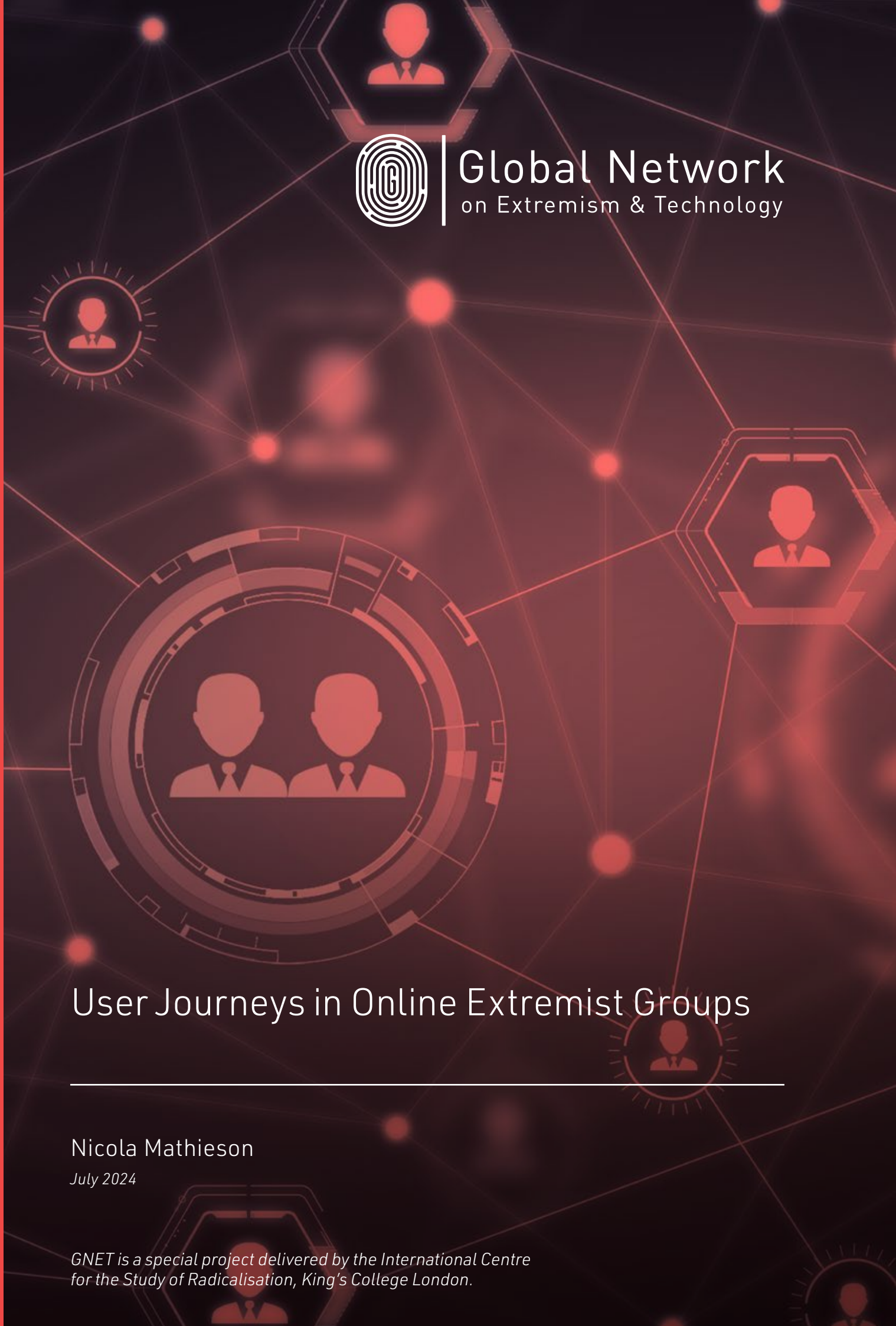

Global Network
on Extremism & Technology

User Journeys in Online Extremist Groups

Nicola Mathieson

July 2024

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

A project by the Global Network on Extremism and Technology (GNET), 2024

The author of this report is Nicola Mathieson, University of Liverpool, United Kingdom

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET, ICSR or King's College London.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Recommended citation:
Mathieson Nicola, "User Journeys in Online Extremist Groups: An Introduction". London: Global Network on Extremism and Technology (GNET), July 2024. https://doi.org/10.18742/pub01-185

User Journeys in Online Extremist Groups

This project by the Global Network on Extremism and Technology (GNET) looks at the user journeys of individuals who enter and participate in the online spaces of extremist communities. A user journey here refers to the distinct path a user may follow to reach their goals when accessing and using an online space belonging to extremist communities.

User journeys are particularly important in offering insights into the rationale and motivations of users on the one hand, and to the inner workings of extremist online communities on the other. This is vital for understanding their goals and objectives.

In selecting the ideologies for this project, we drew upon extremist communities – rather than extremist and terrorist organisations or groups – including those actors that participate in the extremist milieu and share ideas but do not necessarily operate in concert. These ideologies include those of formal and well-defined extremist organisations of White supremacist and anti-government extremist groups in the United States, supporter networks of Islamic State (IS), and looser communities of extremist actors including accelerationists, incels and chan site members who operate on shared platforms, congregating around common beliefs without the connection of formal membership.

This project is a response to the growing interest in understanding how individuals enter and participate in online spaces of extremist communities. A core goal of the project was to understand the role of algorithms in leading users to extremist communities, including the changes in algorithmic recommendations that lead users to more extreme content online. However, examining these changes proved impossible due to the precautions taken by the expert contributors to the project, such as the use of separate technology and VPNs throughout their research.

The project also highlights the distinct posting behaviour and operational security protocols of different groups, usually along ideological lines.

Contents

1 Introduction 4

2 Literature on Online Extremist Communities 7
Online Radicalisation and Recruitment 7
Online Extremist Material 9
Ethics of Researching Online Extremist Communities 10

3 Conclusion 12

1 Introduction

This introductory report represents the first in a series of short reports of user journeys of individuals in extremist communities. There is growing interest in understanding how individuals enter and participate in the online spaces of extremist communities. However, there are inherent challenges to accessing and observing user journeys within these online spaces. Accessing this information comes with risks, specialisation and immense time commitments. There are also important ethical considerations that shape how research into extremist communities is conducted. Instead, most research into the online behaviour of extremist communities draws on public-facing platforms. Focusing on public-facing online platforms can tell us a lot about the types of content the public can access. However, less is known about the content and experiences of users once they move into the private online platforms and channels of extremist communities.

The project which received ethics clearance from King's College London, takes a two-pronged approach to map the full user journeys of individuals in extremist communities.

Firstly, experts on online extremist community provide an overview of the public-facing platforms of extremist communities, which vary in terms of ideological grounding, organisational structure and platform use. This draws on extremist communities – rather than extremist and terrorist organisations or groups – and includes those actors who participate in the extremist milieu and share ideas but do not necessarily operate in concert. The selected communities include:

- Formal and well-defined extremist organisations of White supremacist and anti-government extremist groups in the United States
- Supporter networks of IS
- Looser communities of extremist actors including accelerationists, incels and chan site members who operate on shared platforms, congregating around common beliefs but without the connection of formal membership.

These overviews provide a snapshot of the current operating behaviours that the public can readily access. This content can act as the first sites of exposure to extremist content.

Secondly, drawing on focus groups with experts who have accessed the private communication platforms of extremist communities, this project provides an overview of the platforms, vetting and on-boarding processes, posting behaviour, and content of these private spaces. To maintain the anonymity of research participants, these groups are broadly categorised as far-right and Islamist extremist communities.

One of the core aims of this project was to understand the role of algorithms in leading users to extremist communities and changes to algorithmic recommendations that lead users to more extreme content. However, as all experts used precautions such as separate technology and VPNs throughout their research, it was not possible to examine changes to algorithmic algorithms. All experts were able to identify and access these communities without the interference or influence of algorithms.

The project highlights the distinct posting behaviour and operational security protocols of different groups, usually along ideological lines. The project also summarises the main vetting processes of online extremist communities in the form of invitations, evidence and action, online interviews and questionnaires, in-person meetings and DNA tests. Groups may adopt multiple vetting processes, and the intensity of these processes can accelerate an individual's move through the organisation. There is a notable difference between the vetting processes of far-right and those of Islamist extremist communities. Far-right spaces ask for personal and verifiable information about an individual's identity in conjunction with their motivations and ideology. Islamist extremist communities balance the need for operational security with the desire to spread their message as far as possible. Islamist extremist communities were more likely to verify member information if the channel was being used for planning.

The posting behaviour also differs between far-right and Islamist extremist communities. Islamist communities use the tactic of out-linking to evade content moderation and to provide shareable links to their content outside private channels. Far-right communities make less use of linking as they centralise their activities on Telegram. The functionality of Telegram allows users to post text, photos, memes, videos and recordings with little risk of the content being removed.

While the focus groups stated that attack and event planning occur on platforms, these conversations usually took place in smaller groups and channels that require increased vetting processes. Islamist extremist communities, on the other hand, were dedicated to disseminating the branded, official content of Islamist groups. It was also notable that many extremist communities were also moving to more offline or analogue means of generating community with members, including the use of mailing lists and in-person social events.

The final section of the focus group looked at the types of content shared on extremist communities' private communication platforms. Islamist extremist communities were dedicated to disseminating the branded, official content of Islamist groups. Supporter networks also provide translations of official content to extend its reach. In far-right communities, the lifting of Covid-19 restrictions globally has led to a pivot in content. The three most notable themes observed were migration, LGBTQI+ communities and the current events in Ukraine. Interestingly, the conflict in Ukraine has caused a rift within many extremist communities as some members support Ukraine and its pursuit to join the European Union, while others support Russia's invasion. Whereas far-right extremist communities can be categorised as highly vigilant of operational security concerns, Islamist extremist communities balance their operational security with the need to disseminate their material as widely as possible.

Although understanding the inner workings of extremist online communities is vital to understanding the user journeys of members, researching extremist online communities is dangerous work. All participants in the focus groups had received death threats, with women also experiencing gendered threats of sexual violence and targeting of family members. The work also requires immense time commitment to build networks and profiles to access these spaces. For those researching Islamist online communities, it was noted that the constant removal of channels and platforms, while important for removing terrorism and violent extremism content (TVEC) from platforms, made it increasingly difficult for researchers to stay connected to these communities. Researchers, higher education institutions, ethics boards and tech companies need to come together to develop strategies for making this work safer and more sustainable.

2 Literature on Online Extremist Communities

The role of the internet in radicalisation into and the operations of extremist communities has been a key focus of research. This section outlines the major works, their contributions and continued gaps in the research agenda.

This literature review is divided into three sections.

The first part begins with an overview of the online radicalisation literature that attempts to determine the role of the internet in the radicalisation pathways of individuals. While it is widely agreed that the internet must play a key role in the radicalisation process, literature has struggled to provide empirical evidence of this process and to distinguish this process from offline radicalisation pathways. What is most striking about this traditional radicalisation literature is the lack of engagement with the actual content that extremist groups are posting online.

The second part focuses on the more recent literature that tracks and analyses the actual content of public extremist forums, chats and websites, with a focus on the language, targeting and ideology of extremist groups. This content-focused literature has resolved one of the major shortcomings of radicalisation literature by exposing how viewers and potential recruits interact with this material. However, as will be highlighted throughout, there is a lack of research that examines the private component of these online interactions.

Thirdly, an outline of the ethical challenges of researching online violent extremism is provided. There are challenges around accessing these private forums without engaging with extremists themselves or using the research method of deception. Instead, access to the private communications of extremist communities has been the realm of journalists, activists and researchers in their capacity as private citizens. There are also significant concerns around researcher safety.

Online Radicalisation and Recruitment

As early as 2008, Sageman boldly announced that the internet had replaced offline radicalisation.[1] Since then, debate within radicalisation literature has centred on the exact role of the internet in the process. The focus on online radicalisation was again heightened with the rise of IS in Iraq and Syria, looking

1 Marc Sageman, "A Strategy for Fighting International Islamist Terrorists," *The Annals of the American Academy of Political and Social Science* 618, no. 1 (July 2008): 227, https://doi.org/10.1177/0002716208317051.

particularly at how the internet facilitated the flow of foreign fighters to the conflict.[2]

While there is widespread acknowledgement that the internet plays an important role in the radicalisation and recruitment by extremist groups, debate remains on the online/offline divide.[3] Some scholars argue that social media platforms will never substitute in-person interactions.[4] Others highlight that most radicalisation still features an offline component.[5] However, there is widespread consensus that this online/offline divide is shifting.[6] Here, this project draws on the recent work of Herath and Whitakker, who argue that the online and offline are now so integrated in everyday life that there is little theoretical benefit in distinguishing between the two processes.[7] This conceptualisation builds on the work of Valentini et al. who use the concept of "onlife" spaces as "hybrid environments that incorporate elements from individuals' online and offline experiences".[8] Rather than the online being conceptualised as separate from real life, online activities are now a part of real life. Research should focus on the actual mechanisms of radicalisation and individuals' engagement with extremist material, rather than trying to distinguish between online and offline elements.

How, then, does the internet facilitate radicalisation and recruitment into extremist groups? What distinguishes online extremism is the two-way interactivity. Where previously cassettes, magazines and videos could convey information to supporters, there were few ways to engage with the creators. Now, through chat rooms, forums and messenger

2 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (January 2, 2015): 1–22, https://doi.org/10.1080/1057610X.2014.974948; Joseph Carter, Shiraz Maher, and Peter R. Neumann, "#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks," ICSR, 2014, http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf; Akemi Takeoka Chatfield, Christopher G. Reddick, and Uuf Brajawidagda, "Tweeting Propaganda, Radicalization and Recruitment: Islamic State Supporters Multi-Sided Twitter Networks," in *Proceedings of the 16th Annual International Conference on Digital Government Research* (dg.o 2015: 16th Annual International Digital Government Research Conference, Phoenix Arizona: ACM, 2015), 239–49, https://doi.org/10.1145/2757401.2757408; Matteo Vergani and Ana-Maria Bliuc, "The Evolution of the ISIS' Language: A Quantitative Analysis of the Language of the First Year of Dabiq Magazine," Sicurezza, Terrorismo e Societa (2015): 2,7–20, https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2015/12/Vergani-Bliuc_SicTerSoc_book-2.pdf; Matthew Rowe and Hassan Saif, "Mining Pro-ISIS Radicalisation Signals from Social Media Users," *Proceedings of the International AAAI Conference on Web and Social Media* 10, no. 1 (August 4, 2021): 329–38, https://doi.org/10.1609/icwsm.v10i1.14716; Efraim Benmelech and Esteban F. Klor, "What Explains the Flow of Foreign Fighters to ISIS?," *Terrorism and Political Violence* 32, no. 7 (October 31, 2018): 1458–81, https://doi.org/10.1080/09546553.2018.1482214; Lorne L. Dawson and Amarnath Amarasingam, "Talking to Foreign Fighters: Insights into the Motivations for Hijrah to Syria and Iraq," *Studies in Conflict & Terrorism* 40, no. 3 (March 4, 2017): 191–210, https://doi.org/10.1080/1057610X.2016.1274216.

3 This debate is not exclusive to extremism. For example, Conroy et al. found that engagement with political groups online correlated with offline participation. Meredith Conroy, Jessica T. Feezell, and Mario Guerrero, "Facebook and Political Engagement: A Study of Online Political Group Membership and Offline Political Engagement," *Computers in Human Behavior* 28, no. 5 (September 2012): 1535–46, https://doi.org/10.1016/j.chb.2012.03.012.

4 Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford University Press, 1999), 626; Jason Burke, "Al-Shabab's Tweets Won't Boost Its Cause," *The Guardian*, December 16, 2011, sec. Opinion, https://www.theguardian.com/commentisfree/2011/dec/16/al-shabab-tweets-terrorism-twitter.

5 Nafees Hamid and Christina Ariza, "Offline Versus Online Radicalisation: Which Is the Bigger Threat?: Tracing Outcomes of 439 Jihadist Terrorists Between 2014-2021 in 8 Western Countries," Global Network on Extremism and Technology, 2022, https://gnet-research.org/wp-content/uploads/2022/02/GNET-Report-Offline-Versus-Online-Radicalisation.pdf; Tiana Gaudette, Ryan Scrivens, and Vivek Venkatesh, "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists," *Terrorism and Political Violence* 34, no. 7 (October 3, 2022): 1339–56, https://doi.org/10.1080/09546553.2020.1784147.

6 Mehmet F. Bastug, Aziz Douai, and Davut Akca, "Exploring the 'Demand Side' of Online Radicalization: Evidence from the Canadian Context," *Studies in Conflict & Terrorism* 43, no. 7 (July 2, 2020): 616–37, https://doi.org/10.1080/1057610X.2018.1494409; Paul Gill et al., "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology & Public Policy* 16, no. 1 (February 2017): 99–117, https://doi.org/10.1111/1745-9133.12249; Joe Whittaker, "The Online Behaviors of Islamic State Terrorists in the United States," *Criminology & Public Policy* 20, no. 1 (February 2021): 177–203, https://doi.org/10.1111/1745-9133.12537; Daniel Koehler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, no. 1 (2014): 116–34.

7 Chamin Herath and Joe Whittaker, "Online Radicalisation: Moving beyond a Simple Dichotomy," *Terrorism and Political Violence*, November 22, 2021, 1–22, https://doi.org/10.1080/09546553.2021.1998008; See also Daniele Valentini, Anna Maria Lorusso, and Achim Stephan, "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization," *Frontiers in Psychology* 11 (March 24, 2020): 524, https://doi.org/10.3389/fpsyg.2020.00524.

8 Valentini, Lorusso, and Stephan, "Onlife Extremism."

services, individuals can interact not only with content producers but with other supporters.[9] Scholars also highlight two core features of the internet that reshape the radicalisation process. Firstly, the internet provides increased opportunities to access extremist material online. Secondly, this material, rather than necessarily radicalising individuals, acts an echo chamber for existing ideas.[10] Therefore, the internet is not necessarily the causal mechanism in the radicalisation process, but platforms and facilitates it.

While scholars acknowledge that there is a lack of empirical data supporting radicalisation literature,[11] there is another striking absence: engagement with the online extremist content that is assumed to be responsible for radicalisation. As aptly summarised by Aly, radicalisation studies are "often based on the assumption that the violent extremist narrative works like a magic bullet to radicalize audiences".[12]

The following section outlines the more recent literature that examines the actual content that extremist groups post online, with a particular focus on forums.

Online Extremist Material

The study of online extremist material has increased since the rise of IS. Within this research, there is a dominance of big data projects that rely on data scrapping – usually using publicly accessible APIs. These works have focused on quantitative analysis, in particular through network analysis of extremist communities – that is to say, their transnational connections or the structure of online communities[13] – and content analysis of posts and comments.[14]

This research looks at the types of content posted by extremist communities and how content is disseminated among users. For example, Ophir et al. examine the thematic clusters surrounding the topic of abortion on Stormfront, a White nationalist website

9 Anne Aly et al., "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization," *Studies in Conflict & Terrorism* 40, no. 1 (January 2, 2017): 1–9, https://doi.org/10.1080/1057610X.2016.1157402; Yotam Ophir et al., "Weaponizing Reproductive Rights: A Mixed-Method Analysis of White Nationalists' Discussion of Abortions Online," *Information, Communication & Society*, 2022, 7; Barbara Perry and Ryan Scrivens, "White Pride Worldwide: Constructing Global Identities Online," *The Globalisation of Hate: Internationalising Hate Crime*, 2016, 65–78.

10 Ines Von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon "Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism," 2013. http: https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

11 Ryan Scrivens, Paul Gill, and Maura Conway, "The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, (London, UK: Palgrave, 2019), Cybercrime Series, by invitation, forthcoming, 2.

12 Anne Aly, "Brothers, Believers, Brave Mujahideen: Focusing Attention on the Audience of Violent Jihadist Preachers," *Studies in Conflict & Terrorism* 40, no. 1 (January 2, 2017): 62, https://doi.org/10.1080/1057610X.2016.1157407.

13 For example, see Manuela Caiani and Patricia Kröll, "The Transnationalization of the Extreme Right and the Use of the Internet," *International Journal of Comparative and Applied Criminal Justice* 39, no. 4 (October 2, 2015): 331–51, https://doi.org/10.1080/01924036.2014.973050; Caterina Froio, "Race, Religion, or Culture? Framing Islam between Racism and Neo-Racism in the Online Network of the French Far Right," *Perspectives on Politics* 16, no. 3 (2018): 696–709; Benjamin Lee, "A Day in the 'Swamp': Understanding Discourse in the Online Counter-Jihad Nebula," *Democracy and Security* 11, no. 3 (2015): 248–74; Aleksandra Urman and Stefan Katz, "What They Do in the Shadows: Examining the Far-Right Networks on Telegram," *Information, Communication & Society* 25, no. 7 (2022): 904–23; Ofra Klein and Jasper Muis, "Online Discontent: Comparing Western European Far-Right Groups on Facebook," *European Societies* 21, no. 4 (2019): 540–62; Derek O'Callaghan et al., "Uncovering the Wider Structure of Extreme Right Communities Spanning Popular Online Networks," in *Proceedings of the 5th Annual ACM Web Science Conference*, 2013, 276–85.

14 Ophir et al., "Weaponizing Reproductive Rights"; Meredith L. Pruden et al., "Birds of a Feather: A Comparative Analysis of White Supremacist and Violent Male Supremacist Discourses," in *Right-Wing Extremism in Canada and the United States*, ed. Barbara Perry, Jeff Gruenewald, and Ryan Scrivens, Palgrave Hate Studies (Cham: Springer International Publishing, 2022), 215–54, https://doi.org/10.1007/978-3-030-99804-2_9; Yannick Veilleux-Lepage, Alexandra Phelan, and Ayse D. Lokmanoglu, "Gendered Radicalisation and 'Everyday Practices': An Analysis of Extreme Right and Islamic State Women-Only Forums," *European Journal of International Security* 8, no. 2 (2023): 227–42; Phyllis B. Gerstenfeld, Diana R. Grant, and Chau-Pu Chiang, "Hate Online: A Content Analysis of Extremist Internet Sites," *Analyses of Social Issues and Public Policy* 3, no. 1 (2003): 29–44.

established in 1995. The authors demonstrate how the topic of abortion is used as a "gendered mechanism for reproducing whiteness and White social dominance".[15] Focusing on the social media activities of foreign fighters in Syria and Iraq, Klausen examines how the different narratives posted by individuals and the apparent curation of foreign fighter accounts by IS.[16]

There has also been a shift to systematically examining the use of images and videos within extremist communities.[17] For example, memes have become a tool to convey cultural information to online members, with imagery and text that is often coded in humour and irony to circumvent content moderation policies.[18] While research examining online extremist content is growing exponentially, the common characteristic among peer-reviewed publication is the reliance on data published in public forums or channels.

Ethics of Researching Online Extremist Communities

There are also significant ethical challenges to researching online extremist communities which exacerbate the difficulties in accessing data in private channels. Conway outlines some of these challenges across two core areas: researcher safety and obtaining informed consent.[19]

Firstly, concerns about researcher safety have increased in recent years, with major reports from both GNET[20] and VOX-Pol[21] published in 2023. Issues of researcher safety go beyond emotional wellbeing and encompass the physical safety risks of undertaking online violent extremist communities and institutional responsibilities to researchers.[22] The online practices of doxxing,[23] brigading[24] and swatting[25] can all lead to offline targeting and violence.[26] The risk to researcher safety can also be heightened for those researchers with identity markers that intersect with targeting strategies of an extremist community, including (but not limited to) race, ethnicity, religion, gender and sexuality.[27]

15 Ophir et al., "Weaponizing Reproductive Rights," 16.
16 Klausen, "Tweeting the Jihad."
17 Blyth Crawford, Florence Keen, and Guillermo Suarez-Tangil, "Memes, Radicalisation, and the Promotion of Violence on Chan Sites," in *Proceedings of the International AAAI Conference on Web and Social Media* 15 (2021): 982–91; Ayse D. Lokmanoglu et al., "A Picture Is Worth a Thousand (S)Words: Classification and Diffusion of Memes on a Partisan Media Platform," GNET, March 2023, https://doi.org/10.18742/pub01-117; Benjamin Lee, "'Neo-Nazis Have Stolen Our Memes': Making Sense of Extreme Memes," *Digital Extremisms: Readings in Violence, Radicalisation and Extremism in the Online Space*, 2020, 91–108; Jytte Klausen et al., "The YouTube Jihadists: A Social Network Analysis of Al- Muhajiroun's Propaganda Campaign," 6, no. 1 (2012): 18; Derek O'Callaghan et al., "Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems," *Social Science Computer Review* 33, no. 4 (August 2015): 459–78, https://doi.org/10.1177/0894439314555329.
18 Lee, "'Neo-Nazis Have Stolen Our Memes'"; Lokmanoglu et al., "A Picture Is Worth a Thousand (S)Words"; Ashton Kingdon, "The Meme Is the Method: Examining the Power of the Image Within Extremist Propaganda," *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, 2021, 301–22.
19 Maura Conway, "Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines," *Terrorism and Political Violence* 33, no. 2 (February 17, 2021): 367–80, https://doi.org/10.1080/09546553.2021.1880235.
20 Miron Lakomy and Maciej Bożek, "Understanding the Trauma-Related Effects of Terrorist Propaganda on Researchers," GNET, April 2023, https://doi.org/10.18742/pub01-119.
21 Elizabeth Pearson et al., "Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field," VOX-Pol, 2023, https://www.voxpol.eu/download/report/Online-Extremism-and-Terrorism-Researchers-Security-Safety-Resilience.pdf.
22 Ashley A. Mattheis and Ashton Kingdon, "Does the Institution Have a Plan for That? Researcher Safety and the Ethics of Institutional Responsibility," *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, 2021, 457–72.
23 Publishing the private information of researchers online for the purpose of harassment online and offline.
24 Also known as a "pile on", where users coordinate harassment of another user's profile.
25 Making hoax phone calls to law enforcements to an individual's address.
26 Conway, "Online Extremism and Terrorism Research Ethics"; Adrienne L. Massanari, "Rethinking Research Ethics, Power, and the Risk of Visibility in the Era of the 'Alt-Right' Gaze," *Social Media + Society* 4, no. 2 (April 2018): 205630511876830, https://doi.org/10.1177/2056305118768302; Pearson et al., "Online Extremism and Terrorism Researchers' Security, Safety, and Resilience."
27 Conway, "Online Extremism and Terrorism Research Ethics," 370; Pearson et al., "Online Extremism and Terrorism Researchers' Security, Safety, and Resilience."

Secondly, there are issues around informed consent. Informed consent is the cornerstone of research ethics including human participants. However, gaining informed consent in online environments poses a number of challenges, including contestation as to whether users posting online are participating in public or private spaces,[28] the practicalities of seeking informed consent in big data projects,[29] and whether gaining informed consent may actually put the researcher or participant at risk.[30] For researchers employing deception and concealment, gaining informed consent is not possible without revealing one's intent. In addition, most research that receives ethics approval through ethics departments or Institutional Review Boards (IRB) prevents researchers from doing more than "lurk" on platforms, ruling out any engagement with research subjects and limiting a researcher's ability to enter private spaces that require login or verification of identity.[31] There are also ethical considerations around the publishing of research, including the risk of identifying or amplifying members of extremist communities, legal considerations[32] and requirements of reporting,[33] and data protection and privacy requirements.[34]

Taken together, most researchers of online violent extremist communities design projects that minimise risks to personal safety and rely on the publicly accessible information posted by extremist communities. Therefore, there is limited scholarship on the private communications of extremist communities. This gap in literature limits our understanding of the inner workings of both extremist communities and the full lifecycle of user journeys.

This project seeks to fill the gap on user journeys in two ways.

Firstly, this project draws on the expertise of scholars who focus on the public-facing activities of specific communities. These snapshots provide an overview of the types of information and ideologies that the public can readily access online. As outlined by Baele et al., "public pages act as key dissemination hubs for content… This content then filters down to public groups, which have fewer members and allow for much more interaction between members, and finally to private groups, which have the fewest members, but which allow for active coordination".[35]

Secondly, this project draws on the experiences of individuals who have accessed the inner workings of extremist groups' private communication channels. Using focus groups, this project draws out general processes and behaviours within the private communication platforms of extremist communities.

---

28 Conway, "Online Extremism and Terrorism Research Ethics"; Danah Boyd and Kate Crawford, "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon," *Information, Communication & Society* 15, no. 5 (2012): 662–79.

29 For an overview of the ethics of big data collection see Elizabeth Buchanan, "Considering the Ethics of Big Data Research: A Case of Twitter and ISIS/ISIL," ed. Sergio Gómez, *PLOS ONE* 12, no. 12 (December 1, 2017): e0187155, https://doi.org/10.1371/journal.pone.0187155.

30 Conway, "Online Extremism and Terrorism Research Ethics."

31 Conway, "Online Extremism and Terrorism Research Ethics," 373.

32 Matthew L. Williams, Pete Burnap, and Luke Sloan, "Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, Online Context and Algorithmic Estimation," *Sociology* 51, no. 6 (2017): 1149–68.

33 Ted Reynolds, "Ethical and Legal Issues Surrounding Academic Research into Online Radicalisation: A UK Experience," *Critical Studies on Terrorism* 5, no. 3 (December 2012): 499–513, https://doi.org/10.1080/17539153.2012.723447.

34 Reynolds; Williams, Burnap, and Sloan, "Towards an Ethical Framework for Publishing Twitter Data in Social Research"; Mathilda Åkerlund, "The Importance of Influential Users in (Re)Producing Swedish Far-Right Discourse on Twitter," *European Journal of Communication* 35, no. 6 (2020): 618.

35 Stephane J. Baele, Lewys Brace, and Travis G. Coan, "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism* 46, no. 9 (December 2020): 9; See also Jacob Davey et al., "An Online Environmental Scan of Right-Wing Extremism in Canada," *Institute for Strategic Dialogue* 21 (2020), https://www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf; Klein and Muis, "Online Discontent."

3 Conclusion

The need to understand the nature of the continued threat posed by the activities of individuals perpetuating acts of extremism through online spaces by firstly understanding their distinct paths in reaching their goals continues to increase across a wide range of stakeholders. These include academics, policymakers and technology companies. Drawing on qualitative research techniques including content analysis, ethnographic monitoring and focus group interviews, this project recognises the urgency of this issue and foregrounds the need to provide empirical insights from expert contributors.

This project covers five overviews of extremist activities across five main communities and ideologies: far-right groups in America, IS supporter groups, accelerationists, incels and chan sites, and their operations, including vetting processes and common community beliefs. The project seeks to contribute towards the understanding required to address these issues.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.