Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends

Authors: Maura Conway, Ryan Scrivens, Logan Macnair

This policy brief traces how Western right-wing extremists have exploited the power of the internet from early dial-up bulletin board systems to contemporary social media and messaging apps. It demonstrates how the extreme right has been quick to adopt a variety of emerging online tools, not only to connect with the like-minded, but to radicalise some audiences while intimidating others, and ultimately to recruit new members, some of whom have engaged in hate crimes and/or terrorism. Highlighted throughout is the fast pace of change of both the internet and its associated platforms and technologies, on the one hand, and the extreme right, on the other, as well as how these have interacted and evolved over time. Underlined too is the persistence, despite these changes, of right-wing extremists’ online presence, which poses challenges for effectively responding to this activity moving forward.

Keywords: right-wing extremism, online tools, history, contemporary trends, online forums, social media, messaging applications, Web 2.0, policy challenges
Introduction

Close attention by journalists and policymakers to the widespread use of the internet by violent Western (i.e. American, Australian, and European) right-wing extremists (RWEs) and terrorists is relatively recent. It was a reaction, at least in part, to an eruption of hateful content online in 2015 and 2016, which arose out of the US presidential campaign and subsequent election of President Trump, the Brexit referendum, a spate of Islamic State (IS)-inspired or directed terrorist attacks, and the arrival of large numbers of refugees to Europe from war torn Syria, Iraq, and Afghanistan. The extreme right sought to capitalise on the fear and anger generated by the terrorist attacks and the refugee crisis and the elation generated by the other events to increase its political power and recruit new followers, including via the internet. They were aided in their efforts by foreign influence campaigns spreading disinformation on many of the same talking points. In 2017, more focused attention was drawn to the role of the internet in extreme right activity in the wake of events at the mid-August ‘Unite the Right’ rally in Charlottesville, Virginia, USA. Concerns about the political fallout of online extreme right activity, including disinformation and radicalisation, continued to receive attention throughout 2018—at least partially due to a series of attacks and failed attacks in the US that appeared to have significant online components. The 15 March, 2019 Christchurch terrorist attack mainstreamed these concerns. The New Zealand mosque attack, in which 51 people died, was peculiarly internet-centric, including a pre-planned online manifesto distribution strategy and Facebook Live video stream, which has ensured that the threat posed by contemporary extreme right online activity is now under greater scrutiny than ever before. The April 2019 Poway synagogue attack, the August 2019 El Paso Walmart shooting, the October 2019 Halle shootings, and a series of similar attacks only heightened attention to RWEs’ use of the internet further.

However, the RWE-internet nexus has a much lengthier history than this. RWEs were some of the very first users to engage in online politics and were the earliest adopters of internet technology for violent extremist purposes. This Policy Brief traces how Western RWEs have exploited the power of the internet from early dial-up bulletin board systems to contemporary social media and messaging apps. It demonstrates how RWEs have been quick to adopt a variety of emerging online tools, not only to connect with the like-minded, but to radicalise some audiences while intimidating others—and ultimately, to recruit new members, some of which have gone on to have commit hate crimes and terrorism. Highlighted throughout is, on the one hand, the fast pace of change of both the internet and its associated platforms and technologies, and on the other, the nature and workings of the extreme right, as well as how these two elements have interacted and evolved over time. In our conclusion, we underline the persistence, despite these changes, of right-wing extremists’ online presence and the challenges for practitioners and policymakers of effectively responding to this activity moving forward.

---

1 It is worth noting here that there are large and growing RWE constituencies outside of the West, including in, for example, Brazil, India, and the Philippines, that also have substantial online presences and that insufficient attention has been paid to by researchers to-date.


3 These included the US mail bomb scare, the shooting dead of two African-Americans in a Kentucky supermarket, and the Pittsburgh synagogue attack, all of which took place within days of each other in October 2018.

Worth noting here is that, following J.M. Berger, we take the view that RWEs—like all extremists—structure their beliefs on the basis that the success and survival of the in-group is inseparable from the negative acts of an out-group and, in turn, they are willing to assume both an offensive and defensive stance in the name of the success and survival of the in-group. We thus conceptualise Western right-wing extremism as a racially, ethnically, and/or sexually defined nationalism, which is typically framed in terms of white power and/or white identity (i.e. the in-group) that is grounded in xenophobic and exclusionary understandings of the perceived threats posed by some combination of non-whites, Jews, Muslims, immigrants, refugees, members of the LGBTQI+ community, and feminists (i.e. the out-group(s)).

**Pre-Web Bulletin Board Systems**

Along with a history of violence, the extreme right has a very long online history dating to the earliest days of the public internet. To illustrate, American white supremacist Louis Beam, an early advocate of ‘leaderless resistance,’ established and ran a bulletin board system (BBS) known as Aryan Nation Liberty Net from at least 1984. Accessible via telephone numbers in the US states of Idaho, Texas, and North Carolina, the Liberty Net BBS allowed anyone with a computer and a modem to gain ‘dial-up’ access to a variety of hate propaganda as well as information about Aryan Nation meetings and details about other RWE groups, as well as—in perhaps the world’s first instance of doxxing—the names and addresses of those who were perceived as “enemies.” Users could also leave their own messages on the system. Beam’s service, however, was not the only such BBS operating at around this time. Another US-based service, Info International, was established and run by George Dietz, the owner of a conspicuously extreme right publishing company, Liberty Bell Publications. Tom Metzger, founder of the White Aryan Resistance (WAR), also utilised a BBS—known as WAR Computer Terminal—for propaganda purposes. In an early example of what has since been termed “convergence culture,” Metzger promoted this new medium via his WAR newspaper, with one of the first messages disseminated on the BBS directing viewers to his cable-access television show. In addition to aiding in recruitment and communication efficiency, BBSSs marked “a new departure for hate groups” and represented “an effort to give RWE a modern look”, wrote Lowe in 1985.

---

2 ‘LGBTQI+’ is a shorthand reference to describe the lesbian, gay, bi-sexual, transgender, queer, inter-sex, and other sexual identity-based communities.
5 ‘Doxxing’ is the internet-based practice of finding and posting online private or identifying information about an individual or organisation oftentimes accompanied by implicit or explicit requests to the use the information for online and/or ‘real world’ harassment purposes.
6 Lowe, Computerized Networks of Hate.
7 Berlet, When Hate Went Online.
9 Ibid.
10 Ibid., p. 1.
Web 1.0: Websites and Online Forums

It was not until the mid-1990s and the development and spread of the World Wide Web that a new era of internet-afforded hate truly began. As early as 1996, Stormfront’s Don Black asserted that “[o]rganizations have recruited through Stormfront, and through their Web pages that we’ve linked to.” The original Stormfront was more website than forum, containing a ‘Quote of the Week,’ ‘Texts Library’ of ‘White Nationalist’ documents, a letters page, an assortment of cartoons, and a downloadable graphics section. The ‘Hot Links’ page featured connections to like-minded sites such as those maintained by Aryan Nations, National Alliance, and Posse Comitatus. Some of these websites framed themselves as “news” (e.g. National Vanguard News, Life Site News) or “educational” sites (e.g. martinlutherking.org), and included links to an array of content and services, from “whites only” dating services to white power music and racist video games. Other prominent sites that first appeared in the 1990s—both of which are still in existence—include the American Renaissance and VDARE websites. American Renaissance originated as a white supremacist magazine that was first published in 1990 and evolved into a monthly online publication from around 1995. An array of articles, reports, interviews, conference proceedings, and videos in support of (de-bunked) genetics research have been featured on the site. Another notable site is vdare.com (established in 1999), an American anti-immigration website that—in addition to archiving the content of racists, anti-immigrant figures, and anti-Semites—is “best known for publishing work by white nationalists while maintaining that it is not a white nationalist site.” Organised hate groups also developed websites around this time. Some of these, such as those established by various Ku Klux Klan (KKK) branches, functioned as quasi ‘news’ sites for a more general audience, but others offered more group-specific information such as history, mission, upcoming events, and group-related merchandise (e.g. clothing and music). Some notable examples of these include websites hosted by the US-based Hammerskin Nation (established in 2002) and the UK-founded Blood & Honour (established in 2001).

From the mid-1990s, the extreme right became increasingly reliant on web-forums to facilitate movement expansion by spreading propaganda and connecting with like-minded individuals, both within and beyond national borders. It was around this time that Stormfront, for example, transformed from a website into a forum with an array of sub-sections addressing a variety of topics, including an ‘International’ section composed of a range of geographically and linguistically bounded sub-forums (e.g. ‘Stormfront Europe,’ ‘Stormfront Downunder,’ ‘Stormfront en Français,’ and ‘Stormfront Italia’). Stormfront has also served as a “funnel site” for the RWE movement, wherein forum users have been targeted by other RWE users for the purpose of recruiting new members into violent ‘real world’ groups including, online forums

1. ibid.
3. See Daniels, Cyber Racism.
hosted by Hammerskins, Blood & Honour, and various KKK branches. Today, Stormfront has just shy of 343,000 ‘members’ and contains over 13 million posts, but is now just one node in a much larger constellation of RWE online spaces. The latter include a variety of forums, none of which have either Stormfront’s longevity or volume. An example of the former is the now defunct Iron March, which gained notoriety for its members’ online advocacy of violence and acts of violence carried out by them. The Vanguard National News (VNN) forum (established in 2000), on the other hand, has a similar life span to Stormfront; but, like most other RWE web-forums from the mid-1990s until today, has a smaller base of user activity. Organised hate groups have also hosted their own web-forums (such as the now defunct Hammerskins forum “Crew 38”), but their platforms are much smaller and have even less activity.

While forums have acted as an essential medium for RWEs to air their grievances, bond, and form a collective identity by othering their “common enemies,” traditional websites also have a continuing role in the RWE online firmament. As already mentioned, sites such as American Renaissance and VDARE have persisted since the 1990s, while others have been established much more recently. A prominent example of the latter type is Alternativeright.com, founded by Richard Spencer in 2010, as well as other similar alt-right commentary pages, including altright.com, founded in 2015. Perhaps the currently most notorious active RWE website, however, is The Daily Stormer. The site and its founder Andrew Anglin gained widespread notoriety in the wake of Charlottesville when he wrote and published an article on the site mocking and abusing Heather Heyer, the woman murdered at the event, which was compounded by a series of follow-up articles, including one calling for harassment of mourners at Ms. Heyer’s funeral. With major web-hosting companies refusing to host the site, and Cloudflare refusing security services, it could not remain on the open internet and retreated for some time to the Dark Web. Anglin’s site returned to the surface web in 2018 however, with the new tagline ‘The Most Censored Publication in History’ and with Greek, Italian, and Spanish language sections added. The site continues to advocate against people of colour, Muslims, Jews, immigrants, refugees, and women. A variety of other such dedicated RWE ‘news’ sites are also heavily trafficked by RWEs, including Breitbart News and Alex Jones’ InfoWars site. RWEs also heavily outlink from social media and other platforms to a variety of websites maintained by traditional media outlets, including Fox News, the Daily Mail, and RT (formerly Russia Today).

Right-Wing Extremism 2.0: Social Media, User Generated Content, and the Visual Turn
A newer generation of extreme right adherents—though not unfamiliar with websites and online forums—are more used to communicating via social media, while also generating their own content on a variety of fringe platforms. The latter often takes a visual form.

---

Major Social Media Platforms

While Twitter has largely resolved its IS problem, it continues to come under pressure for the large amounts of RWE content produced and circulated on its platform. Twitter is not the only major social media company fielding such criticism of course; it is, however, the only company that, in the wake of any major change by it to its service, is faced with large numbers of the platform’s users responding with variations of “But what about the Nazis?” or just “Ban Nazis.”

While it is difficult to judge the volume of RWE content on any given platform, some attempts have been made to calculate the latter with respect to specific RWE groups and movements. In a 2016 report, J.M. Berger estimated that accounts associated with major American white nationalist movements on Twitter had added about 22,000 followers between 2012 and 2016, an increase of approximately 600 percent for a total of just over 25,000 followers. In a later report, Berger estimated that in the period April to June 2018, “the alt-right’s presence on Twitter was substantial, probably encompassing more than 100,000 users as a conservative estimate.” More recently, Jacob Davey and Julia Ebner presented data showing that the pan-European white nativist group known as Generation Identity had—as of May 2019—approximately 70,000 followers of its official Twitter accounts. These are just three variants of contemporary RWE online activity.

Twitter has not been unresponsive to calls for it to ‘clean up its act.’ On 31 May 2016, the European Commission, along with Twitter, Facebook, YouTube, and Microsoft, unveiled a ‘Code of Conduct on Countering Illegal Hate Speech Online’ that included a series of Europe-wide commitments to combat the spread of “illegal hate speech” via the internet. In November 2016, Twitter started rolling out new platform-wide anti-harassment tools, including the option to report an account for “hateful conduct.” It followed-up in 2017 by expanding its hateful conduct and media policies to include abusive usernames and hateful imagery. At the same time, Twitter also updated its rules around violence and physical harm to include the glorification of violence and violent extremist groups. The latter changes were widely reported to have resulted in a “purge” of extreme right accounts starting from 18 December, the date of their formal rollout. Twitter made further updates to these policies in September 2018, including expanding their hateful conduct policy to include content that “dehumanises others based on their membership in an identifiable group.”


The full text of the Code is available online at: https://ec.europa.eu/info/files/code-conduct-countering-illegal-hate-speech-online_en.


Given the size of Facebook’s user base, which is roughly seven times greater than Twitter’s, it is possible that Facebook is even more widely used for RWE purposes than Twitter. There has been comparatively less researcher attention directed at RWE on Facebook as compared to Twitter, due at least in part to the much more public nature of Twitter than Facebook. This is slowly changing albeit in a post-Cambridge Analytica context in which researcher access to Facebook data is getting more, not less, difficult. The vast majority of all research into RWE on Facebook is therefore focused on RWE groups’ and movements’ public Facebook pages, including the Facebook activity of Britain First, Patriotic Europeans Against the Islamisation of the Occident (Pegida), and Soldiers of Odin (SoO). This important knowledge—arising from the private nature of Facebook—is referred to by Mattias Ekman:

“SoO uses their open Facebook group ‘Soldiers of Odin Sweden Official’ to promote the network and to display various activities undertaken by activists. Unlike the closed groups deployed by activists for networking, coordination, movement building, and group cohesion, the open platform is far more sanitized.”

SoO, an anti-Islamic vigilante group founded in a small town in Finland in 2015, has used Facebook as a propaganda and recruitment tool to spread anti-Muslim hate globally. Ekman’s observation above, comparing the nature of SoO’s ‘open’ versus their ‘closed’ Facebook activity, draws on his own detailed findings regarding the group’s public page, but on investigative reporting for information about their private Facebook exchanges. It is highly likely that discrepancies of similar sorts are commonplace as regards the ‘open’ and ‘closed’ Facebook presences of a wide variety of RWEs.

Facebook Live’s usage by Brenton Tarrant to film his journey to and attack on worshipers at Christchurch’s Al Noor mosque put Facebook at the center of what has been described as the first “internet-native” terrorist attack. “The point of the attack,” as The Guardian’s Jason Burke pointed out, was “not just to kill Muslims, but to make a video of someone killing Muslims.” His video was, therefore, “not so much a medium for his message insomuch as it was the message, even more so than his actual manifesto” [italics in original]. Facebook’s response was ad hoc. None of the fewer than 200 people who watched the atrocity unfold live flagged the video for moderation.

6. Ibid., p. 6.
7. Ibid., p. 5.
video started, and 12 minutes after the live broadcast ended.”

Before the video was removed from Facebook, more than 1.2 million videos of the attack were removed by Facebook at upload, so they were prevented from gaining any views on the platform; “[a]proximately 300,000 additional copies were removed after they were posted.”

Google’s video-sharing platform, YouTube, was also in the eye of this storm. Neal Mohan, YouTube’s Chief Product Officer, told The Washington Post that a group of senior executives—known internally as “incident commanders”—tasked with responding to crises worked through the night in an effort to identify and remove what The Post described as “tens of thousands of videos.” YouTube has not supplied figures on exactly how many videos it actually removed, but they were being posted as frequently “as one per second in the hours after the shooting,” according to Mohan. Many of these were re-packaged or re-cut versions of the original video that “were altered in ways that outsmarted the company’s detection systems.” This included altering the size of the clips, adding watermarks or logos, and videoing the footage while playing it on another device and then posting this. The continuing availability of the attack footage on their platform caused YouTube to take at least two first-time steps: (1) they temporarily ceased human content moderation to speed-up removal of videos flagged by their automated systems, and (2) they temporarily disabled several search functions, including the ability to search for ‘recent uploads.’ While this worked, it also had downsides such as many unproblematic videos being swept-up in the automated non-moderated deletions.

Christchurch was not, of course, YouTube’s first encounter with RWE material on its platform. In particular, YouTube—which has been described by some as “a radicalization machine for the far right”—has been criticised for the high volumes of white power music found on its platform, as well as the propensity of its recommender system to suggest extreme right content to users. In an article that first appeared online in 2014, O’Callaghan et al. showed that users accessing English- and German-language RWE YouTube videos were very likely to be recommended further RWE content within the same category or related RWE content from a different category, but unlikely to be presented with non-RWE content. Research conducted by Reed et al. in 2019 had very similar findings. Such research undermines the almost exclusive focus to-date on individual users as the main protagonists in RWE cyberspaces and draws attention instead to the way in which “the immersion of some users in YouTube’s ER [extreme right]

"...

50 Ibid.
52 Ibid.
54 Mattias Ekman, “The Dark Side of Online Activism: Swedish Right-Wing Extremist Video Activism on YouTube.” Journal of Media and Communication Research 56, no 1 (2014): 79-99. Many white power bands have also uploaded their music on Soundcloud and were previously on MySpace and elsewhere.
spaces is a coproduction between the content generated by users and the affordances of YouTube’s recommender system.” It is worth mentioning here too that, like Facebook, YouTube has come under pressure regarding the workings of its livestreaming service, including being forced to shut down the comment section on its livestream of a 9 April, 2019 US congressional hearing on white nationalism after it was overwhelmed with hateful comments, including expressions of anti-Semitism and white supremacy.

Fringe Platforms

Beyond the major social media platforms, a diversity of more fringe platforms host increasing amounts of RWE content, due at least in part to its increased takedown by major platforms. The fringe platforms trafficked by RWEs are of broadly two sorts: first, dedicated RWE platforms and, second, general platforms with dedicated RWE boards or boards that have been colonised by RWEs.

Perhaps unsurprisingly, the increasing inhospitableness of major social media and other online platforms to extreme right content and activity resulted in far-right—largely US—activists establishing their own platforms that welcome, indeed encourage, just such content and activity. Pronounced in an August 2017 tweet by the company as seeking “to make speech free again and say F*CK YOU Silicon Valley elitist trash,” Gab is currently the most prominent platform fitting that category. Its founder, Andrew Torba, established it in 2016 in direct response to the ejecting by major social media platforms of high-profile RWE figures including, for example, Laura Loomer, Tommy Robinson, Richard Spencer, and Milo Yiannopoulos. By the tail-end of 2018, it had approximately 450,000 users that had posted approximately 30 million comments. Noteworthy is that in July 2019 Gab changed its hosting infrastructure to Mastodon, which is a free open-source self-hosting social network service. Mastodon promptly released a statement announcing themselves “completely opposed to Gab’s project and philosophy, which seeks to monetize and platform racist content while hiding behind the banner of free speech,” and describing some of the ways the Mastodon community are blocking access avenues to Gab. Despite this, Gab is now Mastadon’s biggest node, with the latter having no effective way of shutting Gab down.

Gab is a hybrid of Twitter and Reddit, with posts capped at 3,000 characters, and users having the ability—through up-voting—to boost their preferred posts in the overall feed. Gab came to public attention when it emerged that Robert Bowers, the man who killed 11 people at a Pittsburgh synagogue in October 2018, had been an active user from January of the same year. Bowers made 998 posts and replies on the site prior to carrying out his attack; his profile picture

---

57 O’Callaghan et al., “Down the (White) Rabbit Hole,” p. 651.
featured the neo-Nazi code ‘1488.’ Bowers’ final post appeared just minutes before his shooting spree commenced and read “I can’t sit by and watch my people get slaughtered. Screw your optics, I’m going in.” An analysis of his Gab posts showed that they were overwhelmingly anti-Semitic, with his most used words “kike” and “jew” [sic], often in association with terms like “vile” and “degenerate.”

Gab was unavailable for a number of days after the Pittsburgh shooting, but came back online thereafter. In terms of general Gab users, a Washington Post analysis of more than 30 million posts on the site identified hashtags such as #maga, #trump, #altright, and #fakenews as the most common. Gab is also rife with conspiracy theory-related discussion, with hashtags such as #qanon and #pizzagate prominent. Pervasive on the platform too is anti-Islam and anti-immigrant sentiment, represented by the prominence of hashtags such as #banislam, #buildthewall, and #bansharia. Bowers was not an outlier, in terms of his anti-Semitic postings, which are commonplace on Gab. It came under fire from its user base in September 2017 for banning infamous neo-Nazi troll Andrew ‘Weev’ Auernheimer after he made a post calling on Jews to be ‘taught a lesson’ and going on to reference Timothy McVeigh, responsible for the 1995 Oklahoma City bombing. Despite this, in the immediate aftermath of the Pittsburgh Synagogue attack, one user initiated a poll using the #treeoflifeshooting hashtag and asking, “What should the future of Jewish people in the West be?” Thirty-five percent of respondents voted for “genocide.” The same poster also posted a poll asking “Do you support the Pittsburgh synagogue shooter, Robert Bowers?” Almost 25 percent of respondents said they did, with one stating “Robert Bowers literally did nothing wrong.”

Unlike Gab, Reddit (established 2005) was not set-up for the purpose of forwarding right-wing extremism. Similar to Twitter, it currently has around 330 million pseudonymous monthly active users. As a result, Reddit is routinely in the top ten most visited sites in the US, UK, and other—particularly English-speaking—Western countries (e.g. Australia, Canada, Ireland, Netherlands, New Zealand), as well as being in the top 20 most-visited sites globally. Several far- and alt-right related subreddits—subsidary threads or forums focusing on a specific topic within the overall Reddit forum—have been established or greatly expanded in size in recent years, with many of them dedicated either explicitly or tacitly to a wide variety of hatreds and conspiracies. Once new users are introduced to and become immersed in these subreddits, they are often ‘rewarded’ in the form of ‘upvotes’, ‘likes’, and general positive reception for their contributions to the sub-forum, especially when sustaining and progressing a subreddit’s

62 The 14 refers to the white supremacist David Lane’s “14 Words” slogan and the 88 stands for ‘Heil Hitler’ as ‘H’ is the eighth letter of the alphabet.
63 Phillips et al., “The Daily Use of Gab is Climbing.”
64 Ibid.
65 The post can be viewed by visiting https://knowyourmeme.com/search?context=images&page=2&q=gab.
66 Phillips et al., “The Daily Use of Gab is Climbing.”
67 This is according to Statista’s ‘Most Popular Social Networks Worldwide as of July 2019.’
68 See https://www.alexa.com/topsites/countries/US.
agreed upon norms,\textsuperscript{71} oftentimes in ways similar to offline reinforcement (e.g. laughter, voicing agreement, etc.).\textsuperscript{72}

An example of one such RWE subreddit is \textit{r/The_Donald}, a popular pro-Trump space. In the immediate aftermath of the Christchurch attacks, many \textit{r/The_Donald} posts justified the shootings and/or displayed anti-Muslim hate.\textsuperscript{73} It has been quarantined since June 2019 for “threats of violence against police and public officials.”\textsuperscript{74} Quarantining means that links to \textit{r/The_Donald} no longer appear on Reddit’s ‘front page,’ it is not returned in Reddit search results, and users must be logged-in in order to contribute to it.\textsuperscript{75} While Reddit has a relatively laissez faire attitude to content moderation, the quarantining of \textit{r/The_Donald} was not the first such action taken by Reddit administrators. In 2015, Reddit closed several subreddits due to violations of Reddit’s anti-harassment policy, including \textit{r/CoonTown}. \textit{R/CoonTown} was a virulently racist subreddit and the first of its type to be removed by Reddit administrators, but was later joined by a variety of subreddits with RWE connections, including \textit{r/incels}, \textit{r/The_GreatAwakening}, and \textit{r/Pizzagate}. This caused some Redditors to migrate to its “censorship-free” alternative Voat, while others showed a preference for 4chan.

Like Reddit, 4chan’s (established in 2003) original purposes were non-RWE in their orientation; instead, the site largely focused on Japanese anime and manga.\textsuperscript{76} Today, it hosts 70 topic-specific image boards, including those devoted to ‘Photography,’ ‘Food & Cooking,’ ‘Science & Math,’ and a variety of ‘Adult’ themes. It claims to have “over 22 million monthly visitors,”\textsuperscript{77}—the majority of whom are assumed to be young men—known as ‘anons’ (dubbed as such due to the site being wholly anonymous).\textsuperscript{78} On 4chan, no logins are required, usernames are optional, and threads expire after a certain time.\textsuperscript{79} 4chan became more widely known in 2014 as a central node—along with Reddit—in the online harassment campaign against women in computer gaming known as ‘Gamergate,’ which had both RWE and misogynist elements.\textsuperscript{80} The RWE QAnon conspiracy was also initiated by 4chan posts. Its /pol/ (‘politically incorrect’) board, in particular, continues to serve the extreme right, largely outside of mainstream scrutiny. That is where the strategies and goals of a younger and ‘hipper’ version of RWE are developed and eventually packaged for more mainstream consumption and appeal, often in the form of memes.\textsuperscript{81}

\textsuperscript{72} Pete Simi, Kathleen Blee, Matthew DeMichele, and Steven Windisch. “Addicted to Hate: Identity Residual Among Former White Supremacists.” \textit{American Sociological Review} 82, no. 6 (2017): 1167-1187.
\textsuperscript{75} \textit{Ibid}.
\textsuperscript{77} See http://www.4chan.org/advertise.
\textsuperscript{78} Anonymity is the default position on 4chan, but users can generate a unique “tripcode” that makes their posts pseudonymous rather than anonymous. For more, see 4chan’s FAQ at http://www.4chan.org/faq#trip.
RWE ‘humour’ and their use of sarcasm to poke fun at adversaries is not new. Racist cartoons were a central component of the propaganda found on a number of then-popular RWE websites in the early 2000s. Similarly—in one of the many examples of such that can be found on RWE websites—Stormfront users created a number of ‘Joke of the Day’ threads, with one popular thread dating back to 2007 that includes countless jokes with racist, sexist, and xenophobic overtones. Together, the use of humour, sarcasm, and similar types of discourse have historically been used by RWEs to (openly) parade their hateful views, defending the material as “just a joke.” What is new, however, is RWEs’ heavy co-optation of meme culture. Memes can take a variety of forms, including catchphrases, easy-to-digest captioned images, and quirky animated GIFs. They are widely popular online, with many achieving viral status. RWE memes are equally various; for example, the use of the catchphrase “Subscribe to PewDiePie” by the Christchurch shooter.

Probably more commonplace, however, especially on online image boards such as 4chan, are images overlaid with ‘humorous’ text. James Alex Fields Jr. was sentenced to life imprisonment in March 2019 for killing Heather Heyer and injuring a number of others by driving his car into a crowd of counter protesters in Charlottesville. Court documents show that he shared two images on Instagram that showed a car hitting protesters months prior to the events in Charlottesville. Both memes, one of which he shared publicly and one in a private chat, show a car driving through a crowd of people described as protesters; the public post carried the caption, “You have the right to protest, but I’m late for work.” Many RWE memes, such as the latter, are generated on 4chan and then spread to more mainstream sites, such as Instagram. Other RWE memes had no original racist or anti-Semitic connotations, but were co-opted by RWEs for these purposes. Perhaps the most well-known example of this is Matt Furie’s Pepe the Frog character, which was widely disseminated across Reddit, 4chan, and 8chan in a variety of bigoted guises. Together, the memes, specialised jokes, and jargon dominating these spaces serve as a constant stream of highly distilled ideological thought, reinforcing these virtual communities’ beliefs, while also acting as a means of identity creation and formation for users both new and old.

8chan was established in 2013 and was basically a more extreme version of 4chan. Mathew Prince, CEO of 8chan’s previously main security provider Cloudflare, termed 8chan not just “a cesspool of hate,” but—in a nod to the concept of ‘privacy by design’—“lawless by design.” This conceptualisation points to the way in which 8chan’s user base was the outcome of a September 2014 decision by 4chan’s founder Christopher ‘Moot’ Poole to ban GamerGate discussions from 4chan, which enraged many users. 8chan’s founder, Fredrik Brennan, saw this

---

83 Daniels, Cyber Racism.
84 See https://www.stormfront.org/forum/t438791.
85 Billig, “Humour and Hatred.”
86 4chan has generated many of the Internet’s most persistent and pervasive memes, including “LOLcats” (i.e. pictures of cats with humorous overlay text) and “Rickrolling” (i.e. unexpected appearances of the music video for Rick Astley’s 1987 hit ‘Never Gonna’ Give You Up’).
as an opportunity to grow his user numbers and attracted the disenchanted 4channers and others to his site by defending GamerGaters and promising very light touch moderation, which meant, in effect, that 8chan was known as being a haven for RWE causes almost from its founding.\textsuperscript{91} By Autumn 2014, 8chan posts had increased from around 100 a day to around 5,000 an hour, according to Brennan.\textsuperscript{92} In 2019, 8chan was directly implicated in three high profile RWE terrorist attacks. On 15 March, 28-year-old Australian Brenton Tarrant opened fire and killed 50 people in two Christchurch, New Zealand mosques. Prior to the attack, Tarrant announced his intentions on 8chan, produced a ‘manifesto’ linked on the website, and live-streamed his attack on Facebook via a link also posted to 8chan’s /pol/ board. On 27 April, 19-year-old John Earnest opened fire, killing one woman, at a synagogue in Poway, California. On 3 August, 21-year-old Patrick Crusius opened fire and killed 22 people in a Walmart in El Paso, Texas. Both Earnest and Crusius also posted ‘manifestos’ to 8chan prior to their attacks. And, like Tarrant, both drew on the concept of ‘the great replacement’—Crusius explicitly and Earnest implicitly—in those documents.\textsuperscript{93}

Tarrant was roundly praised on 8chan following the Christchurch attack, in particular for his ‘high score’ (i.e. the high number of people murdered by him), with a number of memes circulated on the site depicting him as a saint, complete with halo.\textsuperscript{94} The Christchurch shooter was mentioned 10 times in Earnest’s ‘manifesto,’ in which he attributed his attack directly to Tarrant. The Poway shooter was, on the other hand, subject to widespread ridicule on 8chan due to his ‘low score,’ which was attributed to his ill-preparedness, including stemming from his having spent insufficient time on 8chan. Crusius’ ‘manifesto’ opens with a reference to “the Christchurch shooter and his manifesto.” The response to the El Paso attack on 8chan was more muted than the responses to the other two attacks however, with a lot of the discussion centring around the threat to 8chan from yet another attacker being associated with the site and many therefore portraying it as a ‘false flag’ event perpetrated precisely to bring this about. In the event, 8chan is—at time of writing—no longer accessible on the open web, as Cloudflare and a number of other providers have pulled their services.

Prior to 8chan’s banishment from the surface web, it was still not as easily accessible as more mainstream platforms due to its technical workings, on the one hand, and its user culture, on the other. Like 4chan, 8chan had a very pared down appearance; also, like 4chan, 8chan’s users were almost wholly anonymous except when employing a trip code, which allowed for verification that otherwise anonymous posts were contributed by a single user.\textsuperscript{95} In terms of its user culture, 8chan was well known for the very large amounts of so-called ‘hitposting’ on the site, which has been described as “the act of throwing out huge amounts of content, most of it ironic, low-quality trolling, for the purpose of provoking an emotional reaction in less internet-

\textsuperscript{91} A few months later, Brennan sought advice from 8chan users for a proposed Daily Stormer article, a posting that was accompanied by images of KKK-robed beer cans attending a lynching. In the event, he contributed a piece to the Daily Stormer titled ‘Hotwheels: Why I Support Eugenics.’ ‘Hotwheels’ is Brennan’s online moniker.


\textsuperscript{93} Davey and Ebner, ‘The Great Replacement’.

\textsuperscript{94} Other RWE ‘heroes’ portrayed as saints in images posted online include the 2011 Norwegian RWE terrorist Anders Breivik, the May 2014 Isla Vista, California shooter, Elliot Rodger, and the June 2015 Charleston church attacker, Dylann Roof.

\textsuperscript{95} Binder, Matt. “Inside the Fight to Keep 8chan Offline.” Mashable, August 5, 2019, https://mashable.com/article/8chan-down/?europe=true. According to Binder, ‘Q,’ the anonymous generator and transmitter of the bizarre QAnon conspiracy allegedly posted on 8chan using such a code: “Without 8chan, it will be difficult for followers to determine whether any message is from the original Q.”
savvy viewers. The ultimate goal is to derail productive discussion and distract readers.”  

Shitposting is not unique to 8chan, being a part of overall ‘chan culture,’ but could be said to have been particularly prevalent and dense on it. Shitposting can be distinguished from ‘effort posting,’ which Urban Dictionary describes as “when a poster on an internet forum writes about their opinion, project, story or otherwise and actually takes the time to properly research, cite sources, and utilize proper diction and grammar, generally as a means to convince, sway, or otherwise argue.”  

Familiarity with these terms renders the opening line of Brenton Tarrant’s directly pre-attack 8chan post that it was “time to stop shitposting and time to make a real life effort post” comprehensible. In general, meaningfully distinguishing between online shitposts and effort posts on the chans can be difficult as many posts and threads are an opaque jumble of the two. This allows users to continue to insist that their online activity is largely in jest and ironic, while at the same time giving those users familiar with the boards’ sub-cultural languages the opportunity to immerse themselves in RWE communities of support and emulation.

### Messaging Apps and ‘Dark Social’

It should be apparent at this point that the RWE Internet scene is not restricted to a single type of online space, but instead a patchwork of different types of platforms and spaces, of which well-known social media platforms are just one component; a selection of relatively new and highly accessible communication ‘applications’ are another component of this scene. Such ‘apps,’ as they are known, are simply software programs designed to run on mobile devices, such as phones or tablets. Many of these fit into the category of so-called ‘dark social,’ which refers not to the ‘dark’ nature of the content, but to the difficulties of tracking content shared via, for example, messaging apps and other forms of encrypted chat. These difficulties at least partially explain why less research has been conducted on RWE use of these spaces and apps than may be warranted; the relative newness and niche status of some such apps may be other explanations.

Discord, as an example, describes itself as providing “Free Voice and Text Chat for Gamers” and, as the descriptor suggests, was originally developed to allow gamers to engage in group chats while gaming together live online. However, like Reddit, and to a lesser extent 4chan, Discord was effectively hijacked by RWE users. This was largely due to three factors: (1) Discord allowing users to form private, invitation-only chat groups not discoverable by non-users of the app; (2) its allowance of high degrees of user anonymity, and; (3) the ability of the administrators of group chats—referred to as servers—to establish their own moderation rules, which often amount to none. As The New York Times’ Kevin Roose described it, in the period pre-Charlottesville:

> “Leaders like Richard Spencer, who is credited with coining the term “alt-right,” and Andrew Anglin, the editor of the neo-Nazi website The Daily Stormer, used Discord to discuss current events and debate movement strategy. These discussions were not always harmonious, and often featured infighting and disagreement over tactics and cooperation with older and less internet-savvy groups like the Ku Klux Klan and

---


Vanguard America. But Discord became a private sounding board for the movement, and over time, Discord groups devoted to far-right politics — including one where newcomers were required to show proof of Caucasian skin before being given posting privileges — swelled to thousands of members.\(^99\)

Post-Charlottesville, Discord received considerable attention for its role in the ‘Unite the Right’ rally’s organisation, including being used for making ride share and accommodation arrangements.\(^100\)

While Discord banned an unknown number of servers in the rally’s wake, having been resistant to doing so prior, RWE activity continues on Discord. For example, an American RWE organisation, Identity Evropa (established in 2016), have been significant Discord users. In 2019, Unicorn Riot, a non-profit left-wing media collective, leaked more than 770,000 messages from Discord that related to the group, which included rampant racism and anti-Semitism as well as plans to infiltrate local Republican parties to win public office.\(^101\) In a 2019 report, Davey and Ebner too draw attention to the widespread communication of accelerationist views in online Identitarian circles and share the example of a member of an Identitarian Discord group discussing the need to “build islands in our lands, maybe patriotic villages where we can conserve our culture” and underlining that a plan on “what to do when everything around us collapses” was needed.\(^102\) This shares similarities with Atomwaffen Division members’ discussions around accelerationist violence and civilisational collapse, which emerged from Discord chat logs obtained by and reported upon by US media outlet ProPublica. The more than six months of chat logs also shed light on the group’s propaganda, key members and wider network, and their plans to engage in acts of terrorism.\(^103\)

The messaging application Telegram came to many people’s attention due to providing a safe haven for IS supporters.\(^104\) More recently, it has seen an increase in RWE too, including RWE terrorist groups such as those related to Atomwaffen and Siege Culture.\(^105\) Davey and Ebner estimate that in May 2019, just shy of 29,000 users followed official Generation Identity Telegram accounts.\(^106\) In addition, Identitarians have been particularly active in agitating against the *Pacte De Marrakech* or Marrakesh Agreement, a 2018 UN Global Compact for Safe, Orderly and Regular Migration, with Austrian Generation Identity leader Martin Sellner creating a Telegram channel dedicated to undermining it.\(^107\) Earlier, in 2016, National Action used


\(^{100}\) Ibid.


\(^{102}\) Davey and Ebner, ‘The Great Replacement’, p. 14. Accelerationism, is described in Davey and Ebner as “a theory that argues that technological and social advance should be sped up to increase instability and result in revolutionary change” (p. 9).


\(^{107}\) Ibid., p. 9.
Telegram to communicate with other members of the group about a neo-Nazi stickering campaign they were involved in on a university campus. While explicitly instructional channels, such as those common to IS on Telegram, are not apparent, in some instances RWE users share links to Dark Web markets, where guns and other weapons can be purchased “to prepare themselves for the final battle against enemies of the white race.”

### Concluding Remarks

On the one hand, the shift by RWEs—over nearly 40 years—from establishing websites, to a reliance on forums, to a commitment to social media, to the present shift to messaging apps has at least as much to do with transformations in the structures and workings of the internet as it has to do with the workings of RWE and terrorism over the period. On the other hand, RWEs have responded with alacrity to the fast pace of online change, adapting to new spaces, and adopting new tools with relative ease, including oftentimes being ‘early adopters’ of these—just as they were with their first foray into the online world with BBSs. While the contemporary online scene is perhaps the most difficult the extreme right has navigated to-date, due especially to the prominent role of the internet in a spate of right-wing terrorist attacks, they nonetheless persist in their online presence, with many RWE websites and forums now in existence for decades and new platforms springing up (and disappearing) all the time. Efforts to effectively tackle RWEs online presence will therefore require practitioners and policy makers to get ahead of the curve in this regard and not only ‘keep up’ with the trends described in this brief.

---


Bibliography


Kanaley, Reid. “Hate Groups Tap Into the Internet.” *The Philadelphia Inquirer*, July 4, 1996.


About the Authors

Maura Conway
Dr. Maura Conway is Professor of International Security in the School of Law and Government at Dublin City University (DCU) in Dublin, Ireland and Coordinator of VOX-Pol, a EU-funded project on violent online political extremism (voxpol.eu). Prof. Conway's principal research interests are in the area of terrorism and the Internet, including cyberterrorism, the functioning and effectiveness of violent political extremist online content, and violent online radicalisation. She is the author of over 40 articles and chapters in her specialist area(s). Her research has appeared in, amongst others, Studies in Conflict & Terrorism, Media, War & Conflict, Parliamentary Affairs, and Social Science Computer Review. Prof. Conway has presented her findings before the United Nations in New York, the Commission of the European Union in Brussels, the UK House of Lords, and elsewhere. She is a member of the Academic Advisory Board of Europol's Counter-terrorism Centre and a member of the Editorial Board of Terrorism and Political Violence.

Ryan Scrivens
Dr. Ryan Scrivens is an Assistant Professor in the School of Criminal Justice at Michigan State University. He is also a Visiting Researcher at the VOX-Pol Network of Excellence and a Research Associate at the International CyberCrime Research Centre at Simon Fraser University. Ryan conducts problem-oriented, interdisciplinary research with a focus on the local, national, and international threat of terrorism, violent extremism, and hatred as it evolves on- and offline. His primary research interests include terrorists’ and extremists’ use of the Internet, right-wing terrorism and extremism, combating violent extremism, hate crime, research methods and methodology, and computational social science. His research can be found in Studies in Conflict and Terrorism, Terrorism and Political Violence, Behavioral Sciences of Terrorism and Political Aggression, Deviant Behavior, and Critical Criminology, amongst others. He has presented his research before the Swedish Defence Research Agency in Stockholm, the Centre of Excellence for National Security in Singapore, and the United Nations in New York City and Vienna. His work has also been featured in over 100 new stories (television, radio, and print) and covered by an array of national and international media sources.

Logan Macnair
Logan Macnair is a PhD candidate and Research Associate at Simon Fraser University's International CyberCrime Research Centre whose research is primarily focused around the online media, communication strategies, and propaganda campaigns of terrorist and extremist organizations. His research has examined the online media of extremist organizations from a diversity of ideologies including Islamist extremism, right-wing extremism, and gender-based extremism. During his time as a PhD student, Logan has also been involved in the creation and implementation of a local counter-extremist initiative and has worked as a contract researcher for a private security company.
Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends

Maura Conway, Logan Macnair, Ryan Scrivens
November 2019

About ICCT

ICCT The International Centre for Counter-Terrorism – The Hague (ICCT) is an independent think and do tank providing multidisciplinary policy advice and practical, solution-oriented implementation support on prevention and the rule of law, two vital pillars of effective counterterrorism.

ICCT’s work focuses on themes at the intersection of countering violent extremism and criminal justice sector responses, as well as human rights-related aspects of counterterrorism. The major project areas concern countering violent extremism, rule of law, foreign fighters, country and regional analysis, rehabilitation, civil society engagement and victims’ voices.

Functioning as a nucleus within the international counter-terrorism network, ICCT connects experts, policymakers, civil society actors and practitioners from different fields by providing a platform for productive collaboration, practical analysis, and exchange of experiences and expertise, with the ultimate aim of identifying innovative and comprehensive approaches to preventing and countering terrorism.

Contact ICCT

T: +31 (0)70 763 0050
E: info@icct.nl