innovations related to crypto, live streaming and AI. Regarding crypto, based on data collected for the Washington Institute's Islamic State Worldwide Activity Map, since 2015, there have been at least 36 arrest cases globally related to jihadi use of cryptocurrencies, with 13 of them happening in 2024 alone, illus-

trating a huge uptick in the past year. It's likely that there are other cases as well that we just don't know about because it didn't come within the judicial system.

This is not theoretical either. Last year in April, the FBI arrested an 18-year-old plotting an attack on churches in Idaho, and as part of his plot, he attempted to donate \$11,000 to the Islamic State using the Monero cryptocurrency, which they promote in one of their English language magazines nowadays.

Beyond traditional social media platforms, there's also been a rise in the use of TikTok by IS supporters. Based on data from the Islamic State Worldwide Activity Map, there have been 15 arrest cases since 2023 that have shown that the arrestees have been involved in one way or another with IS propaganda on TikTok. Just last week, for example, in Minneapolis, a man was arrested by the FBI and charged for attempting to provide material support to IS in Somalia, but as part of the investigation he also actually praised the perpetrator of the IS-inspired attack in New Orleans on TikTok itself.

As for live streaming, it could have been much more of a psychological effect nationally if the New Orleans attacker had live streamed his attack on his Meta glasses through Facebook instead of only using it for reconnaissance purposes. We've seen past attacks in Europe from IS supporters using live streaming either during or after the attack, so it's not something theoretical.

Last, there are worries that generative AI could be exploited by terrorists. Thus far, at least amongst jihadis, beyond propaganda, there has not been much evidence that it's used in terms of—for deadly effects, but as Daveed mentions, it's definitely a possibility in the future. There have been incoherent conversations by IS supporters on-line only in last 2 weeks or so about the Chinese application DeepSeek and how they could potentially exploit it. It's, of course, too soon to see how that might evolve, but it's definitely troubling.

Beyond the specifics of how terrorists might exploit technology, policies related to technology and platforms also have a role in providing space, making it very difficult to use. In recent years, due to controversies related to censorship within the West politically, there have been a backlash related to moderating content on-line, even if it's extremist in nature. This should not be overblown, however, since jihadi use is still not as wide-spread on mainstream platforms as it was a decade ago, but in a relative sense, there is greater space for jihadis to exploit these platforms than in the past 2 or 3 years.

I know time is short, so I'll just briefly mention that the U.S. Government should urge technology companies and social media platforms to redouble their efforts at content moderation related to the jihadi movement and go beyond just Arabic and English to nascent spaces of greater exploitation in recent years, with languages in Africa and Central Asia in particular. Although there have been recent calls to cut funding and jobs across the U.S. Government, cutting ones related to tracking on-line jihadi recruitment and attack plotting could undermine future security and lead to greater risks at home and abroad. No one, of course, wants to see yet an-

other successful attack like the one we recently saw in New Orleans. Thank you.

[The prepared statement of Mr. Zelin follows:]

PREPARED STATEMENT OF AARON ZELIN

MARCH 4, 2025

Thank you Mister Chairman and Members of the committee for giving me the opportunity to testify today on how terrorists use the internet and on-line networks for recruitment and radicalization. This is an important topic in light of the recent New Year's Eve attack in New Orleans. On that day, Shamsud-Din Jabbar was killed in a shootout with police after driving a Ford pickup truck with an Islamic State (IS) flag through a New Year's crowd on Bourbon Street, killing 14 and injuring 57. Prior to the attack, he visited New Orleans twice, on October 31 and November 10 last year. During his October trip, he recorded a video of the French Quarter using smart glasses from Meta. Jabbar also expressed support for IS in videos posted to Facebook, researched the December 2016 car attack at a Christmas market in Germany, and pledged allegiance to the group shortly before the attack.¹

The following week, the Islamic State wrote an editorial in its weekly newsletter called *al-Naba*, titled "We Were There!," where it gloated over Jabbar's attack.² In the editorial, it highlighted the group's influence and incitement capabilities. The piece also boasted that the perpetrator used American technology, referring to the Meta smart glasses he employed to conduct reconnaissance. The piece concluded by once again urging Muslims in Europe and the United States to carry out more terrorist attacks. Highlighting how IS uses one attack to push for a new one and creates a virtuous cycle from its perspective. That is why it is not surprising that Jabbar himself, prior to his own attack, researched a prior IS attack: the December 2016 Christmas Market car ramming attack in Berlin that killed 12 and injured 48.³

Jabbar's attack also falls in line with Islamic State instructional attack planning. In particular, in mid-November 2016, in IS's English language magazine at the time called *Rumiyah*, it released an article titled "Just Terror Tactics" that provided guidance on the best way to kill as many of their enemies as possible.⁴ It says "the type of vehicle most appropriate for such an operation is a large load-bearing truck." Jabbar did this with the pickup truck. The article also highlights that if one doesn't have the wealth, it suggests renting a vehicle, again Jabbar did this as well. Further, it suggests specific targets, with one of them being pedestrian-congested streets, again something Jabbar followed. The article also suggested that an attacker can use a secondary weapon. In this case, Jabbar placed 2 coolers with explosive devices at 2 other locations in the city's French Quarter. Finally, the article tells prospective attackers to find "an appropriate way . . . for announcing one's allegiance to the Caliphate." Not only did Jabbar do this with his pledge of allegiance on Facebook, but also by raising the Islamic State flag on the truck he used during the attack. This all shows that while this attack occurred in 2025, in many ways examples and guidance literature from almost a decade ago that remains accessible on-line has a long shelf life and that not enough is still being done to make sure that potential attackers do not have access to such content on-line.

BACKGROUND

Unfortunately, none of this is new. Since the commercial internet came about, jihadis have been there in parallel. The first known jihadi presence on the internet can be traced back to 1991, with the Islamic Media Center (IMC). Al-Qaeda's official debut dates to February 2000, with the creation of *maalemaljihad.com*. This was followed in March 2001 by *alned.com*, which was active through mid-July 2002.⁵ In

¹"IS-Inspired Attacker Killed After Driving Through Crowd in New Orleans," Islamic State Worldwide Activity Map, January 1, 2025, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/4029>.

²The Islamic State, "al-Naba' Newsletter Issue #477," January 9, 2025, <https://jihadology.net/2025/01/09/new-issue-of-the-islamic-states-newsletter-al-naba-477>.

³"Attack on Berlin Christmas Market," Islamic State Worldwide Activity Map, December 20, 2016, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/989>.

⁴The Islamic State, "Rome Magazine Issue #3," November 11, 2016, <https://jihadology.net/2016/11/11/new-release-of-the-islamic-states-magazine-rome-3>.

⁵Abdel Bari Atwan, *The Secret History of al-Qaeda*, London: Saqi Books, 2006, pp. 127; Patrick Di Justo, "How Al-Qaida Site Was Hijacked," Wired Online, August 10, 2002, <http://www.wired.com/culture/lifestyle/news/2002/08/54455>.

the summer of 2001, al-Qaeda created a media arm, al-Sahab Media Production Establishment, and released its first video, “The Destruction of the American Destroyer [USS] Cole.” Several other websites at the time were not directly connected with al-Qaeda, but sympathized with its jihadi worldview, including Azzam Publications, al-Tibyan Publications (which had one of the earliest jihadi-leaning, English-language, interactive forums), and Sawt al-Qawqaz.⁶

Since then, the jihadi movement has taken advantage of new on-line technologies at every turn to spread its message, recruit individuals to fight abroad, incite or help plan attacks, and raise money. For example, the onset of interactive forums in the mid-2000’s, concurrent with the rise of Abu Mus’ab al-Zarqawi and the Iraq jihad, shattered the elitist nature of jihadi communications. Web forums still offered administrators (who were often directly connected with al-Qaeda) extensive influence over what was posted because they could delete threads or ban members. But individual forum members, not directly connected to al-Qaeda, could not only view what was posted by administrators, but also comment and post their own content as well.⁷ Mustafa Setmariam Nasir, better known by his nom de guerre Abu Mus’ab al-Suri, called for producing jihadi media in languages other than Arabic, including English, and devising messages that appealed more to the masses. The popularization of the on-line jihadi movement empowered organizations dedicated to translating material, most of which was still produced in Arabic. The Global Islamic Media Front (GIMF), established in August 2004, was a key innovator in this regard, and could trace its roots all the way back to June 2001.⁸

After this, Web 2.0 innovations and the creation of social media platforms (blogging, Facebook, YouTube, and Twitter) flattened control over the production of on-line jihadi media. Social media platforms enabled global jihadi entrepreneurs to share news items, original articles and essays, tribute videos, and anashid (Islamically sanctioned a cappella music). The newer technologies, at that time, lowered the bar for participation, making the involvement of low-level or non-jihadis in on-line conversation a new feature of the global jihadi movement. Those so inclined could talk about jihad all day on the Web, even if they were geographically dispersed. This was not possible beforehand.⁹

As a consequence, when the Islamic State eclipsed al-Qaeda in the mid-2010’s they used this to deadly effect.¹⁰ To further their message they would create innocuous hashtag aggregators yet only post their propaganda, create hashtag targeting bots, have multiple backup accounts in case they were taken down, and build the Fajr al-Basha’ir app.¹¹ The latter let members and supporters connect to it and thereby whenever the app tweeted something it would automatically be posted by those that signed up for it onto their own account. The breadth of IS’s on-line Twitter campaign was unprecedented. However, this would not last, due to massive complaints by countries reeling from the Islamic State’s on-the-ground successes in Iraq and Syria and tens of thousands of foreign fighters being recruited to join their ranks.¹²

That led Twitter (and all the other main technology companies) to originally establish their Trust and Safety teams. This led to a crackdown on IS networks in 2015 by going after IP addresses and those within their follower networks.¹³ This helped also establish the Global Internet Forum to Counter Terrorism (GIFCT), which established a consortium of Western technology companies to work together to take down terrorist content by sharing digital fingerprints (or hashes) of different

⁶For more see: Hanna Rogin, “Al-Qaeda’s on-line media strategies—From Abu Reuter to Irhabi 007,” Norwegian Defence Research Establishment (FFI), January 12, 2007, <http://rapporter.ffi.no/rapporter/2007/02729.pdf>.

⁷Gordon Corera, “Al-Qaeda’s 007,” The Times, January 16, 2008, <https://www.thetimes.com/article/al-qaeda-007-c2sx2r5bdgc>.

⁸Rogin, “Al-Qaeda’s on-line media strategies,” pp. 56.

⁹Aaron Y. Zelin, “The State of Global Jihad Online,” New America Foundation, February 2013, <https://www.newamerica.org/future-security/policy-papers/the-state-of-global-jihad-online>.

¹⁰Aaron Y. Zelin, “Picture Or It Didn’t Happen: A Snapshot of the Islamic State’s Official Media Output,” Perspectives on Terrorism, Volume 9, Number 4, August 2015, <https://www.jstor.org/stable/26297417?seq=1>.

¹¹J.M. Berger, “How ISIS Games Twitter,” The Atlantic, June 16, 2014, <https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856>.

¹²Michael Isikoff, “Twitter under pressure to act more aggressively against terrorists,” February 18, 2015, <https://www.yahoo.com/news/amhtml/politics/twitter-under-pressure-to-act-more-aggressively-114435221601.html>.

¹³“An update on our efforts to combat violent extremism,” Twitter, August 18, 2016, https://blog.x.com/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.

types of content (pictures, audio, videos, etc.).¹⁴ As a consequence, IS and the jihadi movement shifted to the encrypted messaging application Telegram in August/September 2015, which also had a broadcast feature that allowed anyone to follow official IS and other groups' channels.¹⁵ Telegram never had the same utility as Twitter since it couldn't just reach anyone randomly as Twitter had, one had to know where to go ahead of time to find the content. This takedown cycle eventually happened again on Telegram when Europol convinced the company to go after jihadi accounts, which led to a huge purge in November 2019.¹⁶ As a consequence, both IS and AQ networks established their own decentralized forums using block chain technology on RocketChat to make it more difficult for content to be taken down. To this day, both RocketChat forums remain on-line.¹⁷

HARNESSING THE INTERNET TODAY

While al-Qaeda still operates its RocketChat forum, the Islamic State's on-line ecosystem and infrastructure is far more diverse and sophisticated than only its own RocketChat forum. In addition to that, IS also established its own Cloud-based archive of its historical propaganda called Obedient Supporters.¹⁸ Moreover, in recent years, it has also established a number of traditional websites. In some ways, a return to the beginning of the internet in the 1990's and early 2000's since it was much harder to operate on mainstream social media platforms. To make these websites more difficult to take down, they jump domain names often using different country codes to hide in plain sight. To make it even more complicated, they have also developed mirrored versions of these websites on the Dark Web, which can only be accessed using a Tor browser and an Onion router link. Each website also provides a specific purpose to try and break up where all the content is so as to disperse it to make their on-line network more resilient over time. They do this by having a repository website called Fahras al-Ansar, which is based in South Africa right now at least, that shares the last links for each site that are currently available on-line on the surface web and on the Dark Web.¹⁹ The main website that has been most active recently is called Sah al-Wagha, which shares the latest IS attack claims of responsibility, videos, and weekly newsletter al-Naba.²⁰

The latter website is where one would find official media content from IS, which comes directly from its Central Media Diwan (Administration), which today includes al-Furqan Media, Amaq News Agency, Provincial Media Centers, among other lesser-used outlets today. Other websites and the RocketChat forum also disseminate "unofficial" auxiliary propaganda. These are not created by the Central Media Diwan, but by members of the group in their own capacity and work with on-line supporters of the group. These include media outlets such as al-Batar Media, al-Saqri Media, al-Dir'a al-Sunni Media, Sirat al-Khilafah, al-Adilat Media, etc. The next layer under this is IS's translation collective, called Fursan al-Tarjuma, which helps disseminate all of its official propaganda into dozens of languages.²¹ Again, this is "unofficial" insofar as the Central Media Diwan is not involved, but rather members of the group in their own capacity and on-line supporters take part in it. These outlets today include Halammu (English), Nida al-Haqq (Urdu), al-Aza'im (Pashto, Uzbek, Tajik, Farsi), Markaz al-Nur (French), al-Tamkin (Bengali, Indonesian), Arshad (Russian), al-Bahiriyah (Hausa), al-Basha'ir (Dhivehi), Maydan (Turkish), Rastara (Kurdish), Fakhr al-Ummah (Albanian), Sawt al-Andalus (Span-

¹⁴ "Global Internet Forum to Counter Terrorism: an update on our efforts to use technology, support smaller companies and fund research to fight terrorism on-line," June 18, 2018, <https://gifct.org/2018/06/18/global-internet-forum-to-counter-terrorism-an-update-on-our-efforts-to-use-technology-support-smaller-companies-and-fund-research-to-fight-terrorism-on-line>.

¹⁵ "IS exploits Telegram mobile app to spread propaganda," BBC News, October 7, 2015, <https://www.bbc.com/news/technology-34466287>.

¹⁶ "Europol and Telegram take on terrorist propaganda on-line" Europol, November 22, 2019, <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-on-line>.

¹⁷ Peter King, "Analysis: Islamic State messaging on RocketChat still on-line after 7 months," BBC Monitoring, August 9, 2019, <https://monitoring.bbc.co.uk/product/c200zjhjz>; "Veteran jihadist outlet uses RocketChat for al-Qaeda propaganda," BBC Monitoring, December 6, 2019, <https://monitoring.bbc.co.uk/product/c201akwr>.

¹⁸ Miron Lakomy, "In the digital trenches: Mapping the structure and evolution of the Islamic State's information ecosystem (2023–2024)," Media, War & Conflict, August 24, 2024, <https://journals.sagepub.com/doi/10.1177/17506352241274554>.

¹⁹ Ibid.

²⁰ "Briefing: New archive of official IS material appears on-line," BBC Monitoring, October 28, 2024, <https://monitoring.bbc.co.uk/product/b0002o3c>.

²¹ Lucas Webber and Daniele Garofalo, "Fursan al-Tarjuma Carries the Torch of Islamic State's Media Jihad," Global Network on Extremism and Technology, June 5, 2023, <https://gnet-research.org/2023/06/05/fursan-al-tarjuma-carries-the-torch-of-islamic-states-media-jihad>.

ish), and al-Qital (Hindi). Illustrating the breadth of languages IS has access to for spreading its message, ideology, and incitement all across the world. At the height of IS's territorial control in Iraq and Syria a decade ago, they translated their content into even more languages, illustrating that even if it is relatively weaker today, it is still quite resilient and there are enough people interested in its worldview to assist in these endeavors.

EMERGING TECH: CRYPTO, LIVE STREAMING, AND AI

Beyond traditional propaganda efforts to recruit and incite, due to the greater reach and ease of use of cryptocurrencies, there has been a huge uptick in its use by jihadi groups, its supporters, and those involved in attacks abroad. For example, on an official level, beginning in December 2023, the Islamic State's Khurasan Province (ISKP), based out of Afghanistan and Pakistan, began promoting its own wallet for the Monero cryptocurrency to help fund its efforts locally and also as a conduit to pay for external operations abroad. These promotions for ISKP's Monero wallet first appeared in its official English-language magazine the *Voice of Khurasan*.²² The utility of a cryptocurrency like Monero is that it is more difficult to track the movement of money through the wallet like other cryptocurrencies. Thus making it more secure, which in of itself for normal activity, on the surface, would be fine, but for a terrorist group, not ideal. Since then, ISKP has promoted a number of different wallets in subsequent issues of its *Voice of Khurasan* magazine. This is not theoretical either, back in April 2024, the FBI arrested 18-year-old Alexander Scott Mercurio who pledged allegiance to the Islamic State and plotted to attack churches in Coeur d'Alene, Idaho. As part of this plot, he confided in an undercover agent that he wanted to donate his money (\$11,000) ahead of this attack to ISKP using Monero.²³ A similar case in the United Kingdom occurred as well with an even larger donation attempt of £16,000.²⁴ Based on data collected for my Islamic State Worldwide Activity map, since 2015, there have been 36 arrest cases globally related to jihadi use of cryptocurrency, with 13 of them happening in 2024 alone, illustrating a huge uptick in only the past year. And these cases are only known cases that have come through judicial manners, not those that were not detected.

Beyond traditional American social media platforms, there has also been a rise in use of TikTok by supporters of IS. This is not surprising since it has become ubiquitous amongst Gen Z individuals. While the trend likely began earlier, based on data from my Islamic State Worldwide Activity map, there have been 15 arrest cases that began in 2023 that have shown the arrestee to have been involved in one way or another with IS propaganda on TikTok, either sharing it themselves or watching it. Just last week, Minneapolis resident Abdisatar Ahmed Hassan was arrested and charged for attempting to provide material support to the Islamic State. As part of the investigation, he actually praised the perpetrator of the IS-inspired attack in New Orleans on TikTok on January 1, 2025.²⁵ Highlighting how one attack could inspire others to either plot their own attack or to try and travel abroad to fight with IS in a warzone, as Hassan attempted to do with IS in Somalia.

There are also other technological-related issues that terrorists could attempt to exploit, including live-streaming their attack. It could have had much more of a psychological effect nationally, if the New Orleans attacker had live-streamed his attack on his Meta glasses through Facebook instead of only using it for reconnaissance purposes. However, such use is not unprecedented. Back in June 2016, Islamic State attacker Larossi Abballa, broadcast the aftermath of his attack on a French police captain and his partner, in real time on Facebook Live and remained on-line for almost 12 minutes.²⁶ A copy of the recording was downloaded and later

²²The Islamic State's Wilayat Khurasan, "Voice of Khurasan Magazine Issue #31," al-Aza'im Media, December 22, 2023, <https://jihadology.net/2023/12/22/new-magazine-issue-from-the-islamic-states-wilayat-khurasan-voice-of-khurasan-31>.

²³"Idaho Teen Arrested For Plotting Church Attacks," Islamic State Worldwide Activity Map, April 6, 2024, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/3228>.

²⁴"Luton Man Arrested for Sending Cryptocurrency to ISKP," Islamic State Worldwide Activity Map, March 13, 2024, <https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/4191>.

²⁵"Minneapolis Man Arrested for Attempting to Provide Material Support to ISIS," Department of Justice, February 28, 2025, <https://www.justice.gov/usao-mn/pr/minneapolis-man-arrested-attempting-provide-material-support-isis>.

²⁶Caitlin Dewey and Sarah Parnass, "For the first time, an alleged terrorist has broadcast a confession in real time on Facebook Live," Washington Post, June 14, 2016, <https://www.washingtonpost.com/news/the-intersect/wp/2016/06/14/for-the-first-time-an-alleged-terrorist-has-broadcast-a-confession-in-real-time-on-facebook-live>.

reposted via IS's official media outlet Amaq News Agency, since it was taken down from Facebook 11 hours after its recording.

In addition to that, there are also worries that Generative Artificial Intelligence (AI) could be exploited by terrorists. However, thus far, at least among jihadis, there has not been much evidence that they have used it yet to deadly ends. However, that does not necessarily mean they couldn't in the future. For now, it has mainly been used by followers to create on-line graphics to promote the same kind of content they would have previously using Photoshop. Even if this appears to have less stakes, it does lower the bar for those to make content and interact more deeply with the ideology and worldview since one doesn't need the same level of skill set as someone that knows how to use Photoshop, something which takes training and a lot more time. However, there have been inchoate conversations by IS supporters on Rocketchat beginning a few weeks ago, related to the Chinese application Deepseek and how they could potentially exploit it. It is too soon, however, to know how that might evolve.²⁷

MODERATION BACKSLIDING

Beyond the specifics of how terrorists might exploit technology, policies related to technologies and platforms also have a role in providing space or making it very difficult to use. As noted above, beginning in 2015, there was a much greater focus by major technology companies to moderate their platforms so that terrorists couldn't exploit them. While the moderation was in no way perfect vis-à-vis jihadis on-line, overall, it curbed usage on mainstream platforms at a good enough rate that it was not noticeably affecting random people as it easily had in the 2013–15 time period. However, in recent years, due to controversies related to alleged censorship within the West politically, there has been a backlash to moderating content even if it is extremist in nature. As a consequence, beginning with Elon Musk's purchase of Twitter, which is now X, the level of content moderation in general, and related to the jihadi movement specifically has backslid.²⁸ It should not be overblown, however, since it is not as widespread as it was in 2015 prior to the offensive policies against jihadis, but in a relative sense, there is greater space for jihadis to exploit platforms in recent years.²⁹ It should be noted that this is not just an issue with X, but has Mark Zuckerberg's Meta social media platforms as well, including Facebook, Instagram, and WhatsApp as well as the aforementioned TikTok. Yet unlike a decade ago, much of these relative capabilities by IS networks online are by supporters of the group and not at the official level.³⁰

RECOMMENDATIONS

- The U.S. Government should urge technology companies and social media platforms to redouble their efforts at content moderation related to the jihadi movement. In particular, beyond only Arabic and English content, these platforms need to beef up their moderation in languages that are increasingly used as the center of gravity of the jihadi movement on-line such as multiple languages in Africa and Central Asia for example.
- Although there have been recent calls to cut funding and jobs across the U.S. Government, cutting ones related to tracking on-line jihadi recruitment and attack plotting could undermine future security and lead to greater risks at home and abroad. At a time, when greater resources are put toward power competition and less resources are given to counterterrorism, eliminating even more resources in this field could provide more opportunities for adversarial jihadis and entrepreneurial supporters of the movement to take advantage and attack the homeland more easily.

²⁷ "Users on pro-IS chat group begin discussing DeepSeek," BBC Monitoring, February 19, 2025, <https://monitoring.bbc.co.uk/product/b0003e3h>.

²⁸ "Musk admitted to firing 80 percent of Trust and Safety Engineers at Twitter," January 12, 2024, <https://sarajevotimes.com/musk-admitted-to-firing-80-of-trust-and-safety-engineers-at-twitter/>; "Musk's Twitter has dissolved its Trust and Safety Council," Associated Press, December 12, 2022, <https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk>.

²⁹ Moustafa Ayad, "Islamic State Supporters on Twitter: How is 'New' Twitter Handling an Old Problem?," Global Network on Extremism and Technology, November 18, 2022, <https://gnet-research.org/2022/11/18/islamic-state-supporters-on-twitter-how-is-new-twitter-handling-an-old-problem>.

³⁰ Moustafa Ayad, "Teenage Terrorists and the Digital Ecosystem of the Islamic State," CTC Sentinel, Volume 18, Issue 2, February 2025, <https://ctc.westpoint.edu/teenage-terrorists-and-the-digital-ecosystem-of-the-islamic-state>.

- While there have been many discussions about the utility of using AI in terrorism investigations and content moderation on-line, it still does not replace human expertise and contextual clues on these issues whether within tech companies or the U.S. Government.
- The U.S. Government should also urge GIFCT to establish a whitelist for researchers that work on these sensitive issues so that their accounts do not get mistakenly taken down while actual terrorist accounts are targeted. This has been a problem in the past and should be resolved.³¹

Mr. PFLUGER. Thank you, Dr. Zelin.

The Chair now recognizes Mr. Flesch for his opening statement.

**STATEMENT OF DANIEL FLESCH, SENIOR POLICY ANALYST,
MIDDLE EAST AND NORTH AFRICA, ALLISON CENTER FOR
NATIONAL SECURITY, THE HERITAGE FOUNDATION**

Mr. FLESCH. Good afternoon, Chairman Pfluger and Ranking Member Magaziner and Members of the subcommittee. Thank you for the opportunity to testify on this important topic today.

In addition to my work in the Middle East at the Heritage Foundation, I also manage Heritage's National Task Force to Combat Antisemitism, a coalition of organizations committed to defeating the current anti-American wave of antisemitism in the United States.

From my experience, including, sir, as you mentioned, serving in the IDF, I saw how terror organizations engaged in a war against Israel are also recruiting and radicalizing Americans. Put another way, there's a direct connection between the war for survival Israel is fighting in the Middle East and the one America, whether we are aware of it or not, is fighting at home.

The threat today must be understood in the context of Hamas' October 7th attack. Within hours of Hamas executing the deadliest day for the Jewish people since the Holocaust, many across this country took to the streets against the Jewish state, our ally, and in solidarity with a U.S.-designated terrorist organization. Seventeen months later, they have not relented. Just last week, a mob of students wearing masks and keffiyehs and shouting Free Palestine at Barnard College in New York City became violent, leading to several arrests. Among many things, October 7th revealed the extent to which a certain population within our country is already or inclined to become radicalized.

It is telling that Hamas' invasion of Israel and the massacre and abduction of civilians, including Americans, was a spark that prompted this population to reveal itself. Consider the now-commonplace call for an intifada. Those who threaten to globalize the intifada make clear that their goal is not to affect U.S. policy toward Israel or the Middle East, but to destroy the United States through violent political revolution that features a Palestinian-inspired strategy of indiscriminate attacks on civilians to include the murdering of children. These intifada-supporting organizations and individuals and the useful idiots that march or encamp alongside them, presents the most fertile ground for recruitment by terrorist groups. This population is most susceptible to the propaganda of Hamas and other extremist factions within the Palestinian and

³¹ Aaron Y. Zelin, "Highly nuanced policy is very difficult to apply at scale: Examining researcher account and content takedowns on-line," *Policy & Internet*, Volume 15, Issue 4, December 2023, <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.374>.

broader Arab world, who depict the graphic violence of the October 7th attack and the ensuing war as a form of martyrdom. They share videos and images on social media platforms like X, Facebook, and Instagram, and to rally support, spread them on encrypted messaging apps like Telegram.

Extremist groups and supporters turn these platforms and apps into a radicalizing propaganda tool. They post unverified and highly disturbing content that lacks context or factual checks. This is designed to elicit a raw emotional reaction, which is best to reach younger generations. Organizations like Students for Justice in Palestine, SJP, and others rebroadcast and disseminate these messages and images. They invite their social media account followers to various trainings and to join more private communication channels such as Signal, where they may conduct their actual planning and coordination. In framing the October 7th violence, for example, as a noble act in the struggle against an occupying force, Hamas linked in other extreme channels cross-pollinate ideas from different groups, including those agitating against Israel, the Jews, the United States, and the West.

Last summer, the director of national intelligence revealed that the Islamic Republic of Iran was also “posing as activists on-line seeking to encourage protests and even providing financial support to protesters.” The combined effect of these efforts is to radicalize adherence to engage in violent criminal activity. Consider just some recent examples. In November, FBI and local police found rifles, ammunition, an explosive device in the home of 2 Palestinian-American sisters, who are students at George Mason University and leaders in their campus’ SJP chapter. They had previously defaced the student center with threats of a student intifada. On New Year’s Day, as we’ve discussed, hours after an ISIS-inspired terrorist killed 14 civilians in a deadly car attack in New Orleans, pro-Palestinian protesters marched in Times Square chanting for an intifada. One of the organizers of the Barnard College protest from last week, Columbia SJP, proudly and publicly proclaims on its X profile, “Long live the student intifada and glory to our martyrs.”

Terror organizations are actively radicalizing and recruiting an impressionable population for their nefarious means. Efforts should be taken to detect, deter, and defeat their networks, including their organizational supporters and foot soldiers in America. Israel defeated the Palestinian second intifada by simultaneously playing offense and defense. We need such a dual approach today, one that sees law enforcement be proactive against this threat in a civil society that creates its own barrier, beyond which today’s anti-American form of antisemitism is no longer tolerated. If we fail to act now, it is only a matter of time before we may see an intifada on American streets. Thank you.

[The prepared statement of Mr. Flesch follows:]

PREPARED STATEMENT OF DANIEL FLESCH

MARCH 4, 2025

My name is Daniel Flesch. I am the senior policy analyst for the Middle East and North Africa at The Heritage Foundation. The views I express in this testimony are

my own and should not be construed as representing any official position of The Heritage Foundation.

The role of the digital space in how terrorists recruit and radicalize adherents is an important and particularly timely one because we are seeing it play out in real time across this country.

At The Heritage Foundation, I focus on U.S. policy toward Israel and the region. I also manage Heritage's National Task Force to Combat Antisemitism (NTFCA), which is a coalition of organizations committed to combating the current wave of antisemitism in the United States, which is a particular anti-American form of antisemitism.

These 2 policy orientations enable me to see commonalities between how the terrorist organizations fighting Israel are also recruiting and radicalizing Americans. Put another way, I see the direct connection between the war Israel is fighting for survival in the Middle East and the one America, whether we are aware of it or not, is fighting at home.

This is the genesis behind the establishment of the NTFCA and the drafting of Project Esther: a National Strategy to Combat Antisemitism.¹ Project Esther recognizes that today's form of antisemitism that has exploded across the country in the wake of the October 7th attack on Israel by the virulently anti-Israel, anti-Zionist, and anti-American "pro-Palestinian movement" is part of a global Hamas Support Network (HSN) that is trying to compel the U.S. Government to abandon its long-standing support for Israel. Supported by activists and funders dedicated to the destruction of capitalism and democracy, the HSN benefits from the support and training of America's overseas enemies and, within the United States, receives the support of a vast network of activists and funders. This network has a much more ambitious, insidious goal—the destruction of capitalism and democracy. As their ends align, the HSN and its nihilist supporters indoctrinate the gullible into supporting Hamas and hating Israel to create the street mayhem that serves their ends.

In this ecosystem, Hamas and other terrorist organizations and countries are able to recruit and radicalize a willing population on-line with a level of ease and openness that cannot be understated.

It is easy because there are a plethora of social media and digital communication tools—including Instagram, TikTok, Telegram, Signal and others—that organizations and individuals can use to engage with each other.

It is open because many of these organizations do not hide who they are and communicate publicly about their purpose, activities, and intent. Though organizations often use multiple messaging platforms that feature various levels of security, much of their material is intended for public consumption. They are intentional about broadcasting their presence to attract adherents or sympathizers.

The current and immediate threat of malign actors—both foreign and domestic—recruiting and radicalizing within the United States must be understood in our post-October 7th environment.

The October 7th invasion and massacre of southern Israel—in which Hamas, Palestinian Islamic Jihad and Palestinian civilians massacred over 1,200 people and abducted over 250 others back into Gaza, including Americans—catalyzed, or revealed, a unique radicalization that has occurred in America, and across the West more broadly.

In many ways, October 7th was the spark that caused the tinder to burst into a giant, all-consuming flame.

Within hours of the massacre unfolding in Israel, many across this country took to the streets in support of Hamas, which the U.S. State Department designates as a terrorist organization and had just perpetrated the deadliest day for the Jewish people since the Holocaust.

Under the guise of protesting our ally's legitimate response to its people being butchered, mutilated, raped and kidnapped, we saw Americans waving Palestinian and Hamas flags and shouting slogans such as "we don't want 2 States, we want 1948" and "from the river to the sea, Palestine will be free."

These and other evocations demonstrate that rather than seek accommodation and a just solution to the war, these protestors view themselves as active participants and are advocating for the destruction of Israel, the world's only Jewish state and a U.S. ally.

And their calls for violence have only increased, including calling to "globalize the intifada" and threatening "there is only one solution: intifada, revolution".

In calling for an "intifada", the protestors refer to 2 periods of sustained violent Palestinian revolt against Israel. The first intifada (1987–93) ended with the onset of the Oslo peace process, as Israelis believed Palestinian violence stemmed from

¹ Project Esther: A National Strategy to Combat Antisemitism/The Heritage Foundation.

their desire for independence. The second intifada (2000–05) began with the failure of Oslo as Israelis learned that rather than seek their own state, the Palestinians sought to destroy the Jewish state. And they would seek to achieve this through any means necessary, including targeting civilians.²

Prior to Oct. 7, the second intifada was the most traumatic period in Israeli history. In its first full year, Palestinian suicide bombers targeted buses, pizza shops, nightclubs, and other “soft” targets, killing over 100 civilians, including Americans. In a country where it is commonplace for children to take public transportation to school, parents could no longer trust their kids would return home alive. By the time it ended, over 1,000 Israelis and 2,700 Palestinians were dead, with thousands more injured.

This is what those calling to “globalize the intifada” mean to import to American streets. Their goal is not to affect U.S. policy toward Israel or the Middle East, but to destroy the United States through political revolution that features a Palestinian-inspired strategy of indiscriminate attacks against civilians, to include the murdering of children.

Those agitating for an intifada have used Hamas’ invasion and massacre as a pretext to engage in further violence against Jews, including blocking Jewish congregants from entering synagogues while shouting “long live intifada,” stabbing a Jewish man while shouting “free Palestine,” fatally hitting a Jewish counter-protestor in an altercation, and many other incidents.³

Nowhere has discrimination, threats, and violence against Jews and Americans been more concentrated than on university campuses. According to the ADL, in the first 2 months of the Fall 2023 semester, 73 percent of Jewish students had witnessed or experienced antisemitism.⁴ In November of last year, a Congressional investigation into antisemitism on college campuses found that “our most prominent American universities refused to crack down on antisemitism”, including those “students who engaged in antisemitic behavior, encampments, and intimidating tactics such as campus checkpoints and tax-exempt organizations that enabled and funded violent campus protests.”⁵

While the past 16 months have featured the greatest display of overt antisemitism, anti-Zionism, and anti-Israel agitation this country has ever seen, it is all a means to disrupting, degrading, and destroying the fabric of American society and Western civilization.

Many of those who engage in this antisemitic and criminal activity may best be described as “useful idiots” that are supporting the progressive cause du jour; in many cases, they cannot tell you from which river to which sea “Palestine will be free.”

Yet more than the presence of these useful idiots who wave flags or wear the apparel or other paraphernalia of U.S.-designated foreign terrorist organizations, or march alongside or pitch a tent at an encampment of those who support the same, it is the pervasiveness of those who call for an “intifada” that demonstrates there is already a sizable contingent of radicalized organizations and individuals in this country, which presents the most fertile ground for recruitment.

To engage this willing population, Hamas and other extremist factions within the Palestinian and broader Arab world use the graphic violence of the October 7th attack and ensuing war as a form of “martyrdom” to rally support. These groups portray individuals involved in such attacks as heroes, with the violence being framed as a noble act in the struggle against an occupying force. By emphasizing the idealized heroic nature of violence, this framing targets younger generations.

Graphic videos and images are shared across social media platforms like X, Facebook, and Instagram, and spread on encrypted messaging apps like Telegram. Extremist groups and supporters post unverified and highly disturbing content that lack context or factual checks, ensuring that raw emotional reactions take precedence over thoughtful analysis, effectively turning these platforms and apps into a propaganda tool to fuel anger and hate.

These messages and images are then rebroadcast and disseminated by organizations in America, such as Students for Justice in Palestine (SJP), Within Our Lifetime (WOL), Jewish Voices for Peace (JVP), and others.

These groups invite their account followers to trainings and to join more private communication channels, such as Signal, where they may conduct their actual planning and coordination.

² Is Intifada Coming to America?/RealClearPolitics.

³ Ibid.

⁴ The Alarming Surge of Antisemitism on College Campuses/No Tolerance for Antisemitism.

⁵ [edworkforce.house.gov/uploadedfiles/10.30.24_committee_on_education_and_the_workforce_republican_staff_report_antisemitism_on_college_campuses_exposed.pdf](https://www.edworkforce.house.gov/uploadedfiles/10.30.24_committee_on_education_and_the_workforce_republican_staff_report_antisemitism_on_college_campuses_exposed.pdf).

Telegram is also used by Hamas-linked and other extreme channels to cross-pollinate ideas from different groups, including those agitating against Israel, against Jews, against colonialism, against imperialism, against the United States, against the West, etc.

Throughout all this, efforts are made to remain evasive. Account owners and members often change their names. They use coded language to demonstrate alignment across organizations. The intent is not to hide but to maintain a veneer of plausible deniability.

This is the ease and openness with which terrorist groups and U.S.-based organizations that advocate for an “intifada” on American streets coordinate, plan, and execute their activities.

And they are not alone in this regard. In July of last year, the Director of National Intelligence Avril Haines released a statement noting that “Iranian government actors have sought to opportunistically take advantage of on-going protests regarding the war in Gaza.” The statement continued to note that the intelligence community has “observed actors tied to Iran’s government posing as activists online, seeking to encourage protests, and even providing financial support to protestors.”⁶

Hamas has also used public communication channels to disseminate talking points in the United States and radicalize susceptible Americans. In August 2024, the *Palestine Chronicle*, a news outlet run by the People Media Project, a U.S.-based, tax-exempt nonprofit, published an article⁷ about Khaled Meshaal, a Hamas leader, urging university students to protest.

According to a lawsuit filed on February 21, 2025, one of the writers for the *Palestine Chronicle* was Abdallah Aljamal,⁸ who held 3 Israelis—Almog Meir Jan, Andrey Kozlov, and Shlomi Ziv—hostage after their abduction from the Nova music festival on October 7, 2023. Aljamal, the lawsuit alleges, is a member of Hamas.

The combined effect of this evasive and public digital communication is to radicalize adherents to engage in violent, criminal activity.

In November, local police and the FBI raided the home of 2 Palestinian-American sisters at George Mason University (GMU) in Virginia and found rifles, ammunition, and an explosive device, along with signs that read “Death to the Jews” and “Death to America” and the flags of Hamas and Hezbollah, both U.S.-designated terror organizations. The sisters are leaders in their campus’s SJP chapter and previously participated in an act of vandalism when they defaced the student center with threats of a “student intifada.”

In December, the FBI arrested an Egyptian national and GMU student for plotting an attack on the Israeli consulate in New York City because the “building represented the ‘Yahud,’” Arabic for “Jew.” Abdullah Ezzeldin Taha Mohamed Hassan had used X to communicate with the FBI.⁹

On New Years day, hours after an ISIS-inspired terrorist killed 15 civilians in a deadly car attack in New Orleans, pro-Palestinian protesters marched in Times Square in New York City chanting for an intifada.

Particularly on college campuses, many foreign students are engaging in this antisemitic and anti-American rhetoric and activity, including demonstrating for U.S.-designated terror organizations, in violation of their foreign student visa.

In recent news, a Georgetown graduate student was discovered to have direct ties to Hamas. A Committee for Accuracy in Middle East Reporting and Analysis (CAMERA) report found that Mapheze Saleh had previously worked for “the Ministry of Foreign Affairs in Gaza”—which is Hamas—and her father is Ahmed Yousef, “senior adviser to the Hamas Foreign Ministry.”¹⁰ According to CAMERA, Saleh’s “social media profiles have glorified Hamas and its acts of terror” and referred to America as “the plague.”

The revelation of Saleh’s ties came amid a probe into an event the Georgetown Law SJP planned for Ribhi Karajah, who spent 3.5 years in prison for his involvement in the U.S.-designated terror group Popular Front for the Liberation of Pal-

⁶Statement from Director of National Intelligence Avril Haines on Recent Iranian Influence Efforts.

⁷‘Stop this Criminal Aggression’—Meshaal Urges Students to Resume Campus Protests—*Palestine Chronicle*.

⁸Gaza captor told hostages that Hamas collaborates with U.S. campus protesters, lawsuit alleges/*The Times of Israel*.

⁹Concerns Raised About Anti-Israel Sentiment at University.

¹⁰<https://www.msn.com/en-us/society-culture-and-history/human-rights/university-whose-students-invited-terrorist-to-campus-also-enrolled-former-hamas-official/ar-AA1z05St>.

estine's August 2019 roadside bombing that killed a young Israeli woman, Rina Schnerb. Karajah has also promoted PFLP material on his social media accounts.¹¹

In response to the presence of and wide-spread support for U.S.-designated terror organizations on campus from foreign students, the Trump administration's Executive Order to remove those students who provide material support to terror organizations and thereby pose a specific threat of violence is a welcome step to protect Jewish and non-Jewish students on campus. The threat is not to the free speech rights of a few on campus but to the safety, protection, and well-being of all students.

More broadly, efforts should be taken to detect, deter, and defeat the terror organizations' networks, including their organizational supporters and foot soldiers, in America. Those organizations that support calls for an "intifada", provide material support for or receive benefits from U.S.-designated terror groups should be designated as hate groups or domestic terrorists and have their tax-exempt status revoked.

In addition, local, State and Federal law enforcement should share credible and actionable intelligence, including declassifying if and when appropriate, of intent to commit criminal acts.

Terror organizations have found the soft underbelly of American society and will radicalize and recruit an impressionable population for their nefarious means. The ability to counter their efforts exists, it just requires marshalling the requisite capabilities and attention to stem the tide of antisemitism and save America.

Mr. PFLUGER. Thank you, Mr. Flesch.

The Chair now recognizes Dr. Braddock for his opening statement.

STATEMENT OF KURT BRADDOCK, PH.D., ASSISTANT PROFESSOR, PUBLIC COMMUNICATION, AMERICAN UNIVERSITY

Mr. BRADDOCK. Thank you, Chairman Pfluger. Thank you, Ranking Member Magaziner, and distinguished Members of the subcommittee.

I'd first like to thank you for the invitation to appear before this subcommittee. Issues related to recruitment radicalization via the internet have pervaded the study of violent extremism for decades. It's heartening to know that legislators remain cognizant of these complex processes and are determined to undermine them when and where possible.

I'd also like to note that any statements I make in my testimony don't necessarily reflect the position of my institution or any research centers with which I'm affiliated. The testimony I provide here is based solely on my 20 years of findings as a researcher of communication, media radicalization, and terrorism.

I formally studied the communicative tactics of domestic left-wing and right-wing extremist groups, foreign terrorist entities of nearly every political, religious ideology, lone-actor terrorists, and everything in between. Incidentally, it's the time that I've spent studying diverse kinds of terrorist actors that helped me to understand radicalization processes in a systematic manner.

The first and most difficult fact to confront is that the processes by which people come to support the use of terrorism are as varied as the individuals that experience them. As such, no single hearing can be sufficient to comprehensively describe these issues, but I'm glad to hear from Chairman Pfluger that this is only the start of a bipartisan conversation about them.

¹¹Georgetown pressured to cancel event with convicted member of PFLP terror group/Fox News.

Nevertheless, after 20 years of observation, interviews, controlled experiments, and data analysis, I've noticed some patterns among not only the cases of radicalization of terrorism I've studied, but also the context in which they have occurred. It's these commonalities on which I'll focus. But rather than use my initial time to outline the elements of radicalization processes as I've come to understand them, I'd like to offer 4 key themes, lessons learned, and recommendations in my spoken testimony. Of course, I'm happy to elaborate on any of these.

First, I feel it's a mistake to treat quote, on-line radicalization as exclusively distinct from off-line radicalization. In many cases, individuals who are recruited by extremist groups undergo radicalization via their behaviors on-line are often found to be gauging in parallel behaviors off-line. Moreover, the psychological processes that people undergo when they radicalize on-line are similar to what they would experience off-line. Still, there are some technological features of the internet in general, and social media in particular, that can affect these processes. While it can be valuable to be cognizant of these features and their effects, as well as how they can be leveraged by extremist groups, on-line and off-line radicalization are heavily intertwined and should be understood as such.

Second, disinformation perpetuated via social media is a key driver of beliefs and attitudes that make users susceptible and vulnerable to recruitment and radicalization by extremist groups. To a large extent, radicalization to violence via straightforward propaganda disseminated by a cohesive, well-defined extremist group is limited, at least in the United States. Instead, most cases in which an individual radicalizes the violence seems to be due to a process whereby that individual engages with content on social media or other internet-based platforms, both as a function of their own information seeking and algorithmic suggestions that's consistent with their beliefs and attitudes. Consistent with what Daveed said, this often leads to what's been informally called "salad bar radicalizations," where individuals can pick and choose from different ideologies.

Third, the revenue models of many social media platforms are designed such that the platform's executives and administrators are disincentivized from stemming the flow of disinformation and other content that might promote radicalization to violence. Social media platforms are capable of building models of users that help them know what additional content will keep them engaged and thereby valuable to advertisers. As such, users, particularly those who are interested in politics, tend to remain engaged with this ideological content that arouses anger and fear about some out group. This in turn increases polarization and animosity among those who ideologically disagree. The longer eyeballs stay fixed on content, the more valuable ad space is, and content that promotes anger at perceived enemies is very effective at keeping those eyeballs where they're most lucrative.

Finally, fourth, addressing on-line recruitment radicalization requires a multipronged approach that's both reactive and proactive. Research shows that content moderation effectively stems the flow of disinformation and propaganda on social media platforms, expos-

ing fewer viewers to them. However, I would also advocate for digital literacy initiatives that inform users, especially young users, not only about the kinds of content they might encounter, but the strategies used by malicious actors to persuade them. There are several studies in both the United States and in Europe to show that pre-bunking or preemptively undermining this kind of content helps build resilience to its persuasive effects.

With that, I thank you again for the opportunity to appear before this subcommittee and I look forward to your questions. Thank you very much.

[The prepared statement of Mr. Braddock follows:]

PREPARED STATEMENT OF KURT BRADDOCK

To Chairman Pfluger, Ranking Member Magaziner, and the distinguished Members of the subcommittee, I would first like to thank you for the invitation to appear before you. Issues related to recruitment and radicalization via the internet have pervaded the study of violent extremism for decades. It is heartening to know that legislators remain cognizant of these complex processes and determined to undermine them, when and where possible.

I would also like to note that any claims or statements I make in my written or spoken testimonies do not necessarily reflect the position of American University, the School of Communication, or any research center with which I am affiliated. The testimony I provide here is based on 20 years of my findings as a researcher of radicalization and terrorism.

I have studied domestic left-wing and right-wing extremist groups, foreign terrorist entities of nearly every political or religious ideology, lone-actor terrorists, and everything in between. Incidentally, it is the time that I have spent studying diverse kinds of terrorist actors that has helped me to understand radicalization processes in a systematic manner. The first, and most difficult fact to confront is that the social and psychological processes by which individuals come to support the use of terrorism are as varied as the individuals that experience them. As such, no single hearing would be sufficient to comprehensively describe these issues.

Nevertheless, after 20 years of observation, interviews, controlled experiments, and data analysis, I have noticed some patterns among not only cases of radicalization and terrorism, but also the contexts in which they have occurred. It is these commonalities on which I will focus my testimony. Rather than attempt to offer every detail related to why radicalization occurs (which can be discussed in some detail during the hearing itself, should members wish to discuss it), I will be focusing my testimony along 3 key themes that I feel would be of interest to the committee:

- (1) Psychological radicalization to violence and its facilitation on-line,
- (2) Social media as a communicative mechanism for fostering radicalization, and
- (3) Responding to the threat of on-line recruitment and radicalization by malicious actors.

1. RADICALIZATION TO VIOLENCE: PSYCHOLOGICAL PROCESSES

Before delving into the radicalization process as it plays out in on-line spaces, conceptual disagreements about the nature of radicalization—among both researchers and security practitioners—require that we utilize a working definition. For the purposes of this testimony, I define radicalization as a social and psychological process by which an individual comes to adopt beliefs and attitudes that are consistent with an extremist ideology. It is important to note that radicalization, *per se*, does not automatically result in violent behavior on the part of the radicalized. In fact, the vast number of individuals who undergo radicalization never support or engage in violent activity. Radicalization of beliefs and attitudes may render a person a greater risk for engaging in terrorism, but this is by no means a forgone conclusion.¹

An extended form of radicalization—called radicalization to violence²—depicts this process. Radicalization to violence involves not only a change in beliefs and atti-

¹ Ghayda Hassan, Sebastien Brouillette-Alarie, Seraphin Alava, Divina Frau-Meigs, Lysiane Lavoie, Arber Fetiu, Wynnypaul Varela, et al. "Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence," *International Journal of Developmental Science* 12 (2018): 71–88.

² John Horgan, *The Psychology of Terrorism*, 2d ed. (Oxon, UK: Routledge, 2014).

tudes such that they are consistent with those of violent extremists, but also the added intention (and possible opportunity) to carry out a violent attack against civilian targets. To reiterate: not all who undergo radicalization turn to violence, but it does serve as a risk factor.

Given this distinction, and under the assumption that the primary concern of this subcommittee is to prevent violence against American citizens rather than deplorable (yet perfectly legal) beliefs and attitudes, my testimony concerns radicalization to violence—that is, radicalization of behavior—rather than radicalization of beliefs and attitudes.³

Given this, please allow me to turn to psychological mechanisms by which radicalization can occur. As noted above, radicalization processes are various, and are a product of several individual-, group-, and societal-level factors. Still, decades of research on political violence reveals several social and psychological processes that may be affected by the messages with which an individual engages. These processes include (but are not limited to) self-deindividuation, other-deindividuation, dehumanization, and demonization. Although these processes are not unique to the on-line domain, the polarizing nature of social media (see below) can facilitate and catalyze these processes at scale.

First, self-deindividuation⁴ is a psychological process by which a person comes to believe that the importance of their identity as a member of some group has superseded their identity as an individual. That is, they see themselves as part of something bigger or more important than themselves, and are therefore willing to make individual sacrifices to their own well-being (including personal safety) to support the group of which they are a part. In the context of radicalization to violence, individuals who self-deindividuate while engaging with extremists on-line may come to believe themselves to be part of an important social movement, their membership in which is the central part of their identity. This may render them more ready to engage in violence on behalf of that movement.

Other-deindividuation relates to a process by which an individual comes to perceive members of some outgroup (e.g., those depicted as enemies) as lacking individual traits. Instead of perceiving those people as individual human beings, they are instead perceived as a homogenous mass of “them.” By characterizing an outgroup in this way, extremists can psychologically prepare their recruitment or radicalization targets to harm them, should the need arise.

Related to this, dehumanization⁵ is the psychological process by which an individual comes to perceive members of the outgroup to be non-human, thereby suggesting they are not worthy of the respect bestowed upon fellow humans. Often, this is prompted by speakers’ characterization of the outgroup as being animals, vermin, or some other organism worthy of derision and hate. When an outgroup is discussed in these terms over time, audiences come to lose their perceptions of the outgroup’s humanity, which likewise facilitates their willingness to harm them, should the group require it.

Finally, demonization⁶ relates to a psychological process whereby an individual comes to perceive others as embodying evil. When an outgroup is characterized as evil, particularly if an individual believes that their ingroup is charged with defending some constituency, it becomes easier for that individual to commit violence against that group.

Self-deindividuation, other-deindividuation, dehumanization, and demonization are not the only psychological processes that can occur when an individual undergoes radicalization to violence, but many cases of terrorist violence indicate that they are relatively common among the violent.

Given that the purpose of this hearing is to understand recruitment and radicalization in the on-line space, however, it is useful to consider the features of the internet generally, and social media specifically, that facilitate these processes.

³See, for example, Clark McCauley and Sophia Moskalenko, “Understanding Political Radicalization: The Two-Pyramid Model,” *American Psychologist* 72(3) (2017), pp. 205–216.

⁴Originally in Max Taylor, *The Terrorist* (Lincoln, NE: Potomac Books, 1988); for a summary of these processes, see Chapter 5 in Elyamine Settoul and Thierry Balzacq, *Radicalization in Theory and Practice: Understanding Religious Violence in Western Europe*. (Ann Arbor, MI: University of Michigan Press, 2022).

⁵See Nour S. Kteily and Alexander P. Landry, “Dehumanization: Trends, Insights, and Challenges,” *Trends in Cognitive Sciences* 26, no. 3 (2022): 222–240.

⁶See Roger Giner-Sorolla, Bernhard Leidner, and Emanuele Castano, “Dehumanization, Demonization, and Morality Shifting,” in Michael A. Hogg and Danielle L. Blaylock, eds., *Extremism and the Psychology of Uncertainty* (Hoboken, NJ: Wiley, 2011), Chapter 10.

2. SOCIAL MEDIA AS A MECHANISM FOR FOSTERING RADICALIZATION TO VIOLENCE

Understanding the psychology of radicalization to violence requires the understanding that a consideration of “on-line” versus “offline” radicalization is a false dichotomy.⁷ By distinguishing processes that occur in an on-line environment from those that occur away from a computer screen incorrectly suggests that these phenomena are distinct. In truth, individual trajectories toward terrorism are often driven by activities that take place over time in both the real-world and on-line domains.

Still, there are some phenomena that are unique to the on-line sphere generally (and social media specifically) that lend themselves to our understanding of how on-line engagement with malicious actors and problematic content contributes to the radicalization process. In this section, I outline some of these processes and phenomena, with a specific focus on social media, how its revenue streams are structured, and how on-line engagement and the commodification of attention combine to form the perfect storm for radicalization to violence when malicious actors engage with vulnerable audiences.

The primary means by which large social media platforms generate revenue is through advertising.⁸ To generate income, these large companies (e.g., Meta, Twitter/X) allow advertisers to appear among the posts to which users are engaged, and when those advertisements appeal to a user, they may pay closer attention to that ad (measured in clicks or amount of time viewing the ad) or purchase the product or service being offered. To maximize the value of an advertisement, the social media platforms develop models of their users based on previous on-line engagement, thereby allowing them to promote advertisements that will be most appealing. In this way, advertising space on social media platforms is valuable to the degree that the platform can attract views and engagement from its users.

Because attention has been effectively commodified, the social media platforms are financially incentivized to prioritize and feature content that is likely to arouse thoughts and emotions that promote engagement. In many cases, this content takes the form of messaging with which the user has previously engaged, news that will evoke engaging feelings like anger⁹ or otherwise subconsciously persuade the user to keep interacting with the platform.¹⁰ Moreover, the algorithms that determine the basis upon which users are recommended additional content are designed to keep them in ideological echo chambers in which the messages to which they are exposed grow increasingly extreme and no dissenting voices can ever be heard.¹¹

When this content is political or ideological—contexts in which disinformation is abound—users can develop increasingly extreme beliefs and attitudes about the use of violence against perceived enemies on the basis of false perceptions and imagined grievances. In this way, the cultivation of echo chambers in the on-line space due to the revenue structures of social media platforms builds to a “perfect storm” of engagement, isolation, and anger that can lead to the aforementioned psychological processes (i.e., deindividuation, dehumanization, demonization), thereby increasing risk for radicalization to violence.

3. RESPONDING TO THE THREAT OF ON-LINE RECRUITMENT AND RADICALIZATION TO VIOLENCE

Although the on-line space serves to facilitate several processes associated with radicalization to violence, there is an abundance of research on steps that can be taken to mitigate the likelihood that the on-line space (particularly social media) can be leveraged by extremists to recruit and radicalize target audiences.

First, several studies have demonstrated that the responsible moderation of some content, primarily in the form of content takedowns and user bans, can reduce the

⁷Joe Whittaker, “Rethinking Online Radicalization,” *Perspectives on Terrorism* 16, no. 4 (2022), 27–40.

⁸Amanda Raffoul, Zachary J. Ward, Monique Santoso, Jill R. Kavanaugh, and Bryn Austin, “Social Media Platforms Generate Billions in Dollars in Revenue from U.S. Youth: Findings from a Simulated Revenue Model,” *PLOS One* 18, no. 12 (2023), e0295337.

⁹For example, see Jacquelin van Stekelenburg, “Radicalization and Violent Emotions,” *American Political Science Association Politics Symposium* (2017).

¹⁰For a discussion related to subconscious advertising, see Anne-Sophie Bayle-Tourtoulou and Michel Badoc, *The Neuro-Consumer: Adapting Marketing and Communication Strategies for the Subconscious, Instinctive, and Irrational Consumer’s Brain* (London: Routledge, 2020).

¹¹Michael Wolfowicz, David Weisburd, and Badi Hasisi, “Examining the Interactive Effects of the Filter Bubble and the Echo Chamber on Radicalization,” *Journal of Experimental Criminology* 19 (2023): 119–141.

impact of malicious content.¹² These studies have collectively demonstrated that when social media platforms work with experts in extremist messaging, media, and psychology to identify content that poses a risk for audience radicalization, the content is not distributed as widely and the malicious actors are less likely to reach their target audiences. That said, the prevalence of malicious content on-line suggests that exclusive reliance on content moderation would not be sufficient for reducing the efficacy of recruitment and radicalization efforts. Instead, moderation should be considered only a tool in the overall toolkit of platform administrators.

Rather than rely solely on a reactive approach like content moderation, there is also research to suggest that prophylactic strategies that seek to increase audience resistance to extremist content would be particularly effective. Specifically, media literacy initiatives¹³ designed to teach audiences—particularly young audiences—about how malicious actors may develop content designed to lead them to violence could be particularly useful. Given the increasingly young age at which many children are becoming digitally literate, it would behoove interested parties to consider media literacy campaigns as early as is reasonable.

Finally, there exists a specific counter-persuasion strategy in which users are exposed to weakened versions of the extremist messages to which they will later be exposed when they are on-line.¹⁴ Several decades of research have shown that when audiences are told about the content they will encounter (or the strategies that malicious actors may use to distribute that content), and are provided with counter-arguments against it, they are substantially less likely to be persuaded by it.¹⁵ This approach would be particularly fruitful for dealing with propaganda and disinformation produce with generative artificial intelligence,¹⁶ which can be particularly difficult to identify and resist without proper training.

The written testimony I have provided above represents only a small drop in the bucket of our collective knowledge related to the on-line sphere, radicalization to violence, and the increasingly complex ways that extremist groups are targeting vulnerable audiences. However, as extremists develop increasingly sophisticated methods for recruiting and radicalizing audiences to violence, so too must we develop increasingly sophisticated methods for undermining them.

Note that additional scholastic references for the concepts described above are available upon request. I would also be happy to provide the committee with additional information concerning radicalization to violence more generally and the role of the internet in facilitating it.

Mr. PFLUGER. Thank you all for your opening statements.

Members will be recognized in order of seniority. We will also have Members that are cycling in and out. An additional round of questioning may be called after all Members have been recognized, and I will now recognize myself for 5 minutes of questioning.

Dr. Gartenstein-Ross, I mean, the big question here is basically the First Amendment and how we prevent attacks. How we prevent, you know, these terrorist attacks from happening, as I have heard your testimonies and read your written statements. So how do we differentiate between the Constitutionally-protected speech and then also the speech that may advocate for violence and ter-

¹²For a current review of these practices, see latest articles in *Studies in Conflict and Terrorism*, especially Maura Conway and Stuart Macdonald, "Introduction to the Special Issue: The Practicalities and Complexities of (Regulating) Online Terrorist Content Moderation," *Studies in Conflict & Terrorism* (2025, on-line). See also Heather Wolbers, Christopher Dowling, Timothy Cubitt, and Chante Kuhn, "Understanding and Preventing Internet-Facilitated Radicalisation," *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, no. 673.

¹³For an early synopsis, see Jan-Jaap van Eerten, Bertjan Doosje, Elly Konjin, Beatriece de Graaf, and Marielle de Goede, *Developing a Social Media Response to Radicalization: The Role of Counter-Narratives in Prevention of Radicalization and De-Radicalization* (Amsterdam, NL: Colophon), 108.

¹⁴Josh Compton and Kurt Braddock, "Inoculation Theory and Conspiracy, Radicalization, and Violent Extremism," in Sergei A. Samoilenko and Solon Simmons, eds., *The Handbook of Social and Political Conflict* (Hoboken, NJ: John Wiley and Sons, 2025).

¹⁵For experimental evidence in the realm of violent extremism, see Kurt Braddock, "Vaccinating against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda," *Terrorism and Political Violence* 34, no. 2 (2022): 240–262.

¹⁶Stephane J. Beale and Lewys Brace, "AI Extremism: Technologies, Tactics, Actors," *VOX-Pol Report* (2024). <https://dial.uclouvain.be/pr/boreal/object/boreal/291289>. which can be particularly difficult to identify and resist without proper training.

rorism? How do we protect the First Amendment and thwart that violence?

Mr. GARTENSTEIN-ROSS. Thank you, Chairman Pfluger. That's a great question. One case that I recommend people to be familiar with is the Sami Al-Hussayen case. It occurred in Idaho shortly after the 9/11 attacks. He was prosecuted for terrorist propaganda. Ultimately, the jury found him not guilty based on First Amendment grounds. After that case, there have been very few just propaganda prosecutions.

I think Ranking Member Magaziner put it right when he talked about how there's no right to incite people to attack, there's no right to recruit people to terrorist groups. Foreign terrorists don't have a right. But I think when you get into that kind of gray area, I expect to see very few prosecutions. Instead, it's when there's incitement to imminent lawlessness, which is the First Amendment standard.

Mr. PFLUGER. Thank you. Dr. Zelin, you mentioned something in your spoken testimony about Jabbar and his posting. So I want to follow up on this question. Should we have known? Could we have known what could have been done? Did his speech actually violate the protected speech or was he still in that protected speech place?

Mr. ZELIN. Thank you, Chairman. It's definitely a complicated issue, but based off of Facebook's own policies, through their dangerous organizations unit within Facebook, they have their own sort of FTO list. If you provide support to that group, which this individual did by pledging allegiance to the caliph, that would be considered contravening, you know, their own policies. Again, these are private companies. This isn't related to speech about politics per se, but within the context of a private company that sets its own policies. Of course, there isn't such a thing as necessarily 100 percent security or successes in these issues. But if there are more proactive measures with more people involved in trying to follow these issues, I think it's definitely a possibility that something could be stopped, for sure.

Mr. PFLUGER. You talked about content moderation, and is it your belief that is done at the platform level?

Mr. ZELIN. Yes, I mean, of course, Congress could potentially regulate to make sure that they actually follow a certain way of doing it, but there have been methodologies that have been laid out by the Global Internet Forum to counter terrorism, which is essentially a consortium of key American tech companies such as Google, X, Facebook, Microsoft, et cetera, in terms of how they find the digital footprint or fingerprint of these issues, to take this content down. But the terrorists, of course, are evolving themselves as well. So it's key to try and stay on top of it, because as we take content down or ways of taking content, they try and then go around it. For example, instead of saying, like, "the Islamic State" or whatever, they'll put like dots in between each letter or an underscore so that it trips up the content moderation, at least in terms of, you know, written types of stuff.

Mr. PFLUGER. Thank you. Mr. Flesch, you talked about George Mason University. I was made aware that there was an incident on Georgetown's campus where a convicted terrorist named Ribhi Karajah, who was found to be a member of the PFLP, was invited

to speak and allowed to speak at, you know, a student-led organization or on campus there. So you have got somebody that was involved in a bombing in Israel that was part of the PLO and comes onto one of the campuses.

Just what needs to happen here? What is the response, the university's responsibility and then, conversely, what is the responsibility of either Federal or State and local law enforcement?

Mr. FLESCHE. Certainly. Thank you, Mr. Chairman. I think the first thing is to recognize that while we all talk a lot about Hamas, I focus on them in my testimony. The fact is there are a number of terrorist organizations in the, I believe, Palestinian population that has presence here. PFLP, the Popular Front for Liberation of Palestine, goes back 50-plus years of all the other U.S.-designated terrorist organizations. So recognizing that the threat is not just for host Hamas, Hezbollah, these other big names we hear about, there's a number of other organizations that also are designated U.S. terrorist organizations. So that's No. 1.

No. 2 is reaching out to and ensuring that student groups on campus are aware of this and those that do invite members of these organizations, those have been convicted for terrorism and this individual was involved in the killing of a 19-year-old Israeli a few years ago, that they should not be involved—invited to campus whatsoever. I think from a Federal perspective you just have to start looking into the universities that provide for these student groups, provide for these organizations, and if they give platforms to terrorist-supporting individuals or terrorists themselves, they should, you know, withdraw Federal funding from them.

Mr. PFLUGER. I think it was shameful that the university allowed this individual to even announce such of a meeting.

So my time has expired. I now recognize the Ranking Member.

Mr. MAGAZINER. Thank you. I would like to start by focusing on the responsibility of the social media and messaging platforms or what their responsibility should be. I think starting with the framework that we have laid out that, hopefully, everyone here agrees with, which is that there is a First Amendment right to have different political views, even extreme political views. But there is not a First Amendment right to plot violence or incite violence. Like if we can agree with that as a premise, when you have speech that is inciting violence, plotting violence, what does effective content moderation look like and how can we ensure some level of standardization across the platforms to make sure they're actually doing it? You know, we can start here with Dr. Zelin and then Dr. Braddock or anyone else.

Mr. ZELIN. Thank you, Ranking Member Magaziner. In terms of ways of doing this, there have been a few methodologies that have tried out. One is related to having a digital fingerprint for different textual, audio, pictorial, and video content, so that if that particular piece of content shows up on any particular platform, it'll be wiped out right away. Going further than that, there's also a way of going after IP addresses of people who have posted this type of content to make sure that they're not allowed to create secondary accounts because this is one of the things that has happened before.

The bigger question, though, beyond just content in English language, is that other languages have lagged far behind on these fronts when we're talking about issues like ISIS, where Arabic and English has gotten better, but when we get into Africa, Central Asia, and elsewhere, it's way worse. There's a free-for-all in some ways.

Mr. MAGAZINER. Thank you. Dr. Braddock.

Mr. BRADDOCK. I would just echo what Dr. Zelin just said about the moderation of content and automating it, looking for visual content, looking for written content. But something that I think that we haven't missed it, but something that can be emphasized is it's not just content that's taken down. Dr. Zelin mentioned the banning of IP addresses, but banning users who spread this kind of information, I think that needs to be part of the tool kit as well because there's research that shows that as these users are banned from certain platforms, their reach grows smaller and smaller. That's what we want from these mass propagandists.

Mr. MAGAZINER. So this is a helpful use of sort-of best practices. But when we think about what the role of Congress should be, I mean, you know, I personally feel that Congress does have a role to ensure that a baseline of best practices are followed across all platforms. Again, to me, this is not a First Amendment issue because we are not saying that we are moderating political beliefs or anything like that. It is specifically incitement of violence. There is precedent here because Congress has essentially banned non-consensual pornography and other types of content. There is no successful First Amendment challenge to that.

So, you know, again, what would Congressional action look like potentially in order to ensure that there is at least a baseline of appropriate moderation occurring across all platforms? Because I agree some platforms are doing it, they are doing it well, doing it somewhat well, others aren't even trying. So what is our role here?

Mr. ZELIN. I mean, one way would be to potentially regulate to make sure that all platforms that work in the United States follow certain types of, you know, methodologies, I guess you can say, so that when certain companies change, who's in charge of them or, you know, policies change for whatever reason, that there's a certain standard that everybody lives up to, to make sure that violent extremists, terrorists, what have you are not able to take advantage.

Mr. MAGAZINER. Yes. We have been talking a lot about social media platforms and I think we all, you know, we think about TikTok and X and Facebook, et cetera. But my understanding is that on-line gaming platforms are becoming ripe ground for radicalization as well. Sort-of the messaging and communication features on gaming platforms, people are recruited and sort-of groomed sometimes for extremism. Would anyone like to comment on gaming platforms specifically and what you are seeing?

Mr. BRADDOCK. I can comment briefly. My understanding is it started really, in some of these games, it starts in the interactive chat where people are spreading epithets or trying to recruit almost passively. But there are certain—I mean there's social media gaming-type platforms, like Discord, where people can meet and talk and plan and exchange different kinds of pictures, text, any-

thing they want in the same way they could on another social media platform. So it's almost like traditional social media and gaming social media, so to speak. There's this intersection where they're exploiting the freedom they have there.

Mr. MAGAZINER. Yes. I am low on time, but real quick, pre-bunking, can you just explain a little bit more what that is and so forth?

Mr. BRADDOCK. Yes. So there's a lot of research out of Cambridge that shows that when you address a person, if we know they're going to be persuaded by a certain kind of content, if we make them aware of that content before they're exposed to it and let them know that they're susceptible to persuasion, people, especially in the United States and the United Kingdom, they don't like knowing that they're susceptible to persuasion. So they put their defenses up and they're more likely to recognize it when they encounter it. The research coming out of Cambridge has shown that you can gamify this, you can turn it into a game. People get very, very good at recognizing when malicious actors, whether they be foreign or domestic, are trying to persuade them.

Mr. MAGAZINER. Thank you. That is helpful.

I yield back.

Mr. PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentlelady from Georgia, Ms. Greene.

Ms. GREENE. Thank you, Mr. Chairman. Thank you for being here today, our witnesses.

As we know, the politically-weaponized FBI and DOJ under the Biden administration went after peaceful pro-lifers, J Sixers, and Catholics attending Latin Mass, parents trying to hold their school boards accountable, and many more conservatives. They refused to prosecute heinous sex crimes against children and actual terrorists who wanted death to America and chanted it in our streets.

In October 2020, 3 rioters from the Jewish Voice for Peace and IfNotNow, both violent pro-Islamic groups that support Hamas, invaded the Capitol complex. As a matter of fact, they came in this building right here and they took over the Cannon Rotunda. Their actions, they completely shut down the elevators, the stairwells, the hallways, they blocked exits, and the police officers were assaulted. They took over and stopped hearings and they stopped Congress, same way January 6th did, although they were not prosecuted and they were not held accountable the same way protesters on January 6th were.

Now, I bring this up today because the riot organizers that held this riot here in the Cannon Building not only communicated through a chat that appears to be Signal, similar to the ones—similar to different messaging programs you have spoken about, but the title of the chat was Global Intifada. So if you see—it is hard for you to see, I know from here, but this picture right here is a screenshot of one of their cell phones as they were communicating with each other. You can see in the background their signs. It was taken over in the Cannon Rotunda, but right here it says Global Intifada. They were an organized group and they had organized this pro-Hamas, pro-terrorist riot here in the Cannon Building.

Mr. Flesch, in your testimony, you talk about globalizing the intifada. What is the goal for globalizing intifada not only world-wide, but in the streets of America?

Mr. FLESCHE. Yes, ma'am. Well, the goal of people calling to globalizing intifada is to bring a Palestinian-inspired strategy of violent political revolution targeting civilians, including children, and essentially to overthrow the United States and to defeat the fabric of society of the United States.

Ms. GREENE. So their stated goal is to overthrow the United States. They organized and they call themselves Global Intifada and they came in this building in 2023. That is shocking.

If you look at the names of the members in the group chat, you will find the lead attorney for the Southern Poverty Law Center, the SPLC, Katrina Bleckley, right here. Katrina Bleckley is part of the Global Intifada, lead attorney for the Southern Poverty Law Center. This is the same law center that provided nearly 40 pages of testimony to the same January 6th committee that was prosecuting people for protesting the 2020 election. This is also the same law center that was cited in the FBI memo that labeled traditional Catholics as radical extremists. This is the same law center which has nearly \$770 million in assets, by the way, and was given over \$8,000 by the Department of State in 2021 for speaking engagements with Lecia Brooks.

So we are here talking about on-line radicalization, but we are also through this, this right here is proof for every single American that this radicalization that is happening on-line is radicalization that has happened right here in our Government that stopped Congress.

I would also like to highlight the threat of on-line radicalization and how the threat within our own homeland has been exasperated by more than 12 million illegals the Democrats allowed to pour into our communities under Biden, with 2 million of them being known gotaways who we have no clue where they are from, where they are now, and what their motives are inside our homeland.

Dr. Gartenstein-Ross, can you briefly outline, I know I am out of time here, the key methods foreign terrorists groups use to radicalize individuals on-line to not only join their ranks, but carry out attacks?

Thank you, Mr. Chairman.

Mr. GARTENSTEIN-ROSS. Thank you.

Mr. PFLUGER. You have about 30 seconds.

Mr. GARTENSTEIN-ROSS. Sure. To do it very quickly, as Dr. Braddock said, there often is not a great gulf between what's done on-line and off-line. On-line, generally speaking, methods include looking at people who seem susceptible to propaganda, forging a relationship with them. They sort-of act as a social movement in that way, getting to know people who they want to recruit. I've written about what's called the virtual plotter model that was—that ISIS used a lot, and I believe still does in a number of different ways, which uses encryption often to be with attackers right up until the moment that they attack. Thank you.

Mr. PFLUGER. The gentlelady's time has expired.

The Chair now recognizes the gentleman from California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman.

I think one thing that unites all of us across the aisle is our interest and our goal of protecting our citizens from terrorist attacks, domestic or foreign terrorists as it may be. That job, I would say, is like finding a needle in a haystack. You need intel, you need to work with our foreign partners. That is why we have FISA and our ability to gather intelligence to figure it out.

You know, General Kelly, former Secretary of Homeland Security, used to say that border security does not end or begin at the border, but it is rather a compilation of a lot of work, a lot of intel work with our partners across the seas and other places. At the end of the day, you have U.S. Government agencies that put this stuff together and decide, try to decide, try to anticipate these attacks. FBI, CIA, other agencies, along with State and locals that try to figure this out. I would say a lot of these agents are patriots. They work Government where they could be making a whole lot more money private sector, but they are working for the Government because they believe in the mission.

I am concerned over these firings that I see FBI and CIA agents. What is it going to do for morale for those who are left? What is it going to do for those that just got fired? There is a story that Chinese and Russian operatives are trying to recruit some of these fired individuals to work for them. But at the end of the day, I want to ask you, gentlemen, each of you, these firings, is this good for our national security?

Mr. Gartenstein-Ross, is this good or bad morale? You are losing a whole lot of intelligence experience. Please, opine.

Mr. GARTENSTEIN-ROSS. Sir, thank you for the question. I'd be very happy to talk to you about this. I'm not here to testify on it and the reason specifically—

Mr. CORREA. Thank you very much. Dr. Zelin.

Mr. ZELIN. It's hard to know what specifically is being cut with a bit more transparency, but there's definitely a case to be made that less people focusing on these issues could lead to greater risks in the future.

Mr. CORREA. Look, you fire folks, even though that person fired may be somebody who is new 2 years, 5 years, I mean, they are going to look, the person that is left behind working on this stuff is saying, what is it going to do for your morale? I might be the next one. Do you think that would possibly affect your effectiveness defending the homeland?

Mr. ZELIN. It's definitely plausible. Obviously, what's going on now is very new, so we don't have a test case to know the specifics of what could happen. But less people focusing on these threats online definitely could mean less eyes on something that something then passes through.

Mr. CORREA. Let me say that these folks have to have defense. You can't score one point on us. They cannot. That means American lives.

Mr. Flesch, what do you think? Firing good, bad, morale?

Mr. FLESCHE. I would echo what my colleagues have said, that it's a little early to tell the effect of this policy, but certainly I'm happy to have a conversation after the fact, but focusing on the radicalizing element is why I've been brought here to talk.

Mr. CORREA. Well, I certainly hope that we don't get to the day when we say it was a little bit too late. Not too early, but not too late.

Mr. Braddock, thoughts?

Mr. BRADDOCK. I'll say bad, but not so much—I agree with Dr. Zelin about the fact that it's an issue of the number of personnel, the number of eyes you have on this content and the users. I also think it's a issue of institutional knowledge. There are ways the terrorists communicate on-line that take a long time to understand. Give you an example. I recently saw a study that are showing that some foreign terrorist organizations, they communicate via exclusively emojis. They just use emojis and they're coded in different ways. Now, if somebody has that institutional knowledge related to the use of emojis—

Mr. CORREA. So experience matters.

Mr. BRADDOCK. Experience matters.

Mr. CORREA. Firing people may not be the wisest thing to do. I am not trying to get political here. I am just saying that all of us have a vested interest in protecting the homeland. That is why Homeland Security was created after 9/11, when we had holes in the system, when we had silos that didn't talk to each other. Nine-eleven could have been prevented possibly, but that is why we are here. I am concerned that the firing of these individuals will hurt us defending the homeland in the long term.

Thank you gentlemen, for your testimony. Mr. Chairman, I'm out of time. I yield.

Mr. PFLUGER. The gentleman yields.

The Chair now recognizes the gentleman from Texas, Mr. Luttrell.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Good afternoon, gentlemen. I represent a small portion of Harris County, Houston, Texas, and this pains me to say it is, but Houston, Texas, is the worst city in the country for sex trafficking. I have had multiple discussions, meetings, various agencies, law enforcement, up and down the elected leadership, not only in Harris County, but the State. How do you solve a—I sit on the I-10/45 corridor. How do you solve a problem where these—and just to be clear, cartels are now known as terrorist organizations. So I am going to throw this on you guys. The conversations that I have with these folks is like, how do we solve this problem? How do you cut the head off the snake? How do you get rid of these bad actors to save our babies? Because they are going after our children. It always circles back to the metaverse. It lives and breathes on-line. That is how they communicate. That is how they recruit, and that is how they set the hook. Then our children are moved into this horrible space and become victims.

I want to hear from all 4 of you. How do we—and I think it was Mr. Flesch who said regulate. How do we regulate the system? I am sorry, might have been you, Doctor, that said we regulate the space, right, regulate the system, which I am not speaking for my colleagues, but I am sure they would absolutely get on board with the fact that this is a problem we shouldn't have when it comes to the protection of our babies. Right?

How do we fix this? If we regulate it, it is going to have to come from the subject-matter experts, which would be you all or those that control either the social media platforms, the gaming systems. Because the best thing I can do for my children is inform them of what happens out there. But when I talk to the parents whose children have been taken, they never saw it coming.

Dr. Ross, I will start with you, sir.

Mr. GARTENSTEIN-ROSS. Thank you, sir. It's a great question, and I'll take it from the cartel's angle first and foremost. That's something that I've done a fair amount of work on in some of my projects for U.S. Customs and Border Protection.

I'd move it a little bit away from the on-line space. The way we've looked at cartels in our work for CBP is how do you shift their incentives? Cartels are many things, but among them, they're a business. I would look at the cartel's center of gravity. I think that right now we're playing defense vis-a-vis the cartels with respect to trying to stop them at the borders. One way I would look at it is there's a number of different vulnerabilities that they have. How do you shift those incentives? Through causing some pain to them, but doing so in a way that isn't too costly for us at the same time. I think that that's very important because the flow of human trafficking—

Mr. LUTTRELL. Where would that—great. I mean, that's—OK, you are opening up—I don't know if I am going to say you open up Pandora's box there. But if we are going to move them away from sex trafficking, drug trafficking, and all that illegal nefarious acts, we are not going to make them a legitimate company. I mean, where do we push them?

Mr. GARTENSTEIN-ROSS. Yes, I don't think that trying to make them a legitimate company is the way to go.

Mr. LUTTRELL. Yes.

Mr. GARTENSTEIN-ROSS. Obviously, there are some who argue for that, but I think that there are different ways that we can undertake points of pain vis-a-vis cartels. Obviously, there's a whole conversation around cartels right now, designations, possible use of military force, and the like. One thing that we know is that cartels are fighting against two sets of enemies in most places they operate. They're fighting, No. 1, against the Mexican government, both Federal and State. No. 2, they're also fighting against other cartels as well.

Oftentimes, you know, picking your enemy and leaving other enemies alone can have a very serious effect on them. Anyway, I don't want to advocate for something specific other than say that I think there's a different way to look at it, that we tend to look at defense at the border. I think there's a secondary way to look at it, which is cartels have incentives, they have vulnerabilities. If we look at the question as, how is it that rather than doing what you could call Operation Same the same, meaning we have the same operations over and over mobilizing to the border, how is it that you shift their incentives in a way that will have a lasting effect? I think that it's a complex answer, but that's the way I would formulate the question to hopefully get something that is more lasting than what we have now.

Mr. LUTTRELL. Dr. Zelin, you got 21 seconds, sir. How we doing?

Mr. ZELIN. Thank you for the question, but it's not a subject I personally focus on, so I don't have as much experience on it.

Mr. LUTTRELL. Mr. Flesch, go ahead.

Mr. FLESCHE. I'd echo my colleague.

Mr. LUTTRELL. Then we can't run. Hey, hey, hey, hey. You need to hear me say this. Don't run away from this. This is the worst, worst thing you can possibly imagine when you see these babies. OK? If you are not studying it and I'm not going—I can't sit here on this dais and tell you to do that. OK?

Mr. BRADDOCK. I'll take 10 seconds because I know we're out of time. But—

Mr. LUTTRELL. You good?

Mr. BRADDOCK. Am I good with that?

Mr. LUTTRELL. Yes.

Mr. BRADDOCK. Yes. We had a child abducted near my home town as well a couple of years ago, assumed to have been sold into sex trafficking as well, so it's near and dear to me as well.

My main point would be we've been focusing on content moderation, the responsibility of the platforms to focus on content. I also think that there can be more, the platforms can do more to regulate what's going on in private messaging on those platforms between people. Because that's a lot of the ways that these individuals are reaching out to children is they're engaging with them in these private messages on Facebook, on Instagram, on whatever platform you choose. When those personal relationships develop, that's how kids are groomed and they're taken.

Mr. LUTTRELL. Thank you.

Mr. BRADDOCK. So I want you to focus on that as well.

Mr. LUTTRELL. Thank you, Mr. Chairman.

Mr. PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you very much, Mr. Chairman. I also want to echo my support for having this hearing, especially because I tried futilely and desperately last Congress to have a hearing on a similar topic. In November 2023, I wrote a letter, led a letter to Elon Musk on X, because in the 6 weeks following October 7th attack that Mr. Flesch so powerfully referenced, there was massive distribution of Hamas and other terrorist propaganda videos and even some generated profit on X. I got no response, written response. I guess that part of the 75 percent cut in Twitter that Elon Musk did went to the Government Affairs Office.

So then, in March, I wrote to Chairman Comer. I was on the Oversight Committee asking for a hearing on this because it continued. In fact, the secretary general of Hezbollah, Hassan Nasrallah, actually wrote a tweet complaining about having his blue checkmark taken down. So that was an issue that also related to violating sanctions. No word from Chairman Comer.

Then we wrote a letter to the Speaker in August. No response, no hearing. So I am glad we are having this and I take the gesture of bipartisanship seriously.

Dr. Zelin, I want to come to you first because I noticed in your opening statement, Dr. Braddock, you said the similar things, that a lot of these problems have been exacerbated by a reduction in

content moderation. In fact, you said beginning with Elon Musk's purchase of Twitter, the level of content moderation in general has backslid. Of course, recently Mark Zuckerberg announced that Meta was eliminating all content moderation.

Certainly we are grappling with the First Amendment, but there is no possible way to stop the on-line proliferation of terrorism without some degree of content moderation. Is that right, Dr. Zelin?

Mr. ZELIN. Yes, thank you for the question. I agree. I mean, obviously we have our own internal debates within the United States, partisan debates, what have you. But when we're talking about foreign terrorist organizations, we need to be clear that they should not have a space on these platforms, especially American-owned companies. The current state of things has definitely backslid in recent years.

Mr. GOLDMAN. Part of the reason that they should not is that they are professional criminal organizations, to put it a different way. Is that right?

Mr. ZELIN. Yes. I mean, they do—you know, they're doing things illegally according to the U.S. law for sure.

Mr. GOLDMAN. So we don't want crimes to be committed on-line on our American companies, right?

Mr. ZELIN. That's correct.

Mr. GOLDMAN. So this is where we run into a problem because some believe that the free speech is an absolute right. You can say anything you want to say. Of course, that would include inciting violence, potentially committing crime, and also sex trafficking, as my colleague aptly pointed out. So this is not an academic exercise in discussing the First Amendment. This has real-world significance that you all have identified.

Mr. Flesch, when I was walking over here after we just voted, outside the Capitol, I saw a huge poster with a swastika on it. I know you have spoken a lot about the rise of antisemitism, anti-Israel sentiment post-October 7th, and I agree with you about that and I condemn it wholeheartedly. But we are also seeing a rise of neo-Nazi attitudes on-line. In fact, some of them are truly perpetuated by the owner of X, who has expressed support for AfD in Germany, which, I think you will agree with me, is effectively a neo-Nazi organization.

I guess I would just ask you, you have addressed a lot of the rise in the global intifada and I agree with you, but talk about the risk of the on-line support and proliferation of nuclear neo-Nazi views.

Mr. FLESCHE. Well, I think certainly neo-Nazis are antisemites. They certainly present a risk to everyday Americans. A lot of my focus has been on the current immediate threat that the—and for short-hand, this Hamas supporting network that we've been looking at Heritage presents to Americans of all persuasions, not just Jews. So neo-Nazis, you know, will certainly be a threat for—maybe endemic, but they're not, as we estimate, the immediate threat that a lot of these individuals I've identified in my testimony we see almost every day who are attacking Jewish and non-Jewish students and Americans across the country.

Mr. GOLDMAN. Yes. Well, I mean, we can debate which is worse. Certainly the white supremacist theory affects Jews as well as non-Jews as well.

So I see my time is up. But I appreciate all of you for being here and I look forward to addressing this issue together.

Mr. PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you all for coming to testify before the Homeland Security, Counterterrorism and Intelligence Subcommittee. The threat picture Americans face is constantly changing, and with the development of AI and the use of the internet, any small group can have a relatively high impact on any given population.

Dr. Aaron Zelin, I know you have written about on-line mobilization of foreign fighters. To counter that, the United States has taken some steps through blacklisting some terror groups from posting on-line. According to Adam Hadley, the executive director of Tech Against Terrorism, who gave an interview to *Wired* magazine, big tech platforms have worked hard to create databases of known violent extremist content, known as hashing databases, which are shared across platforms to quickly and automatically remove such content from the internet. Are any of the witnesses familiar with the industry term "hashing sites"?

Mr. ZELIN. Yes, I am.

Mr. CRANE. Or groups to create a censorship database to prevent bad actors from spreading misinformation from terror groups? My question is this, how would you recommend the committee evaluate the balance between freedom of speech and the need to protect the public from terror groups using AI to conduct deepfakes?

Mr. GARTENSTEIN-ROSS. That's a good question. Thank you for raising it. I would judge it in 2 ways.

The first one is whether the deepfake poses an immediate threat. In some cases, deepfakes can be created, you know, designed specifically to incite. For example, we've seen deadly riots overseas based on Koran desecration. Something like that would have a purpose of trying to incite. In cases like that, I think that legislative efforts are important.

There are other areas that were referenced before, such as deepfake pornography and the like, where I think, again, there is a strong impetus for the legislature to step in in order to stop harm for individuals. That's essentially where I would say the line is drawn with respect to deepfakes.

I think there's other ways to deal with propaganda deepfakes because ultimately there is a purpose for deepfakes. Right? Deepfakes can be used for cinema and the like. There's a reason why people create them. They're not just pure harm, but harm to the individual, I think is the area where the legislature can come in and should be able to have a strong hand.

Mr. CRANE. Thank you, Dr. David Gartenstein-Ross, extremist groups are becoming more tech-savvy. Former Google Chief Executive Officer Eric Schmidt highlighted his worry during the February 13, 2025, hearing with the BBC. He said there is extreme risk posed by AI development that could harm innocent people. In his opinion, countries like Russia, North Korea, and Iraq have ulte-

rior motives and could misuse emerging technologies for their own purposes.

My question, is the correct balance for the tech companies and government that take into account the need for freedom of these companies to develop AI and the government's interest in protecting the public from deepfakes and AI-generated images that stir panic?

Mr. GARTENSTEIN-ROSS. It's another great question. A lot of these are difficult to answer because of the fact that it's a balance. But I'd say that this is also understood in light of an AI competition between U.S. companies and PRC-led companies. Ultimately, most people looking at it, including Mr. Schmidt, who you mentioned, believe that the country that's able to win the AI race is also going to be the global leader. So I think there's a lot invested. I'd also say, as I mentioned in my opening statement, that right now, the safeguards that are put in place, even by very responsible companies, are extraordinarily easy to jailbreak and to get around.

Mr. CRANE. Thank you.

Mr. GARTENSTEIN-ROSS. Thank you.

Mr. CRANE. Thank you. Mr. Braddock, on March 24, 2023, you were quoted in *Business Insider* saying, "If there is violence as a result of Trump's words, the former President will hide under a blanket of plausible deniability, saying that he never ordered anyone to become violent." Did you say that?

Mr. BRADDOCK. Probably.

Mr. CRANE. My question is this, you are extremely critical of Republicans through what you call stochastic terrorism, inciting terrorism through volatile rhetoric and what you deem as extremist rhetoric. But when Democrats incite violence, you seem to be a little bit silent. My colleague who just left, Dan Goldman, said Trump is dangerous to democracy and that he has to be eliminated. Did you speak out or criticize Mr. Goldman when he said that? We couldn't find anything.

Mr. BRADDOCK. I was—never, ever heard that quote.

Mr. CRANE. OK. How about this?

Mr. BRADDOCK. I can give you—

Mr. CRANE. Hold on.

Mr. BRADDOCK. I can give you examples of when I did speak out.

Mr. CRANE. Nor did you, when Maxine Waters said, tone down the rhetoric, when she encountered protesters in Minnesota to get more confrontational, encouraging Democrats to confront Trump officials if they see them in public, did you say anything about that one?

Mr. BRADDOCK. I did.

Mr. CRANE. You did? Can you provide that for the committee, please?

Mr. BRADDOCK. During conferences and stuff? Sure.

Mr. CRANE. Yes. Can I have one more quick question? How about this one? President Biden on October 23, 2024, who said we got to lock him up or that Trump was a threat to democracy right before numerous assassination attempts. Did you say anything about that one?

Mr. BRADDOCK. No. That wouldn't meet my threshold.

Mr. CRANE. We got to lock him up, that doesn't reach your threshold?

Mr. BRADDOCK. No.

Mr. CRANE. OK. Thank you. I yield back.

Mr. PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentlelady from New Jersey, Ms. Pou.

Ms. POU. Thank you, Mr. Chairman and to our Ranking Member Magaziner, for holding this very important hearing.

You know, while terrorism is by no means a new problem, the internet gives extremists a broader reach for spreading dangerous ideas. It also provides for those seeking to commit violent attacks. I was proud to join my committee colleagues last month on a visit to New Orleans to see first-hand the scene of a devastating terrorist attack on New Year's Day. We can and must do more to prevent tragic attacks like this. Doing this demand, we address how the internet radicalizes people.

In my own State of New Jersey, authorities arrested a man in November 2022 for using social media to share a manifesto containing threats to synagogues. In the manifesto, he claimed Jewish people were responsible for Muslim hatred. He drew inspiration from the white supremacist attack at a Black church in Charleston and stated a desire to attack a gay club.

Mr. Gartenstein-Ross, you have referred to this as a salad bar extremism, where an attacker lacks a clear ideology or cites numerous categories for extremist views to justify violence. How does mixing of extremist ideas impact the ability to accurately predict extremist behavior?

Mr. GARTENSTEIN-ROSS. Thank you. That's a great question.

To clarify my remarks, I refer to it as composite violent extremism, which rather than salad bar. The reason why is I think that oftentimes the internet and ideas and grievances that are in the ether impact the individual much more than they pick and choose. I think that it has a tremendous effect on complicating the idea of when someone is radicalizing to pose a threat.

If they're radicalizing with respect to a traditional ideology, oftentimes there's a few different models, but to put it simply, you can understand when they fulfill the threat criterion that they seem to, you know, have grievance meet ideological justification, and then you can look to whether they're also taking preparation. When it's mix-and-match and grievances and sentiments, I think it's much more complex and that's kind-of the petri dish that we're all living through currently.

Ms. POU. In addition to learning how to prevent on-line radicalization, sorry about that, I am interested in how we can prevent people back from dangerous ideas. Again, to you, in your written testimony, you said about terrorism prevention, "The existing toolkit remains valuable, but fine-tuning is necessary to account for the ideological fluidity, digital dynamics, and the radicalization unique to composite violent extremists." How exactly do we fine-tune and are there opportunities for on-line counter messaging?

Mr. GARTENSTEIN-ROSS. I think there are a lot of opportunities. Those which I see in the prevention sphere as being most important are when you look at the individual who poses a risk of car-

rying out an act of violence, looking at whether there are needs that aren't being met. One of the models, for example, is to look at whether there are mental health needs, who an individual could be connected to. Sometimes that provides an opportunity for interventions other than efforts to take off-line or to use content moderation to eliminate bad ideas because for as long as human history has been around, there've been a profusion of bad ideas. Legislators don't want to stop bad ideas, but what we can try to stop is that connection to violence.

Ms. POU. Thank you. Very quickly, Dr. Braddock, could you please also provide us with your thoughts? I know we have like 30 seconds, but I would love to hear your thoughts on that real quickly, please.

Mr. BRADDOCK. Is there something you'd like me to focus on in 30 seconds?

I mean, one of the things that we've been talking about over the course of this hearing is the importance of content moderation. The fact that the way that people pull their ideologies together, the fact that they pull from such disparate ideologies, makes it very, very difficult. But I think that also speaks to the fact that one of the things we mentioned earlier was the need of human eyes on these things. We want to automate everything. We want to use AI to take care of everything. But I think in situations like this, which are so nuanced, I think we do need human eyes to make these sorts of judgments. I'm not in a place to say which eyes those should be, but humans can make better judgments about nuanced content like this better than AI can, at least presently.

Ms. POU. Thank you. The word "radicalization" was difficult for me to say just moments ago, but thank you, Mr. Chairman. I yield back.

Mr. PFLUGER. The gentlelady's time has expired.

In lieu of a second round, what we will do is give each side 5 minutes, and I will hold to the 5 minutes. We won't go overboard. So after this 5-minute period, and I will yield to my colleagues for their questions, I will let the Ranking Member also yield to his colleagues if they so choose.

So at this point, we will yield 5 minutes to our side of the aisle. I will start with Mr. Zelin. Just you mentioned a couple of things on platforms, and I am kind-of interested on, you know, how do you go about, on platforms like TikTok, on platforms like Facebook, what does that training look like to recognize? We have talked about the human in the loop here and maybe go into a little bit of depth if, you know, you could wave that magic wand. What does that look like?

Mr. ZELIN. I haven't worked at these companies, so I'm not quite sure how they specifically train people, but I would imagine that they have different, you know, lessons related to understanding specific ideologies, groups, looking at the propaganda, and bringing in outsiders so that they understand the context and then build up from there. Obviously, there will be more senior versus junior people on these issues.

Then besides that, when we're talking outside of the human element, there's, of course, the digital footprint, which, you know, is the hashing methodology, but that sometimes has false positives.

Mr. PFLUGER. Thank you. I yield to the gentleman from Texas.

Mr. LUTTRELL. Thank you, Mr. Chairman. Dr. Zelin, or it might have been you, Mr. Flesch, talking about the language barriers on the social media platforms and how we are substantially behind. Is that a fair statement to say? Did I say that correctly?

Mr. ZELIN. Yes.

Mr. LUTTRELL. That is remarkable considering our ability to aggregate data in 2025. How do we fix this problem? By the way, which one—the emoji thing? I had not heard that yet. That is horrible to hear that. But OK, go ahead, sir, sorry.

Mr. ZELIN. I mean, part of it is just making sure that you're hiring people with these language skills that also know English, too, so they can work within the context of an American company. Part of the issue, too, though, when you get in that context is that usually might be working with people that live in authoritarian regimes, so they might insert people, also, and, therefore, degrade the possibility that certain things are done in a correct manner. So it gets more complicated once you get sort-of out of that Western mold of things in some ways, even if it's something that's important when we're talking about jihadis and the fact that they've proliferated in different areas in the last 5 or 6 years.

Mr. LUTTRELL. In order to combat that, I mean, AI machine learning, we got to be somewhere close.

Mr. ZELIN. It's definitely something that should be used and tried, but there are, of course, certain nuances that are used in different languages as well that we might not even know about because we're not native speakers. So that's why you also need the human element, too.

Mr. LUTTRELL. OK, thank you.

Mr. ZELIN. Yield to the gentleman from Arizona.

Mr. CRANE. Thank you. I want to come back to you, Mr. Braddock. Do you believe that President Trump is a stochastic terrorist?

Mr. BRADDOCK. I believe he has been in the past.

Mr. CRANE. Yes? Why is that?

Mr. BRADDOCK. Typically stochastic terrorism, if you want to offer a definition, is where an individual utters things that can be perceived by a reasonable person as a promotion of violence, if not outright incitement.

Mr. CRANE. So you think that——

Mr. BRADDOCK. There have been things that he has said that I think——

Mr. CRANE. So you think that President Trump is trying to incite violence?

Mr. BRADDOCK. Whether he wants to or not is immaterial. Stochastic terrorists typically don't need to be able to incite it on purpose or not. It's their words that are important.

Mr. CRANE. OK.

Mr. BRADDOCK. If I could, on the record, I could say stochastic terrorism and stochastic terrorist is a terrible term. I've actually been trying to get rid of that term as something that describes this phenomena. I call it malicious provocation, because that has to relate to——

Mr. CRANE. But you have used that word a lot, haven't you?

Mr. BRADDOCK. Yes, it's what we use in the field.

Mr. CRANE. OK. Do you think that our colleague, Congressman Goldman, with the statement I just read you, do you think he's one as well?

Mr. BRADDOCK. If I could see the context in which he said it.

Mr. CRANE. I already read it to you.

Mr. BRADDOCK. You read the statement, but I need the context as well. Statements aren't—

Mr. CRANE. "Trump is so dangerous to democracy that he has to be eliminated." I will read it for you again. Do you think that that is stochastic terrorism?

Mr. BRADDOCK. If you can tell me the context of when he said it.

Mr. CRANE. I can't tell you the context of which he said it, but those are his words.

Mr. BRADDOCK. Context is important when people say things.

Mr. CRANE. Yes. So is partisanship. I think that that is what we are seeing here today.

Mr. BRADDOCK. Is that right?

Mr. CRANE. Yes, exactly. I am going to tell you this right now. This is why Americans have such a hard time with censorship coming from guys like you. They call balls and strikes only on one side of the aisle, and then they won't do it on the other side.

Mr. BRADDOCK. Would you like me to do it for the other side of the aisle?

Mr. CRANE. Yes, yes, go for it.

Mr. BRADDOCK. Be happy to.

Mr. CRANE. Yes. OK. Tell me who on the other side of the aisle?

Mr. BRADDOCK. We talked about Maxine Waters, which I have said in public statements to threat analysts that counts as stochastic terrorism—

Mr. CRANE. Yep.

Mr. BRADDOCK [continuing]. Because the context in which she said it was already heightened aggression. So there's a bigger chance that people are going to engage in violence.

Mr. CRANE. So you don't think that anybody would take Dan Goldman's statement that Trump is so dangerous to democracy that he has to be eliminated, and you don't think that that has the potential to incite violence? Are you serious?

Mr. BRADDOCK. I don't make judgments based on statements I haven't seen in the context in which they're said. Do you want another one from the left to make it feel better?

Mr. CRANE. Yes, please.

Mr. BRADDOCK. Yes. When Chuck Schumer was on the steps of the I think it was Supreme Court near *Roe v. Wade* and a very energetic crowd and said these justices will reap a whirlwind. Does it make you feel better?

Mr. PFLUGER. The gentlemen's time has expired.

Mr. CRANE. Well, it would make me feel better if you could actually listen to the statement from Goldman and say the same thing, but—

Mr. PFLUGER. The gentleman's time has expired.

Mr. CRANE [continuing]. Clearly you can't. All right, I yield back.

Mr. PFLUGER. The Chair now recognizes Mr. Magaziner.

Mr. MAGAZINER. All right, thank you. I thank the Chairman again for a, I think, productive, enlightening, and mostly bipartisan hearing today. I think this was actually a very productive back-and-forth for the most part. So I thank you guys, all of you, for your insights. I probably won't use my full 5 minutes, but there are just two things I wanted to follow up on real quick.

We had, I think, a very good conversation about where the line should be in terms of free speech, you know, inciting violence versus not, and about methods of content moderation that we should encourage and potentially legislate. One thing that we haven't delved into is the algorithms. So I wonder if any of you have any insight into that. Should there be certain standards or best practices that the social media companies should adhere to in terms of algorithms that kind-of lead people deeper down the rabbit hole to more and more extreme content? Or is it not really a matter of policing the algorithms, it is more just about the underlying content? I ask any of you to weigh in.

Mr. GARTENSTEIN-ROSS. I would counsel the legislature against trying to moderate or legislate for algorithms. There's a lot of problems with algorithms. There have also been attempts to legislate algorithms before. Specifically, both Florida and Texas implemented bills known as anti-censorship bills, which, among other things, would limit the amount of times that social media companies can change their algorithms, No. 1, and No. 2, demand algorithmic transparency.

The reason why I personally was against those bills is, No. 1, algorithms change constantly, and I think it's anti-free enterprise to try to limit the number of times they can change algorithms. No. 2, if they reveal what's going on with algorithms and what they're flagging, then every single bad actor knows exactly what those companies are looking for. So I think to me right now, I think the safest thing is to stay away from their algorithms.

Mr. MAGAZINER. OK. No, that makes sense. That is a helpful answer.

Last issue, and this is more of a comment than anything else, the importance of open-source data collection I think is important. You know, when we talk about Signal's intelligence and trying to find bad actors who commit acts of violence before they can commit those acts, you know, we often are thinking about covert methods. But as I understand it, with the attacker in New Orleans and many others, I mean, oftentimes people are posting stuff openly and in an environment where the social media companies are not effectively regulated and some aren't removing that content or not doing it in a timely way. It's important to have, you know, Department of Homeland Security I&A office, which does open-source collection. National Counterterrorism Center has an open-source desk. So I just want to make sure that we are emphasizing the importance of those collection efforts as well when we are making budgetary decisions and the like, because we need to be putting more resources toward that, I think, not less.

You know, with the time I have remaining, I just ask any of you, is there something that you were dying to say that we didn't get to? If you want to take a final minute here. I see, Dr. Zelin, go ahead.

Mr. ZELIN. I'll just add to your comment that I think, you know, working together amongst Government agencies is important, but I also think Government to tech companies important and between tech companies because I think all of us in this room know that we all use more than just one social media application or other, you know technology in our phones or what have you all the time. So it's, you know, just as we do, so do the terrorists in some ways. These are commercial usages. So there needs to—even if when we're talking about the digital footprint type of issue, that's one aspect of it. But there also needs to be greater coordination.

One of the issues where we get to is when it's companies outside of sort-of the American jurisdiction or they're companies that are in adversarial countries, like TikTok with China or DeepSeek and things along those lines, that makes it that much more complicated. That's why, you know, talking about bans and things like that is something that I think should continue to be on the table.

Then one more point related to the algorithms, while I agree with Daveed that it's definitely complicated from a legal perspective, we should also recognize that if you follow somebody on whichever platform, they'll start feeding you recommendations. If you start following people that are terrorists or extremists, they'll feed you people within that broader network or if you're watching videos along those lines. So that's one aspect of the algorithm that maybe should be looked at in greater detail.

Mr. MAGAZINER. All right. I thank you all again for a good, productive conversation. I will yield back.

Mr. PFLUGER. Will the gentleman yield for 10 seconds? We had a conversation up here, just so you are aware, that I think what Energy and Commerce is doing to look at Section 230 is very important. That is really a lot of what we talked about here. I hope that that committee will take this issue very seriously.

Mr. MAGAZINER. Agreed.

Mr. PFLUGER. I thank the witnesses for your testimony today, for your study in this field, for the conversation that we have had. The Members of the subcommittee may have additional questions for the witnesses. We would ask that you respond to these in writing. Pursuant to committee rule VII(E), the hearing record will be open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 3:46 p.m., the subcommittee was adjourned.]

