Strategic Security Analysis

White Crusade: How to Prevent Right-Wing Extremists from Exploiting the Internet

Christina Schori Liang and Matthew John Cross

Photo: Anthony Crider
Key Points

• The rise of right-wing extremists (RWEs) in the West has been neglected in the global battle against terrorism until recent high-profile attacks.

• Copycat terrorism is becoming the new modus operandi of nation-based, lone wolf extremists who are inspired by previous terrorist attacks and leave instructions for others to follow, refreshing the cycle of violence.

• RWEs are profiting from the global disruption brought on by the Covid-19 pandemic by promoting conspiracy theories, racism and plotting large-scale violence to start a civil war or a ‘race war’ as seen during the ongoing protests.

• RWEs have created an effective strategy that uses several off and online tools to help carry out their operations and recruit new members.

• The internet has become the most important tool of RWEs to spread propaganda, plan events, recruit, finance and communicate. It provides unparalleled opportunities to reach broader audiences with subversive exposure.

• RWEs are effective at subversive exposure: infiltrating non-extremist sites and skirting moderation efforts, rendering conventional online strategies ineffective.

• Counter-narrative programmes to explicitly deconstruct and delegitimise propaganda may be the best way forward in breaking down RWE networks and influence.

About the Authors

Dr. Christina Schori Liang is Head of Terrorism and PVE at the Geneva Centre for Security Policy (GCSP). She is the Director of the New Issues in Security Course (NISC) and contributes to (Track 1.5 and Track 2) dialogue events and research. Dr. Liang has testified for the US National Intelligence Council, the European Commission, NATO and the OSCE. She is a Visiting Professor at the Paris School of International Affairs, Sciences Po.

Matthew John Cross recently received his master’s degree in International Security from the Paris School of International Affairs, Sciences Po. His research interests focus on countering violent extremism and ethical intelligence. He previously worked for the Royal Canadian Mounted Police, developing international capacity building projects. Mr. Cross received his bachelor’s degree in honours P.P.E. from Mount Allison University, Canada.
Introduction

Right-wing extremists (RWEs) are using the current protests over police brutality in the United States as a cover to commit terrorist acts and to grow their numbers. They present a significant danger to public safety and security and are a growing threat in the West. Despite this, the rise of right-wing extremism (a homogenized term for white ethnonationalists, alt-rights, white supremacist groups, male supremacist groups, and right-wing anti-government extremists) has not been afforded the priority and attention it justly deserves. There are three reasons for this. First, the global narrative maintains that terrorism rests almost exclusively in the hands of a balaclava-clad Salafi-jihadist holding a Kalashnikov. Second, Western right-wing media has largely pushed back against covering the rise of right-wing extremism and the media as a whole has failed to contextualize the systematic threat RWEs present. Third, the global pandemic has forced governments to focus their attention on maintaining public health and socioeconomic order and have consequently failed to see how RWEs are subversively using the pandemic to support and expand their own agenda.

RWEs have utilized the lawless and unmoderated internet to reach broader audiences, disseminate literature, and target vulnerable people. They have done so quietly, pushing an ideological campaign that manifests itself under the surface of popular internet discourse, rather than the aggressive proselytizing of Salafi-jihadist groups like the Islamic State. These efforts can be understood as a kind of subversive exposure, where memes and fake news dominate discourse. This paper will analyse the scope of the RWE threat, describe their latest modus operandi, and explore how the pandemic is being instrumentalized by such groups and how the internet has become their principal tool and battleground. The paper will then provide theory and evidence for how counter-narrative programs, especially through digital disruption, can help neutralise the threat.
Right-Wing Extremist Practices and Theories

How the Threat of Right-Wing Extremism Manifests in the West

In the West, right-wing extremism is a less understood and pressing issue for people than the threat of Salafi-jihadist terrorism, which is overreported in the media relative to other types of extremism, although this is slowly starting to change. Despite this, right-wing extremism has had a greater impact on the lives of people affected by attacks because RWEs commit more attacks. One report found that in the United States, from 2010 to 2019, 20 percent of extremist-related killings were caused by someone affiliated with Salafi-jihadist extremism, while more than three quarters of extremist-related killings were caused by someone affiliated with right-wing extremism. This issue is exacerbated by the fact that views of RWEs are more pervasive and accepted in North America, where some extremist beliefs are normalized by both politicians, lawmakers and civil society. In May 2019, the FBI testified to Congress that they were pursuing about 850 domestic terrorist investigations, of which a “significant majority” were related to white supremacist extremists.

In Europe, the percentages of RWE-related killings are lower than that of their North American counterparts, but this is due in part to recording issues. Extremist attacks in Europe are often cited in court under hate crime offences, rather than terrorism offences, muddying the respective figures between the two problems. Despite this challenge, the number of incidences and arrests for RWE attacks in Europe has risen each year since 2016, and counter-terrorism operations in Western Europe to combat RWE activity have almost tripled between 2016 and 2018. In 2020, Germany’s top security threat was identified to be far-right terrorism. German Interior Minister Seehofer called right-wing terrorism “the biggest danger to democracy in Germany.” The growing threat of RWEs has made the need for response evident, as right-wing networks appear to be better armed and larger than originally thought in Europe.

The threat of right-wing extremism, despite the reticence of the media in reporting it, has grown more visible in recent years. The 2019 Global Terrorism Index highlighted that far-right terrorism incidents have increased 320 percent in the past five years. In the attack on two mosques in Christchurch in 2019 which killed 51 people, the right-wing terrorist posted a manifesto the day before and livestreamed the attack on the internet. Facebook reported that the video was shared 4,000 times before it was removed and that within 24 hours individuals had attempted to re-upload the video 1.5 million times. Concurrently, the number of attacks by RWEs are growing each year, as are their transnational links. Extremists from Australia, Canada, Russia, South Africa, and elsewhere are sharing expertise on recruitment, financing, and propaganda. Geographically, Eastern Ukraine has become the hub that links transnational white supremacist groups. Far-right foreign fighters have been traveling there since the conflict began in 2014 between pro-Russian separatists and Ukrainian government forces. So far 17,000 fighters from 30 countries have flocked there, contributing to both sides of the conflict hoping to acquire combat experience in order to take the fight home.

As of now, most attacks are undertaken by nation-based, lone wolf extremists, the most difficult attacks to predict and to prevent. Unlike violent Salafi-jihadists, RWEs have been unable to orchestrate large attacks, preferring instead to conduce lone wolfs into committing attacks and hoping copycats will follow. In the 1980s, Louis Beam, a veteran of the Vietnam War, a member of the Ku Klux Klan and an activist for the
Aryan Nation, advocated for what would become the most influential modus operandi of the racial supremacists. Arguing attacks were increasingly difficult to launch because of law enforcement agency’s ability to infiltrate groups, he suggested a tactic of ‘Leaderless Resistance,’ where small cells or lone wolves would carry out non-coordinated attacks. This model is being adopted by modern RWEs who are following the lone-actor small cell model.

Media presentations of terrorist acts can also have a powerful influence on moving terrorist sympathizers to commit terrorist acts. Social psychologists have called this the ‘behaviour contagion’ or ‘copycat actions,’ where an individual could take their cues and beliefs from events presented by the mass media, allowing them to self-radicalize without central control. Like-minded individuals could then stage their own attacks on the same or similar targets as their idol. In this way, insurgency can be launched against an ‘oppressive government’ without direction.

With the advent of the internet, modern extremists can now self-radicalize faster than ever before and more importantly, they now have a playbook to follow. The Christchurch shooter followed a specific pattern, including a pre-planned online manifesto distribution strategy and a Facebook video livestream. In his manifesto, the attacker, Brandon Trenton, said he drew inspiration from similar attacks, especially Anders Breivik, a Norwegian RWE who killed 77 people, mostly youths who were participating in a summer camp in Utøya. The shooter explained in his manifesto he had been inspired by similar right-wing attacks in Norway (2011, 77 killed), Charleston, South Carolina (2015, 9 killed), and Quebec (2016, 6 killed). This has led to a growing fear of copycat attacks given the simplicity of the attacks these extremists use.

With the advent of the internet, modern extremists can now self-radicalize faster than ever before.

(Source: The Economist, March 18, 2019)

Since 2011, one third of white supremacist attackers were inspired by others conducting similar copycat attacks, professing admiration for them online. The attack in Christchurch inspired copycat killings in 2019 in Poway, California (1 killed), El Paso, Texas (22 killed) and Halle, Germany (2 killed); each of these attackers drawing inspiration from Trenton. The perpetrators of the Christchurch, El Paso, Halle and Bærum all announced their plans on 8chan or other, similar online forums and sought to live-stream their attack on major platforms to maximize their impact. These attacks follow similar trends: the extremist is ‘educated’ by propaganda, often starting online with memes; they begin to join and engage in
forums, causing their views to radicalise; they begin to create their own work, such as manifestos; and then they commit violent acts, inspiring copycat killings and thus refreshing the cycle.

How the Threat of Right-Wing Extremism Manifests Online

The rising trend of RWE attacks, and the apparent interconnection and inspiration between each new terror act, demonstrates the immediate need for a way to combat this form of extremism at its source. Western agencies must shift focus and intelligence by penetrating far-right networks to prevent future attacks. To do this, they must recognize that extremism has moved quickly towards the online domain and must respond accordingly by understanding the theory of how people become radicalised. Looking at the process of self-radicalisation exhibited in recent attacks, it would appear that the process for right-wing radicalisation is similar, if shortened and less formal, to Horgan’s theory of how child terrorists are socialized in six stages: seduction; schooling; selection; subjugation; specialization; and stationing. RWEs lure unsuspecting victims into their world (seduction); educate them on the tenets of the beliefs (schooling); select the most viable candidates for extremism (selection); and disperse information on how to plan and organize various types of attacks (specialization). Because of the online nature of these relationships, there appears to be no physical subjugation, although it is likely that mental subjugation and bullying are used to break down a victim’s mental state. Likewise, stationing is determined by the location of the lone wolf, rather than by a central command, although the attacker could be encouraged to strike certain targets.

It is also important to recognize that right-wing extremism is not the only extremism prevalent on the internet. For example, the Islamic State (IS) possesses “a sophisticated and effective communication strategy that uses online media tools to disseminate its multidimensional propaganda. It has populated social media platforms and has attracted a global network of supporters that articulate, magnify and circulate its violent extremist messages worldwide.” Both groups now use the internet to propagandize their beliefs and proselytize to vulnerable people, populate social media with their content, raise funds, and organize protests and other events.

In fact, RWEs were the first to instrumentalize the internet when, in 1988, white nationalists used the internet to discuss effective tactics, resulting in the murder of an Ethiopian immigrant in Portland, United States. However, despite the operational similarities of these two groups, their differences must be recognized to effectively combat them. The difference between IS and RWEs, and the key to understanding how to combat them, is to recognize the difference in how they use the internet to achieve their goals, which can be divided into two stylistic methods defined for this paper: aggressive exposure and subversive exposure.

The Difference between Aggressive and Subversive Exposure

Aggressive exposure is the style IS has used in its online efforts against Western media: furiously controlling the narrative with force and heavy engagement, bringing ‘cyber-jihad’ to a whole new level. Their media campaigns promote terror through graphic images and videos and active engagement in spheres they do not control. Aggressive exposure relies on controlling the entire media sphere that IS exists in, ensuring that dissident voices are silenced or removed and that there exists no countervailing voice to its proselytization. In contrast, right-wing
Extremism possesses a second method for promoting its views. Like IS, right-wing extremism’s basic methodology has been to openly show itself online, on websites like 4Chan or Stormfront, where users can discuss and promote their radical beliefs without interruption. This indoctrinates those already holding preconceived beliefs about white supremacy, or anti-government ideals. But although this method is effective at riling up an already-established base, it is less effective at targeting people who might have views that resemble RWEs, but who do not yet hold any strong beliefs towards the subject nor have a willingness to actively think about them; it may even push them away from radical views.

This is where right-wing extremism benefits from its more accepted position in Western media, by using the second and more seditious method of engagement, subversive exposure, for online intrusion. Subversive exposure involves the use of disinformation, deception, duplicity, and the normalization of extremist right-wing ideas to lure ignorant and vulnerable people, like youth (and especially gamers), into right-wing groups, without them knowing that it is a radical group. For example, extremist groups use memes (an idea, message, or joke spread over the internet, usually a combination of a visual and a text overlay) to create inside jokes with supremacist undertones that are commonly shared on websites like Instagram. Such memes joke about how global warming is a leftist plot, how Donald Trump is actually the “God Emperor” of the earth, or how it would be better if the Holocaust had happened. They can even create a connection between the founding fathers and contemporary RWEs, as evidenced by the meme below.

(Figure 1 Pepe Meme: https://me.me/i/20325520)

These memes are not meant to turn someone into a RWE, but to be funny and subversively evocative, to get them to thinking about whether the views they had been taught are true, or if alternative facts are available. For right-wing extremism, the slow radicalisation of unsuspecting victims begins with this type of subversion, where standard norms of decency become unwound and RWE views are bandied about with other mainstream jokes. Importantly, the normalization of these RWE views begins by virtue of being a
’harmless’ online tactic, defensibly nothing more than a joke. This allows these memes to generate more interaction and consequently begin to normalize these views, or ideally, have them be seen as countercultural opinions.

Pepe the Frog, an internet meme, serves as an example to this subversive exposure. The cartoon frog, created for humour on a non-political site, became appropriated as a popular figure in far-right circles. Recent appropriations of Pepe as Hitler, a Klansman, and multiple racist caricatures has earned the frog a spot in the ADL hate symbols database. But what gives memes like Pepe their power is their ability to spread messages quickly. Because they use widely recognizable visuals and text formulas to pass their message (referencing famous movies, pop culture, famous political events), they are effective at generating ‘lols.’ Whether their content is comedic and light-hearted or angry and nihilistic, they make the viewer laugh and easy to consume no matter the message. Memes, whichever way they are generated, can effectively convey a message to millions of people across the world and are incredibly effective at targeting youth on sites like Reddit or Instagram. The result of this is a format for disseminating information virally, regardless of its veracity.

Attracting youth through memes and other sources has become an integral part of the RWE strategy. Over the last four years, RWEs have made a concerted effort to recruit and proselytize at college campuses, which has become their new battleground for hate. RWEs are using groups like Turning Point USA, the American Identity Movement (formerly Identity Evropa), and the Patriot Front to promote their extremist views. While these groups aim to foster right-wing communities on campus spaces with sometimes mainstream views, these groups have come under fire for promoting extremist ideology. For example, Turning Point USA has had to repeatedly fire coordinators for racist actions or for promoting extremist views at conferences. While these groups promote right-wing views with propaganda campaigns like leaflet drops or the disruption of on-campus activities, the extremists within quietly foster hateful communities. These events are coordinated on a national scale through channels like Gab and Telegram, masking their efforts in digital secrecy. Their results are informative: during the last week of November 2019, there were hate incidents reported on five different campuses in the United States. According to the ADL, white supremacist material being circulated in the US grew by 120% in 2019. These particular efforts are done without having to control the entire sphere of discourse, making them far more successful for infiltrative actions. Consequently, aggressive exposure and subversive exposure rely on fundamentally different online tactics and they must be treated differently for both to be neutralized effectively.

How Subversive Exposure Empowers Right-Wing Extremism

A study by the Institute for Strategic Dialogue has found the value this subversive exposure can create is immense. Britain First, a far-right political party, used this simple but deceptive strategy to gain fans, posting content about issues that attract popular support in the state, like opposing child abuse or animal cruelty, or the benefits of Brexit for the NHS. Then, after gaining new followers through what could be construed as harmless but patriotic views, they slowly began to equate these ideas with more openly xenophobic and anti-Muslim messages. This did two things: first, it normalized radical views by connecting them to more mainstream views; and second, it slowly pushed the beliefs of new followers towards the right, helping them develop biased views.
on these issues. In June 2016, after the murder of British Member of Parliament Jo Cox, Britain First saw a jump in visibility of 251 percent and a follower increase of 15 percent, gaining “a disproportionate share of voice in the days following Jo Cox’s murder as their name was referenced an exceptional amount of times.”  Although most sentiment surrounding Britain First was negative, a small but significant number of people were attracted to the group after this terrorist murder, because it made them think about the realities of what they were being told and by whom. It is in these small spaces of the internet that subversive exposure attracts people towards extremism.

The sum of this aggressive and subversive exposure by RWEs is an internet co-opted by extremism: there exists a right-wing extremism undercurrent on the internet, one that entwines itself through the largest communities, like Facebook and Reddit, and pushes the dialogue further right, until people enter the smaller communities, their controlled sphere of total influence. Colloquially, this environment is known as the electronic community of hate. Though the number of active RWEs online is relatively small, they create significant noise and cause significant disturbance in non-right-wing communities. They are particularly effective at latching onto influencers like Joe Rogan, an American comedian, mixed martial arts commentator, and host to the world’s most popular podcast, and PewDiePie, a Swedish comedian, philanthropist, and currently the most subscribed YouTuber in the world. While these men may not actually promote extremist views themselves and have denounced violence, they have both seen controversies in promoting guests with a history of extremism, which has attached a negative label to their brands. RWEs have used these controversies to infiltrate their respective communities and create gateways towards right-wing extremism.

It is also important to recognize that governments are not the only ones involved in this fight. To put it bluntly, there is a joint failure by mainstream media and social media to combat this subversion. As the New York Times editorial board states, “the fundamental design of social media sometimes exacerbates the problem. The algorithms that underpin these networks also promote engaging content, in a feedback loop that, link by link, guides new audiences to toxic ideas.”

A study on information spread found that misinformation flourishes online because users aggregate in communities of interest, which cause reinforcement and fosters confirmation bias, segregation and polarisation. In turn, these online echo chambers cement dubious notions, giving them a semblance of legitimacy which builds an increasing separation from reality.

Western media, in refusing to denounce right-wing extremism or warn against it, has helped normalize this practice; a major criticism they receive is labelling white shooters with mental health issues, rather than extremist ideologies. Social media has also not taken adequate safeguards to stop the spread of extremism, allowing it to fester and grow. RWEs are free to propagandize and coordinate attacks, but more importantly, they can recruit vulnerable people.

RWEs use social media to promote the ability to self-radicalise, by creating echo chambers and recursive loops that drag the vulnerable down toward right-wing extremism. This is important, because although historical evidence suggests that self-radicalisation and self-recruitment via the internet exclusively are still unlikely, research is now saying that the internet does increase the opportunities for self-radicalisation, potentially from start to finish. This field does require more research, although it is difficult to find willing participants. Crucial to this point, growing evidence suggests RWEs might differ from other extremists in radicalization: often, the kernel of extremism they need to push can come entirely from online discourse, like seeing memes about minorities or
questioning their identities. They do not necessarily need a seed from outside, because subversive exposure plants these seeds without them actually knowing it, which means that any attempts to combat this issue must do so with this understanding in mind. Combating RWEs online must therefore consider how to disrupt the seeding before germination.

Right-Wing Extremism During the Covid-19 Pandemic

How Right-Wing Extremists are Exploiting the Covid-19 Pandemic

Unsurprisingly, RWEs have been quick to capitalize on the Covid-19 pandemic; extremism thrives in times of economic distress. Studies have shown that financial crashes cause voters to be attracted to the political rhetoric of the extreme right, which often attributes blame to minorities and foreigners, causes outside the control of the voter but still affecting their lives. RWEs are seizing upon the uncertainty and turmoil the global pandemic has caused, profiting from the uncertainty and anxiety brought on by the public health threat and the massive job losses. On platforms such as Facebook, 4chan, 8kun and extreme right Telegram channels, the pandemic has generated a huge amount of excitement, with users reveling in the opportunity to indulge in conspiracy theories, racism, and incite social turmoil and even ‘civil war.’

As regards conspiracy theories, Covid-19 has sharpened in-group and out-group boundaries and has enhanced out-group prejudice, triggering fears of foreigners and increasing general feelings of xenophobia. Online narratives rooted in racism and bigotry are evolving and transforming in the new social context created by the pandemic. American, European, and Oceania RWEs have disparaged all non-white immigrants in the past and are now using the context of Covid-19 to scapegoat them further by spreading conspiracy theories about the origin of the virus and its virality. Historically, RWEs have cast immigrants as vectors of disease who poison both the physical and moral health of race. The global pandemic has provided the ideal opportunity for repackaging this thinking, to create posts across Facebook, Twitter, Telegram and WhatsApp groups that identify narratives claiming mosques and Muslims are spreading Covid-19 and that the “UK’s Muslim population is responsible for a quarter of the country’s Covid-19 related deaths.” In the United States, Chinese and Jewish populations are being targeted for spreading the disease. In May, the FBI warned police forces nationwide that white supremacists were encouraging followers to deliberately spread the Covid-19 to Jewish communities, Muslim communities, and police officers by spreading the disease with human saliva. A man suspected of planning to bomb a hospital in Missouri was killed when FBI agents tried to arrest him; he had ties to two neo-Nazi groups. The man had considered other targets, including a mosque and a synagogue, but chose a hospital because of the increased media attention on the health care sector during the pandemic.

The global pandemic had provided ideal opportunities for RWEs to repackage enduring extreme-right conspiracy theories about ‘Jews’ and ‘Muslims’ and the perils of ‘globalization’ and ‘liberalism’ worldwide. Some prominent voices are claiming that Covid-19 is a tool for the Jewish and/or Chinese peoples to expand their global influence. The pandemic is also supporting movements in Europe inspired by the French author, Renaud Camus whose book Le Grand Remplacement wrote about the “crisis of mass immigration” which he identified as an “assault on the European
people that if not combated, will ultimately result in the complete racial and cultural replacement of the European people.” Members of the French Les Identitaires movement share similar ideas, while they claim to reject violence, their xenophobic ideology of protecting European identity from cultural corruption feeds directly to it and is now further propagated by the fears of immigration during Covid-19. The New Zealand terrorist entitled his manifesto “The Great Replacement” and despite being censored it still circulates among extremists worldwide. In the United States, RWEs are claiming that white people are being replaced by hordes of immigrants from Latin America and by a growing native-born Latino population.

**Spreading Hate Online and Digital Activism During the Lockdown**

RWEs are also spreading bigotry and racism. Xenophobia exists on fringe Web communities but is also becoming more visible in mainstream ones. RWEs have been actively scapegoating non-ethnic whites to build a bridge from the fringe community to the mainstream spheres. With campuses emptied due to the global health crisis, RWEs have lost their traditional methods of recruitment and harassment in targeting college spaces. They have now transitioned to online harassment strategies like ‘Zoom Bombing’ online classes in the quest to attack and troll professors and students by shouting racial slurs and sharing violent videos. One situation in May saw a community group in East Oakland, California inundated with trolls, who began to shout profanities and racial slurs; there have been hundreds of reports of far-right and white nationalist trolls, virtually attacking Zoom meetings, including virtual meetings of synagogue congregants. RWEs are practicing virtual intimidation by doxing: the act of sharing the confidential personal information of those they scapegoat or wish to see harmed. While most of the grassroots RWEs have traditionally relied on public meetings, demonstrations, and concerts for mobilization, during the lockdown their activism has been pushed online. Neo-Nazi bands deprived of live performances are propagating their ideology through Covid-19 themed music videos. RWEs are adding neo-Nazi paraphernalia and KKK-inspired Klan hoods to their sweaters to comply with social masking measures and selling these designs online. Using the opportunity to quickly find innovative ways to continue pushing their message, the co-founder of the Patriotic Europeans against the Islamization of the Occident’ (PEGIDA) has organized weekly virtual marches online. His YouTube channel ‘LUTZiges,’ a pun of his name and the German word lustig (funny), invites people to his ‘virtual evening march’ every week, which, in early April, attracted over 1000 participants.

RWEs are also profiting from the global pandemic by inciting social unrest, with several groups plotting large-scale violence in the hopes it will start a civil war and ultimately a ‘race war.’ Within the groups inciting social unrest, there is a growing terrorist threat emanating from so-called “accelerationist” groups. These accelerationist groups believe that by sowing chaos and violence they will be able to hasten the collapse of society through civil war; allowing them to build a white ethnostate in its place. A neo-Nazi, accelerationist, paramilitary hate group calling itself ‘The Base’ hopes to give rise to a white ethno-state of its own in the US Pacific Northwest by killing minorities, particularly African-Americans and Jewish people. Formed in July 2018, and led by an American residing in Russia, some members of The Base were recently arrested for plotting an attack at a gun rights rally in Richmond, Virginia. Their plans were as wide-ranging as they were chilling: “Derail some trains, kill some people, and poison some water supplies.” Among those arrested was a Canadian
Armed Forces Reserve Combat engineer. They were accused of building assault weapons and producing the drug DMT. It is also apparent that The Base closely follows the model of Al Qaeda and the Islamic State, working to radicalize independent cells or lone wolves. The group has dozens of members worldwide, runs paramilitary and survivalist camps, and recruits online with dubious methods.

Another such group promoting this accelerationist rebuilding of society is known as the “Boogaloo Bois/Boys.” It is a movement first noticed in 2019, when fringe groups from gun rights and militia movements to white supremacists began referring to an impending civil war using the word boogaloo, a joking reference to “Breakin’ 2: Electric Boogaloo,” a 1984 sequel movie about breakdancing and a common meme in its own right. Boogaloo Bois fundamentally believe in their right to bear arms and profess a willingness to begin the armed overthrowing of the government if that right is threatened. They believe in armed insurrection as a means of installing their preferred government. The Boogaloo Bois have fostered an online community with tens of thousands of members, using an ideological base that has attracted both hard-line libertarians and anti-government extremists. This has made it difficult for social media moderators to foil their online groups and interactions, since the movement includes both violent accelerationist and white nationalists, who hope to spark a civil or ‘race war,’ and libertarian ‘shitposters’ who believe boogaloo is countercultural and ironic.

In early June 2020, the Boogaloo movement gained greater notoriety when armed Boogaloo Bois began showing up to anti-police brutality protests in America, which were sparked by the inhumane police killing of George Floyd in Minneapolis. The incident has generated demonstrations against police racism, brutality, and lack of accountability in over two thousand US cities and multiple cities across the world. Some Boogaloo Bois are trying to position themselves as allies of Black Lives Matter (BLM), believing they share the same disapproval of government law enforcement; they have been appearing at protests to defend black protesters from police. However, it would also appear that most members are instrumentalizing BLM demonstrations in the hopes of wreaking havoc, inciting violence, and sowing chaos, helping to turn protests into riots. Ultimately, their presence has had the effect of instilling fear in the demonstrators and distracted from the real purpose of the demonstrations, which is to highlight police brutality against the African American community in the United States.

The Boogaloo movement is also rapidly gaining followers due to the Covid-19 pandemic. A recent report concluded that more than 60% of the 125 identifiable Boogaloo groups on Facebook have appeared since January, picking up many devotees during the Covid-19 lockdowns in the US. Recently, boogaloo is blowing up on TikTok, where the #Boogaloo hashtag gained over 2 million views. TikTok, a Chinese-owned app, is full of teens dancing with guns and cracking jokes about starting a civil war. It is a sign that the Boogaloo movement, despite its violent foundations, is being adopted by the mainstream due to its innate humour. In Las Vegas, three Boogaloo Bois (one active-duty member of the Army and two veterans) were charged with trying to provoke violence at a BLM protest. They are facing federal charges for allegedly bringing explosives to the event. In Oakland and Santa Cruz, California, a US Air Force sergeant was accused of two ambush-style attacks on law enforcement officers, allegedly murdering two and wounding two others. He allegedly wrote “boog” and the phrase “I became unreasonable” (a popular meme among boogaloo groups) on the hood of a van that he hijacked. These attacks took place during BLM protests. Another member was recently arrested in

The Boogaloo Bois have fostered an online community with tens of thousands of members, using an ideological base that has attracted both hard-line libertarians and anti-government extremists.
Texas while allegedly attempting to find and kill police officers, streaming his actions on Facebook Live. Boogaloo supporters were also arrested at demonstrations in Colorado, Texas, and Ohio in recent months.

At the Network Contagion Research Institute (NCRI), researchers analysed more than 100 million social media posts and comments. They found that through the use of memes, extremists have pushed anti-government and anti-law enforcement messages across social media platforms. The memes are either considered “humorous” or represent physical violence and militaristic shows of force similar to armed militias like III Percenters or the Oath Keepers. The Boogaloo movement not only uses social media to share memes but also to “strategize, share instructions for explosives and 3-D printed firearms, distribute illegal firearm modifications, and siphon users into encrypted messaging boards en masse.”

According to NCRI, the Boogaloo concept has been monetized, with merchandise advertised through Facebook and Instagram advertisements and marketed to current and former members of the military. NCRI represents a breakthrough case study in the capacity to identify cyber swarms and viral insurgencies in nearly real time as they are developing in plain sight.

How Right-Wing Extremists are Accelerating White-Jihad Online

The White-Jihad touted by Accelerationist and Neo-Nazi groups is posing an imminent and direct threat to law enforcement, government authorities, and minority and civil rights groups. As tensions escalate due to the global pandemic, and Covid-19 leads to widespread economic uncertainties and massive unemployment, boxed-in audiences already glued to a 24-hour news cycle sensationalizing every disaffected group and global calamity will be increasingly ripe for conspiracy theories and hatred. Within already-tense communities previously impacted by racial divides, gun violence, and political polarization, this tension is even more exacerbated. Unfortunately, what is already bad in these online communities will surely become worse, as these new hate narratives are being shared more frequently across both fringe and increasingly mainstream. “According to Rickli, a growing global trend during Covid-19 is that multiple actors from politicians to fringe groups are exploiting the crisis by spreading disinformation and ‘fake news.’ This in turn is helping extremists to feed existing and emerging far-right conspiracy theories in the hopes of accelerating polarization and ultimately attempting to break-down the current “System.” One channel issued an eight-point plan for “the boog,” a term used to denote what they believe to be a looming civil war. Their advice included acts of terrorism and sabotage, asking people to “encourage locals to join your cause, if have to do it by force (sic)” and “attack key locations for federal entities, NATO outposts, and military presence.”

Concurrently, these groups are using the pandemic to sharpen condemnations of ‘the system’ and encourage people to lose hope in normal political processes. Neo-Nazi parties are advising followers online that large protests would be a good opportunity to commit murder. Such posturing, which often combines nihilism, exhortations to violence, and racism, are shared by groups like the Atomwaffen Division, The Base and Feuerkrieg Division.

It is likely RWEs will continue to attempt to radicalize and recruit veterans, designing seditious memes tailored for infection among active service members and veterans.
While incidents of soldiers holding extremist views are still marginal, social media is amplifying their threat because the expertise they share on social media can make attacks significantly more effective and lethal.

White supremacist leaders were actively recruiting active-duty soldiers and recent combat veterans. In 2019, US Coast Guard Lieutenant Christopher Hasson was arrested and sentenced to 13 years in prison for plotting extreme right-wing terror attacks on a scale rarely seen before. He called for ‘focused violence’ to establish a white homeland. The worst right-wing attack on US soil was perpetrated by a Gulf War veteran, Timothy McVeigh, who killed 168 victims in 1995 with his bombing of the Alfred P. Murrah Federal Building in Oklahoma City. While incidents of soldiers holding extremist views are still marginal, social media is amplifying their threat because the expertise they share on social media can make attacks significantly more effective and lethal. For example, US Army Specialist Jarrett William Smith was charged with distributing bomb-making information largely due to the bomb-making lectures he was distributing over social media.
Disrupting Right-Wing Extremism Activity Online

Why Current Policy Fails to Combat Right-Wing Extremism

According to Cederberg, cyber power is a global game changer. He points out that “it brings along new asymmetries to power politics. All aspects of our lives and functions of our societies will be transformed by all-pervasive and hyper connected digitalisation.” RWEs know this truth better than most. Fighting them in cyberspace is different too; there are few physical bases of operation, no figureheads to decree a caliphate, and no possibility to use drones. While it is true that right-wing networks and individuals have broadened their contacts in other countries, especially in Europe and North America, the perpetrators of right-wing terror acts have mostly been lone wolves or small networks of nationalists, not large groups. Consequently, conventional neutralization operations are very ineffective against RWEs. Preventing and countering violent extremism (P/CVE) operations against right-wing extremism must therefore focus more on the internet than in the field.

In the West, and especially the United States, a game of catch up to right-wing extremism is occurring. According to a report from 2018, "For two decades, domestic counterterrorism strategy [in the United States] has ignored the rising danger of far-right extremism. In the atmosphere of wilful indifference, a virulent movement has grown and metastasized.” RWEs have had decades to burrow into the underbelly of the internet, a significant part of why current methods to counter right-wing extremism have been unsuccessful, as they are based on P/CVE against Salafi-jihadist-type terrorism. For Salafi-jihadist terrorism, which has been vilified in the public psyche for years now, educating the public to fear extremism and embrace moderation has been a worthwhile tool in the P/CVE playbook. But while there has been an attempt to counter the pull of right-wing extremism influence with the same method of building resilience among populations vulnerable to radicalisation, it has not been nearly as effective.

Because right-wing extremism has lived under the surface of public psyche for decades, it is far more difficult to create education campaigns vilifying right-wing extremism or educating about the harm it causes. Recalling the example of memes shared on Instagram, it is far more likely a vulnerable teen will relate to what makes him laugh, even if it is a sad frog named Pepe, than it is to some government-sponsored program that causes him to think about the nature of the things he sees. Perhaps even more importantly, he will be exposed to many more right-wing memes than he will to government P/CVE writings; the prevalence of subversive exposure by RWEs assures that. Contrast that to Salafi-jihadist propaganda, which will not show up on social media at rates dwarfing its inverse, and it becomes clear to see why these strategies do not work equally well. RWEs are far better positioned to radicalise online.

To compensate for this, governments in the West have tried to respond to this competitive disadvantage against RWEs by mass-autoblocking extremist content. Governments want to understand what can be done to counter this content when it is both illegal and legal, and so a strong emphasis has been placed on restrictive measure like automated content removal, takedowns, filtering, or removing sites altogether. However, a report from the Institute for Strategic Dialogue in 2013 has questioned the value of these measures, stating that, “While it is important for governments to enforce the law, and be seen to be doing so, there are severe limitations on the effectiveness of this response, given the
Currently Facebook is under scrutiny for creating a divided world.

speed with which new data is uploaded and the limited capacity of law enforcement agencies.” The internet is a massive, interconnected computer network with millions of websites, and while many websites exist as entities within Western states, and thus are subject to their laws, getting them to agree to this type of content policing and catch the bad content is near impossible. This is compounded by the difficulty in determining what content to police. For example, the use of triple parentheses ((()()()()()()()) is a right-wing style of indicating who they believe runs the global cabal, i.e. “the Jews.” A content flag to block this might work, but the difficulty arises in trying to find all these writing quirks and auto moderating them away; using human capital would be too labour intensive. In early May, Facebook updated its “Violence and Incitement policy” to ban “boogaloo” and similar terms when used alongside images or statements glorifying armed violence. In June, they began adjusting algorithms so that they would not recommend boogaloo pages or groups to users. However, the Boogaloo Bois had already developed an array of homophones to substitute for the word “boogaloo” including #BigLuau, #Blueigloo or #Boojahideen making Facebook’s efforts mute. Currently Facebook is under scrutiny for creating a divided world. An internal investigation at Facebook concluded that the company’s algorithms were designed to drive people apart; one presentation by the Facebook company in 2018 proclaimed “Our algorithms exploit the human brain's attraction to divisiveness.” It warned that if left unchecked, Facebook would feed users “more and more divisive content in an effort to gain user attention & increase time on the platform.” However, while many of its own experts appear to want to mitigate its problems, the company has currently chosen not to. This has a significant impact in view of Facebook’s 2.6 billion monthly users.

The rise of fast-content websites like Instagram and the rise of image-based memes makes this work all but impossible. Further, blocking content can exacerbate problems, especially in the United States, where arguments on free speech extends beyond reasonable discussion. While there is some use for this type of CVE operation, it cannot be the basis for any successful plan.

**Targeted Counter-Narratives for Combatting Right-Wing Extremism Online**

Counter-narratives could be a successful tool in the fight against right-wing extremism. It is important to recognize that counter-narratives are a catch-all term for a wide range of activities with different aims and tactics, from public diplomacy and strategic communications by government, to targeted campaigns to discredit the ideologies of violent extremists. These counter-narratives explicitly deconstruct, delegitimise or demystify extremist propaganda, with the goal of either de-radicalising those who have already been radicalised, or disrupting the process of extremists trying to subversively expose vulnerable targets to extremist content. For Salafi-jihadist extremism, the focus has been on the former, which is why only programs to-date have been designed to proactively counter violent extremist messages through the Internet and social media. However, for right-wing extremism, evidence suggests that countering should focus on the latter process, creating counter-narrative programs that disrupt the process.

This paper suggests a policy prescription towards using targeted types of counter-narrative programs. Especially those that seek to disrupt narrative formation, because the goal for neutralizing right-wing
Counter-narratives against RWEs should focus on trying to destroy the undercurrent of right-wing sentiment that has metastasized on the internet over the past two decades.

Extremism should be less about trying to de-radicalise current or leaning extremists and instead more about trying to disrupt them before they have a chance to share their views and begin to radicalise other people. A recent study evaluating a Swedish helpline for radicalisation showed how concerns for Salafi-jihadist radicalisation were spurred by the mere exercise of religious practice but concerns about right-wing radicalisation occurred only when individuals had already taken some radical non-violent or violent actions. Instead of using the same method used to stop the spread of Salafi-jihadist extremism, counter-narratives against RWEs should focus on trying to destroy the undercurrent of right-wing sentiment that has metastasized on the internet over the past two decades. This latter type of counter-narratives involves a much more targeted campaign, where ‘going viral’ is not realistic or even necessary for the success of the project. Because the number of active RWEs online is very small, neutralizing their efforts will have the best results overall at curtailing the total extremist content available online.

Worldwide, there are some targeted programs that actively engage in this counter-narrative work against RWEs online. They exist under a broad range of strategies, including government interventions; credible messengers; dissemination of counter-narrative products; products for de-radicalisation or disengagement; digital disruptions; and offline interventions. The United Kingdom, for example has decided on government interventions, which gives “the Joint Terrorism Analysis Centre, the domestic spy agency MI5, and the police more resources to collect intelligence on, and arrest, right-wing terrorists.” Their work involves penetrating far-right networks, finding right-wing extremists on social media forums, and developing unique plans to de-radicalise these users and stop them posting content. It is labour intensive but has shown promising results. The United States is working closely with some social media companies to disseminate counter-narrative products online, like tools for deradicalization. However, these are bandage fixes; results must seek to neutralize the threat, not the symptoms.

In 1996, MIT researchers warned of a potential dark side of global interconnectivity. They maintained that “Individuals empowered to screen out material that does not conform to their existing preferences may form virtual cliques, reinforce their biases, and insulate themselves from opposing points of view. Internet users can seek out interactions with like-minded individuals who have similar values, and thus become less likely to trust important decisions by people whose values differ from their own.” They referred to this phenomenon as ‘cyberbalkanization’ and ominously warned that the loss of shared experiences and values may be harmful to the structure of democratic societies.

Digital Disruptions for Combatting Right-Wing Extremism Online

It is also true that counter-narrative programs have been subject to criticism for their failure to work. A 2017 European Parliament study on counter-narratives concluded “the concept itself is rather underdeveloped and lacks a thorough grounding in empirical research.” Many of the current programs, which focus on deradicalization, rely on undefinable metrics and sparse empirical foundations that lack a fully articulated theory to underpin their impact against RWEs. In short, their focus is on neutralizing the top ends of the scale, on cutting the Hydra’s heads, rather than seeking to undermine the methods that right-wing extremists use online.

This paper makes the following policy recommendation for neutralizing RWEs online: If RWEs are using subversive exposure to radicalise, states...
and other actors must also do so, using digital disruption counter-narratives to neutralize these networks. Investing in and developing digital disruption activities that focus on using the same type of subversive exposure RWEs use to obscure and diminish their visibility and influence has the potential to be the breakthrough needed in destroying the right-wing undercurrents that have infected the internet. Reactionary policies like deradicalization of individuals or government interventions are much harder and more costly than digital disruption, themselves having mixed outcomes.

Digital disruptions, as a counter-narrative tactic, are activities “that can make it more difficult to find extremist content online and via social media or poke fun at that which does exist. These activities involve the use of tools or smart technological fixes and go with the grain of the essential characteristics of the Internet, such as user-generated content and the push towards big data.” These disruptions are attempts to use the same type of subversive exposure used by RWEs, like the memes of the sad frog or the cherry-picked statistics, and use those to obscure what the RWEs are doing. One notably successful example of this was in 2011: after the Norway attacks, the ‘hacktivist’ group Anonymous uploaded altered copies of Breivik’s manifesto in order to prevent the Norwegian terrorists’ political ideas from influencing future acts of violence and extremism. This had the effect of completely obscuring the manifesto from view (it would require an already dedicated extremist to find them, but they would likely be beyond the point where disruptions affect them). These digital disruptions are effective at obscuring right-wing propaganda, obtaining three results: stopping vulnerable targets from radicalisation; destroying the pathways that lead to right-wing extremism; and discouraging RWEs.

Digital disruption methods present a unique opportunity in the world of P/CVE as a significantly underdeveloped tool compared to other counter-narrative methods. Digital disruption methods present a unique opportunity in the world of P/CVE as a significantly underdeveloped tool compared to other counter-narrative methods. This method is still in the developmental stages but has the potential to scale production quickly due to the relative simplicity of its technical outputs. For example, Instagram has introduced a “false information” label that obscures posts that have been debunked by fact checkers. It uses an algorithm to mark and obscure these posts, reducing the overall need for human involvement and disrupting one of the main methods RWEs use to begin planting the seeds of radicalisation. This is one of the more technically advanced ways social media platforms can bear some of the burden of creating tools to combat RWEs and this work shows how easily the right-wing undercurrent of the internet can be disrupted if social media invests in combatting these right-wing networks.

A digital disruption approach has the advantage that states have more resources to address the problem, as “those battling extremism have size and scale on their side; violent and non-violent extremists are in the minority, so mobilising just a tiny proportion of those seeking to combat them would reverse the balance away from their favour.” The European Commission’s Radicalisation Awareness Network (RAN), for example, works with the private sector to identify and create crowdsourcing tools which might have the potential to disrupt RWE propaganda, and can work with the government to identify how government knowledge and resources can play a role in shaping these tools. RAN exists as both a policymaking tool that brings together practitioners working on the prevention of radicalisation, and as a disruption creator that funds the tools that can be used to make it more difficult to find extremist content online or to mock RWE content.

The end result of these digital disruptions is replacing the pathways and nodes that lead from innocuous-but-malicious posts that lead to RWE networks with nodes and pathways that lead to counter-narrative information instead. This end-state is currently being trialled by Moonshot...
CVE against Salafi-jihadist extremism, who use data-driven innovations to build digital capacity in CVE and to assist with counter-narratives through digital disruption. An example of their work is the partnership with Jigsaw [Google Ideas] in the Redirect Method, which uses targeted advertising for users that are using keywords associated with violent extremism and redirecting them to a curated YouTube library of anti-IS videos. If this type of redirecting could be used against right-wing extremism, then decades of subversive exposure built up by RWEs could be neutralized very quickly and their subversive exposure could be replaced with a subversive exposure that directs towards non-extremist communities.

At its core, disrupting these pathways is essential: the rise in influence online in right-wing extremism has not been met with appropriate response by governments, private entities, or social media firms. The use of subversive exposure by these right-wing extremists has helped them to normalize their views online and they have burrowed deep into the undercurrent of the internet. While there are many options towards tackling this subversion, counter-narratives, especially through digital disruptions, present a significant, if underdeveloped, way forward in breaking down their online structures and influence. Memes, statistics, and lies used by RWEs to generate views and interest, if redirected to non-extremist links, would become valueless, especially if these extremists are not made aware of this development. Replacing these pathways would also help deradicalize those people engaging with these extremist views. Most importantly, the base of right-wing extremism, those who are unknowingly engaging in and sharing right-wing propaganda, would be greatly reduced. Digital disruption, therefore, strikes the Hydra's heart, not its head.

Memes, statistics, and lies used by RWEs to generate views and interest, if redirected to non-extremist links, would become valueless.
### 35 Selected Agencies and Initiatives for Countering Violent Extremism

**Themes:** Network; Prevention; Rehabilitation; Research

<table>
<thead>
<tr>
<th>Organization</th>
<th>Theme</th>
<th>Focus</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alliance of Women Against Radicalisation and Extremism (AWARE)</td>
<td>Network (Women)</td>
<td>An online platform and network to exchange and foster successful initiatives focusing on the crucial role played by women in preventing radicalization.</td>
<td><a href="https://euaware.eu/">https://euaware.eu/</a></td>
</tr>
<tr>
<td>Against Violent Extremism (AVE)</td>
<td>Prevention (Advocacy)</td>
<td>Leverages the lessons, experiences and networks of individuals who have dealt first-hand with extremism to connect, exchange, disseminate and fight against continued extremism.</td>
<td><a href="http://www.againstviolentextremism.org/">http://www.againstviolentextremism.org/</a></td>
</tr>
<tr>
<td>Anti-Defamation League (ADL)</td>
<td>Prevention (Education)</td>
<td>A global leader in exposing extremism and delivering anti-bias education and is a leading organization in training law enforcement.</td>
<td><a href="https://www.adl.org/">https://www.adl.org/</a></td>
</tr>
<tr>
<td>Berghof Foundation</td>
<td>Prevention (Engagement)</td>
<td>Engages and partners with key local religious institutions to counter violent extremism by mitigating the appeal of radical ideas and promoting moderate narratives in the MENA region.</td>
<td><a href="https://www.berghof-foundation.org/">https://www.berghof-foundation.org/</a></td>
</tr>
<tr>
<td>Bold Creative</td>
<td>Prevention (Education)</td>
<td>Program that uses digital disruption to raise the ability of young people to critically engage with content they consume, create, and share online.</td>
<td><a href="https://www.boldcreative.co.uk/">https://www.boldcreative.co.uk/</a></td>
</tr>
<tr>
<td>Building Resilience Against Violent Extremism (BRAVE)</td>
<td>Prevention (Engagement)</td>
<td>A systematic strategy to counter the rising radicalization and extremism focusing on their violent and non-violent manifestations in Kenya.</td>
<td><a href="http://cscrcenter.org/brave-programme/">http://cscrcenter.org/brave-programme/</a></td>
</tr>
<tr>
<td>Christchurch Call to Action</td>
<td>Network (Government)</td>
<td>A commitment by governments and tech companies to eliminate terrorist and violent extremist content online.</td>
<td><a href="https://www.christchurchcall.com/">https://www.christchurchcall.com/</a></td>
</tr>
<tr>
<td>Counter Extremism Project (CEP)</td>
<td>Prevention (Advocacy)</td>
<td>Combats extremism by pressuring financial and material support networks; countering narratives of extremist online recruitment; and advocating for smart laws, policies, and regulations.</td>
<td><a href="https://www.counterextremism.com/">https://www.counterextremism.com/</a></td>
</tr>
<tr>
<td>EXIT-Deutschland (EXIT groups include USA, Fryshuset, etc.)</td>
<td>Rehabilitation (Education)</td>
<td>Provides support and rehabilitation for neo-Nazis wanting to leave that subculture, and support for parents and those whose work brings them into contact with people involved in Nazism.</td>
<td><a href="https://www.exit-deutschland.de/">https://www.exit-deutschland.de/</a></td>
</tr>
<tr>
<td>Extreme Dialogue</td>
<td>Prevention (Policy)</td>
<td>Provides a structured framework that suits different groups, objectives, and sensitivities for approaching issues around hate or extremism</td>
<td><a href="https://extremedialogue.org/">https://extremedialogue.org/</a></td>
</tr>
<tr>
<td>Fempower, from the Quilliam Foundation</td>
<td>Network (Women)</td>
<td>Outreach program on gender extremism addressing women’s grievances through community engagement, clear communication of policy, and better reporting structures.</td>
<td><a href="https://www.quilliaminternational.com/fempower/">https://www.quilliaminternational.com/fempower/</a></td>
</tr>
<tr>
<td>Free Radical Project</td>
<td>Rehabilitation (Engagement)</td>
<td>A global disengagement platform that aids individuals, and their families or communities, in exiting hateful and violence-based extremism through non-aggressive methods.</td>
<td><a href="https://www.freeradicals.org/">https://www.freeradicals.org/</a></td>
</tr>
<tr>
<td>Organization</td>
<td>Theme</td>
<td>Focus</td>
<td>Resource</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global Center on Cooperative Security (GCCS)</td>
<td>Prevention</td>
<td>Through its countering violent extremism platform, works with local, regional, and international partners to promote holistic, preventative responses to violent extremism.</td>
<td><a href="https://www.globalcenter.org/">https://www.globalcenter.org/</a></td>
</tr>
<tr>
<td>Global Community Engagement and Resilience Fund (GCERF)</td>
<td>Network</td>
<td>The global fund dedicated to preventing violent extremism, connect local communities to global resources and supporting initiatives.</td>
<td><a href="https://www.gcerf.org">https://www.gcerf.org</a></td>
</tr>
<tr>
<td>Global Counterterrorism Forum (GCTF)</td>
<td>Network</td>
<td>Forum for practices on preventing, combating, and prosecuting terrorist acts and countering incitement and recruitment to terrorism.</td>
<td><a href="https://www.thegctf.org">https://www.thegctf.org</a></td>
</tr>
<tr>
<td>Hedayah</td>
<td>Research</td>
<td>Works to enhance understanding and share good practices to effectively build the capacity of CVE actors to promote tolerance, stability, and security.</td>
<td><a href="https://www.hedayahcenter.org/">https://www.hedayahcenter.org/</a></td>
</tr>
<tr>
<td>Inclusive Security</td>
<td>Network</td>
<td>Influenced the creation and strengthening of 40+ country policies on women’s inclusion, including national action plans on violent extremism.</td>
<td><a href="https://www.inclusivesecurity.org/">https://www.inclusivesecurity.org/</a></td>
</tr>
<tr>
<td>Institute for Strategic Dialogue (ISD)</td>
<td>Research</td>
<td>‘Think and do’ tank dedicated to innovating real-world responses to the rising tide of polarisation, hate and extremism of all forms.</td>
<td><a href="https://www.isdglobal.org/">https://www.isdglobal.org/</a></td>
</tr>
<tr>
<td>Just Unity</td>
<td>Prevention</td>
<td>Offers customized courses, lectures, and workshops for students, teachers, local authorities, police, businesses, and organizations to prevent radicalization and extremism among youth.</td>
<td><a href="https://justunity.no/">https://justunity.no/</a></td>
</tr>
<tr>
<td>Kosovo Centre for Security Studies (KCSS)</td>
<td>Research</td>
<td>Conducts research on the causes and consequences of citizens’ involvement as foreign fighters and implements projects focused on raising awareness</td>
<td><a href="http://www.gkss.org/en">http://www.gkss.org/en</a></td>
</tr>
<tr>
<td>Life After Hate</td>
<td>Rehabilitation</td>
<td>Helping people leave the violent far-right to connect with humanity and lead compassionate lives.</td>
<td><a href="https://www.lifeafterhate.org/">https://www.lifeafterhate.org/</a></td>
</tr>
<tr>
<td>Moonshot CVE</td>
<td>Prevention</td>
<td>Connects with people at risk of violent extremism and offer them an alternative path through digital methods.</td>
<td><a href="http://moonshotcve.com/">http://moonshotcve.com/</a></td>
</tr>
<tr>
<td>Mothers Opposing Violent Extremism (MOVE), from Women Without Borders</td>
<td>Prevention</td>
<td>Provides mothers the encouragement, support, and necessary tools to protect their children from the threat of violent extremism.</td>
<td><a href="https://wwb.org/">https://wwb.org/</a></td>
</tr>
<tr>
<td>Prevention Project</td>
<td>Prevention</td>
<td>Operationalize and sustain a “whole of society” approach to preventing the spread of violent extremism.</td>
<td><a href="https://organizingagainstve.org/">https://organizingagainstve.org/</a></td>
</tr>
<tr>
<td>Organization</td>
<td>Theme</td>
<td>Focus</td>
<td>Resource</td>
</tr>
<tr>
<td>------------------------------------------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Radicalization Awareness Network (RAN)</td>
<td>Research</td>
<td>Connects frontline practitioners from across Europe with one another, and with academics and policymakers, to exchange knowledge, first-hand experiences and approaches to preventing and countering violent extremism in all its forms.</td>
<td><a href="https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en">https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en</a></td>
</tr>
<tr>
<td>RESOLVE Network (USIP)</td>
<td>Network</td>
<td>Global consortium of researchers, research organizations, policymakers and practitioners committed to empirically driven, locally defined research on the drivers of violent extremism and sources of resilience.</td>
<td><a href="https://resolvenet.org/">https://resolvenet.org/</a></td>
</tr>
<tr>
<td>Southeast Asia Regional Centre for Counter-Terrorism (SEARCCCT)</td>
<td>Network</td>
<td>Aims to enhance regional competence in countering terrorism through quality and comprehensive capacity-building programmes.</td>
<td><a href="https://www.searcct.gov.my/#">https://www.searcct.gov.my/#</a></td>
</tr>
<tr>
<td>START (University of Maryland)</td>
<td>Research</td>
<td>A university-based research and education centre comprised of an international network of scholars committed to the scientific study of the causes and human consequences of terrorism in the US and the world.</td>
<td><a href="https://start.umd.edu/">https://start.umd.edu/</a></td>
</tr>
<tr>
<td>Violent Extremist Risk Assessment 2 Revised (VERA-2R)</td>
<td>Prevention</td>
<td>A tool and program to support the judgement of risk assessment and risk management of terrorists and violent extremists.</td>
<td><a href="https://www.vera-2r.nl/">https://www.vera-2r.nl/</a></td>
</tr>
<tr>
<td>VOX-Pol</td>
<td>Research</td>
<td>European Union Framework Programme 7 (FP7)-funded academic research network focused on researching the prevalence, contours, functions, and impacts of Violent Online Political Extremism and responses to it.</td>
<td><a href="https://www.voxpol.eu/">https://www.voxpol.eu/</a></td>
</tr>
<tr>
<td>The Youth Civil Activism Network (Youth CAN)</td>
<td>Network</td>
<td>Connects a wide array of youth activists from around the world to represents young people’s needs and views to policymakers, a voice to challenge hate, counter extremism, and promote peace.</td>
<td><a href="https://www.youthcan.net/">https://www.youthcan.net/</a></td>
</tr>
</tbody>
</table>
Bibliography


Endnotes


18. Ibid.


25. The two groups being the National Socialist Movement and Vettrucks Division.


29. Ibid.


31. The quote is attributed to Marvin Heemeyer, who bulldozed 13 buildings in Colorado in 2004 over a zoning dispute. He killed himself but became a hero among antigovernment extremists who call him “Killedeer” in chat rooms.


33. The Three Percenters are an American far-right militia movement and paramilitary group. The group advocates gun ownership rights and resistance to the U.S. federal government’s involvement in local affairs. Oath Keepers is an anti-government American far-right organization associated with the militia movement.


35. Ibid, 3.


46. Ibid.


55. Ibid, 5, 23.


Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.