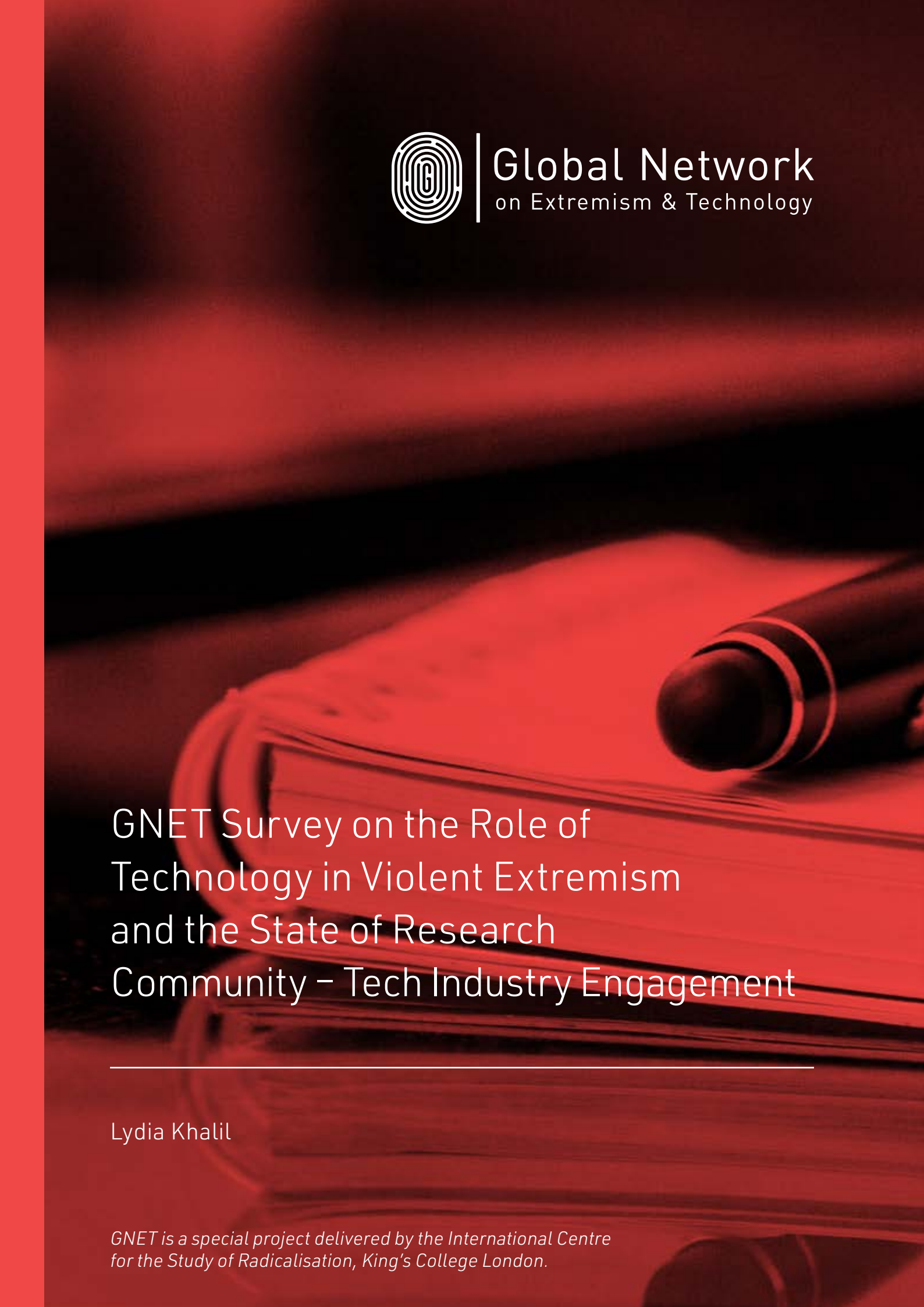


Global Network
on Extremism & Technology

GNET Survey on the Role of Technology in Violent Extremism and the State of Research Community – Tech Industry Engagement

Lydia Khalil

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

The author of this report is Lydia Khalil, Research Fellow, Lowy Institute.

Acknowledgements
The author would like to thank Dr Maura Conway for her advice in the development of the survey questions, J. M. Berger for his insights, Lowy colleagues Natasha Kassam and Alex Oliver for sharing their experiences and insights from their experience developing surveys, and Dr Matteo Vergani for his input on the survey questions. This report would not be possible without the engagement of the many researchers and experts who responded to the survey despite the incessant demands on their time and resources. Any flaws in the survey design or analysis are strictly the author's own.

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 or ICSR.

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.

© GNET

Executive Summary

What role does technology, particularly computer-mediated communications, play in violent extremism? This is the animating question driving the Global Network on Extremism and Technology (GNET) as a research-tech industry initiative. Since extremist actors have been some of the earliest adopters of the Internet and recognised its potential as a communications and mobilisation tool, researchers have been grappling with answering questions related to the role of technology and extremism for decades, but particularly since the advent of Islamic State and the growth in violent extremism motivated by right-wing ideologies, as well as the rapid emergence of violent conspiratorial extremist movements, such as QAnon, that was largely facilitated by the Internet.

To compliment past literature reviews on the role of Internet technology and extremism, to gain a current understanding of the research community's findings that may not be included in previously reviewed literature and to understand the academic research community's level of engagement with the tech industry, the Lowy Institute conducted a survey among researchers of terrorism and violent extremism on facets of this core question.

The findings of the survey reveal that there is a great deal of consensus within the research community that Internet enabled communications and social media platforms "support, encourage or mobilise real world harm." However, according to the responses to more detailed survey questions, parsing the role of technology on violent extremism is incredibly complex, multifaceted and still contested.

Survey responses to questions about researchers' engagement with the tech industry revealed that this is a potentially fruitful but also fraught space – much in the same way there remain dilemmas and considerations around collaboration with governments and security agencies among the terrorism research community and concerns around the securitisation of academic research. A number of responses indicated a cynicism about tech industry engagement with the academic community and a number of concerns including the opacity and lack of transparency of major platforms, their reactive nature, differing research priorities to industry and scepticism around how seriously and effectively social media platforms are tackling violent extremism and harmful disinformation.

Contents

1 Introduction

What role does technology, particularly computer-mediated communications, play in violent extremism? This is such a broad question that it practically begs for follow-ups, such as what role does the Internet, including social media, play in the radicalisation process? Has the use of social media increased the production and exposure to violent extremist content and narratives, and does this exposure radicalise individuals to violence? Does the use of computer-mediated communications and social media platforms make it easier to recruit or mobilise individuals to join violent extremist causes? Is there something about the technologies and platforms themselves – their design, logic, affordances and limitations – that contributes to and facilitates extremism? Does the precise role of technology depend on the type of extremist ideology or organisational structure of a particular movement, or indeed the gender or background of an individual? How does Internet technology and computer-mediated communications facilitate relationships or develop online social ecologies that contribute to extremism? Even if an individual comes to espouse extremist beliefs via online exposure to extremist narratives and content or participation in online subcultures, does that then necessarily lead to violence, militancy or other offline harms?

These questions are by no means exhaustive or new. Since extremist actors have been some of the earliest adopters of the Internet and recognised its potential as a communications and mobilisation tool, researchers have been grappling with these and similar questions around the role of technology and extremism for decades, but particularly since the advent of Islamic State, as its rapid rise, global reach and adept use of social media challenged terrorism researchers and counter-terrorism officials alike.

We are now in a similar moment with the growth in violent extremism motivated by right-wing ideologies and conspiracies. There has been a 205% increase in far right terrorism in the past five years,[1] as well as the rapid emergence of violent conspiratorial extremist movements, namely QAnon, facilitated by the Internet. While some claim that the fear of QAnon may be overblown,[2] the conspiracy movement has been labelled as a domestic extremist threat by the FBI[3] and has been the motivation for a number of recent violent attacks.[4] During the coronavirus pandemic, many people have lived under a cloud of anxiety and insecurity, while also spending copious amounts of time online. The rise in Internet usage has prompted

1 Global Terrorism Index (2020), Institute for Economics and Peace, https://www.visionofhumanity.org/global-terrorism-index-2020-the-ten-countries-most-impacted-by-terrorism/
2 CIVIQS (2021) "QAnon Support, Registered Voters" live survey, https://civiqs.com/results/qanon_support?uncertainty=true&annotations=true&zoomIn=true
3 Jana Winter (2019) "FBI document warns that conspiracy theories are a new domestic terrorism threat", Yahoo News, https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html
4 Amarnath Amarasingham and Marc-André Argentino (July 2020) "The QAnon Conspiracy Theory: A Security Threat in the Making?" *CTC Sentinel* vol. 13 no. 7: pp.37–41, https://ctc.usma.edu/the-qanon-conspiracy-theory-a-security-threat-in-the-making/

concerns, as yet unsubstantiated, that this has increased the risk of radicalisation online, or at least of the exposure to extremist content online.[5]

Dr Maura Conway facilitated this conversation around the role of technology in violent extremism in 2017 with her article, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research".[6] In it she describes how the terrorism research community grapples with the role of the Internet. But as Dr Conway noted at the time, there is "insufficient substantive empirically grounded social science research [that] has been undertaken to date in order to allow us to convincingly answer these questions".[7]

There are still few definitive answers, but since the article's publication, the extremism and terrorism research community has made progress in answering questions around the role of the Internet, causality and the affordances that particular technologies or platforms provide to violent extremist actors. There has been a great deal of new research into the role of the Internet and other technologies in extremism and terrorism in the past five years. There has been greater collaboration among data scientists and terrorism researchers from the social sciences. There is now more attention paid in the field of Internet studies to extremism and terrorism – in a similar fashion to when media and communications studies and social psychology also interacted with terrorism studies.

The very establishment of the Global Network on Extremism and Technology, and the greater willingness of the tech industry to acknowledge, however haltingly, that their platforms and technologies are not only exploited by extremist actors but that their affordances have contributed to the rapid spread of extremist ideologies, has progressed our understanding.[8] Mainstream platforms are now grappling with their role in the creation of extremist online milieus[9] and their contribution to the changing nature of extremism and its organisational structure.[10] Industry is also more engaged with work coming from the violent extremism research community.

The growing body of evidence does indeed demonstrate Internet technology can be an important factor in facilitating extremism. At the same time, there is an acknowledgement that we need to dig more deeply into what that exactly means for such a broad conclusion to make any kind of useful sense. There has emerged a more nuanced understanding that Internet technology, while not necessarily *causing* violent extremism, can have *multiple* and *various* roles in *facilitating* radicalisation and mobilisation to violent extremism.[11]

5 Caleb Spencer (2020) "Children may have been radicalised during lockdown", BBC News, https://www.bbc.com/news/uk-wales-53082476

6 Maura Conway (2017) "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research", *Studies in Conflict & Terrorism* vol. 40 no. 1: pp.77–98, DOI: 10.1080/1057610X.2016.1157408

7 Ibid.

8 Mason Youngblood (2020) "Extremist ideology as a complex contagion: the spread of far-right radicalization in the United States between 2005 and 2017", *Humanities and Social Science Communications* vol. 7 no. 1: pp.1–10, https://www.nature.com/articles/s41599-020-00546-3

9 Department of Security Studies and Criminology (2020) "Mapping Networks and Narratives of Online Right-Wing Extremists in New South Wales", http://doi.org/10.5281/zenodo.4071472

10 Bruce Hoffman and Colin Clarke (2020) "The Growing Irrelevance of Organizational Structure of Domestic Terrorism", The Cipher Brief, https://www.thecipherbrief.com/article/united-states/the-next-american-terrorist

11 Paul Gill, Emily Corner, Amy Thornton and Maura Conway (2015) "What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists", VOXPol Network of Excellence, https://www.voxpol.eu/download/vox-pol_publication/What-are-the-Roles-of-the-Internet-in-Terrorism.pdf

Additionally, we now understand that there is "no easy online and offline dichotomy" when it comes to actual violent behaviours motivated by extremist beliefs.[12] Furthermore, instead of conceptualising 'online radicalisation' writ large, there is a greater awareness that Internet technologies have different roles in the extremism process and that these technologies afford various uses and allow for various actions.[13]

There is also an awareness that the role of technology in radicalisation and mobilisation to violence has shifted over the decades alongside advances in technology itself. The shift from static websites and closed forums to public social networking sites back to alt-tech platforms and skulking in the 'dark web' or 'deep web'[14] by extremist actors has significantly changed the role of the Internet and other technologies related to extremism, depending on the affordances of each platform or technology. Current technology that did not exist in previous years, such as end-to-end encryption messaging services and drone technology, has impacted the tactics, communications and operations of extremist actors. Further advances in technology will prompt similar shifts. As David Benson notes in his article examining whether the Internet has led to an increase in transnational terrorism, "Since the Internet is ubiquitous, it would be strange if today's terrorists did not use the Internet, just as it would be strange if past terrorists did not use the postal service or telephones."[15] Just as advances in technology shift every aspect of our lives, so too will they impact extremism and terrorism.

Until recently, there was an understanding that Internet technology is a "facilitative tool": radicalisation to violence, recruitment, mobilisation and attack planning could be aided but were not necessarily dependent on the Internet; nor did the Internet cause radicalisation.[16] That may still be the case. However, during the pandemic, and particularly after the Capitol Siege in the United States, concerns about the causality of Internet technology gained new urgency. The Capitol Siege brought together a wide array of networks, groups and individuals, from organised militant groups to individual QAnon believers and pro-Trump activists, who all believed in the 'Big Lie', perpetuated and spread largely as online disinformation, that the US presidential election was fraudulent. The ground for the Capitol Siege was laid for months on online forums by a variety of established extremist groups[17] and the disinformation around the election process and election results was awash in the open Internet and mainstream social media platforms.[18] Social media also featured prominently as the Siege was conducted: a preliminary report by George Washington University's Program on

12 Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom and John Horgan (2017) "Terrorist Use of the Internet by the Numbers", *Criminology and Public Policy* vol. 16 no. 1: pp.99–117

13 Gill et al. "What are the roles of the internet in terrorism?"

14 According to the Merriam-Webster dictionary, the dark web is defined as "a set of web pages on the World Wide Web that cannot be indexed by search engines, are not viewable in a standard Web browser, require specific means (such as specialised software or network configuration to access, and use encryption to provide anonymity and privacy for users."

15 David C. Benson (2014) "Why the Internet Is Not Increasing Terrorism", *Security Studies* vol. 23 no. 2: pp.293–328, DOI: 10.1080/09636412.2014.905353

16 Alexander Meleagrou-Hitchens and Nick Kaderbhai (2017) "Research Perspectives on Online Radicalisation a literature review, 2006–2016", VoxPol Network of Excellence, https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf

17 Robert Evans (2021) "How the Insurgent and MAGA Right are Being Welded Together on the Streets of Washington D.C.", Bellingcat, https://www.bellingcat.com/news/americas/2021/01/05/how-the-insurgent-and-maga-right-are-being-welded-together-on-the-streets-of-washington-d-c/

18 Network Contagion Research Institute (2021) "NCRI Assessment of the Capitol Riots – Violent Actors and Ideologies Behind the Events of January 6, 2021", https://networkcontagion.us/wp-content/uploads/NCRI-Assessment-of-the-Capitol-Riots.pdf

Extremism found that 68% of participants who have been charged by law enforcement "documented their alleged crimes in real-time at the Capitol."[19]

The report also found that social media also "played a central role in the organization of the siege and the dissemination of material which helped to inspire involvement in it." Social media also played a role in allowing the disparate groups and individuals that participated in the Capitol Siege to interact and eventually coalesce in Washington, DC, on 6 January 2021.[20] Cases profiled in the report detail how social media facilitated the formation of spontaneous 'clusters' of previously unknown individuals finding each other and travelling together to participate in the siege with little planning[21] – in many ways echoing the process of ISIS-inspired foreign travellers but with less lead time, distance or barriers to travel.

As social media and algorithmic technologies become more and more embedded in our daily lives, could the Internet not only facilitate but actively enable violent extremism? In their 2015 study of the online behaviours of convicted UK terrorists, Paul Gill, Emily Corner, Amy Thornton and Maura Conway found that "The Internet has not led to a rise in terrorism. It is largely a facilitative tool; radicalisation is enabled by the Internet rather than being dependent upon it."[22]

But are we witnessing an emergence of "a new of terrorism that can't exist without the internet"?[23] Was the Capitol Siege an example of the Internet enabling and leading to mass digital radicalisation and mass mobilisation?[24] Did the Internet usage of some of individuals involved in the siege and their steady exposure to extremist narratives and disinformation online – particularly those not affiliated with already established organisations – accelerate their process of radicalisation to violence? In fact, was their radicalisation to violence in this instance actually determined by or dependent on the Internet? Has the 'logic' of various platforms contributed to the growth of extremism and does it now play a more significant part in an individual's trajectory to radicalisation to violence?

In attempting to outline the new social media logic and understand the ways in which social media platforms have "penetrated deeply into the mechanics of everyday life" and affected institutional structures and people's interactions, José van Dijck and Thomas Poell have compared social media logic to the mass media logic that emerged before it and theorised that social media has created a new ecosystem that "reshapes social orders or chains of events." Because social media has the ability to transport its logic outside its platforms via the "strategies, mechanisms and economies underpinning social media platforms' dynamics," broader society becomes subject to its logic and principles.[25]

19 George Washington University's Program on Extremism (2021) "This is Our House! A Preliminary Assessment of the Capitol Hill Siege Participants", https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This-Is-Our-House.pdf
20 Ibid.
21 Ibid.
22 Gill et al. "What are the roles of the internet in terrorism?"
23 Craig Timberg, Drew Harwell, Razzan Nakhlawi and Harrison Smith (2021), "Nothing can stop what's coming: far right forums that fomented Capitol riots voice glee in aftermath", *The Washington Post*, https://www.washingtonpost.com/technology/2021/01/07/trump-online-siege/
24 Robert Pape and Keven Ruby (2021), "The Capitol Rioters Aren't Like Other Extremists," *The Atlanic*, https://www.theatlantic.com/ideas/archive/2021/02/the-capitol-rioters-arent-like-other-extremists/617895/
25 José van Dijck and Thomas Poell (2013) "Understanding Social Media Logic", *Media and Communication* vol 1 no. 1: pp.2–14, https://ssrn.com/abstract=2309065

While van Dijck and Poell do not focus on extremism specifically, extremism researcher J. M. Berger has outlined a similar argument around how the logic and nature of computer-enabled communications, and social media in particular, have fundamentally changed the conditions around social interaction and reorganised our public sphere in such a way that has led to extremism. This rise of the Internet, especially social media, according to Berger, has contributed to greater uncertainty and frayed "consensus reality" by creating "a volatile and unwelcoming environment for the idea of objective truth." Social media platforms have increased uncertainty because they have allowed all manner of contradictory information, opinions and analysis to populate their platforms.[26] Berger posits that "Social media creates an environment in which multiple alternative views of reality can win support by attracting measurable levels of engagement sufficient to be understood by audience members as consensus. To reconcile the uncertainty created by these conflicting viewpoints, audience members are likely to rely on in-group validation of perceived reality, which is often accompanied by hostility toward out-group views".[27] It is human nature to meet this fracturing of consensus reality with a corresponding effort to seek out certainty via "exclusive, all-encompassing identities – many of which are toxic and fragile – and hold the seed of violent extremism".[28] Extremism also emerges because an out-group's consensus is experienced as an existential threat that must be countered. Berger also contends that there are critical differences between old and new media, particularly regarding the lack of gate keepers or content regulation, the low cost of production and "engagement metrics bundled inextricably with distribution."[29]

26 J. M. Berger (2020) "Our Consensus Reality Has Shattered", *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/10/year-living-uncertainly/616648/
27 Interview with J. M. Berger, via message (6 April 2021).
28 J. M. Berger, "Our Consensus Reality Has Shattered"
29 Interview with J. M. Berger, via message (6 April 2021).

2 Exploring the Role of Extremism and Technology

Conducting a literature review of the available research is one way to respond to the enduring debates around the roles of technology in relation to violent extremism and examining the newer issues and questions that have arisen. Indeed, there have been a number of high-quality literature reviews on the role of the Internet and technology on radicalisation and violent extremism over the years.

What the Literature Says

In 2013, a study by RAND Europe incorporated a literature review as one part of their study *Radicalisation in the digital era*, which explored how the Internet is used by individuals in the process of radicalisation. That study found in its literature review, in combination with primary research, that the Internet did "enhance opportunities to become radicalised, as a result of being available to many people, and enabling connection with like-minded individuals from across the world 24/7." It also found that the Internet can act as an echo chamber and provides greater opportunities than offline interactions to affirm extremist beliefs. But it further found that, at the time, the Internet didn't necessarily accelerate this radicalisation nor serve as a substitute for the need for in-person interaction during the radicalisation process.[30]

In 2017, Alexander Meleagrou-Hitchens and Nick Kaderbhai conducted a literature review into online radicalisation and similarly found that the "Consensus is that the Internet alone is not a cause of radicalisation, but a facilitator and catalyser of an individual's trajectory towards violent political acts." They cite literature that cautions against overemphasising the role of the Internet, such as Benson in 2014 who finds that existing studies also "lack independent and dependent variables that would include both the use of the Internet by terrorists and states, thus omitting negative cases which would help to 'determine the net effect of the Internet on transnational terrorism.'"[31]

Meleagrou-Hitchens and Kaderbhai also note that the literature on the role of technology and the online environment on radicalisation is contested because the concept of radicalisation in extremism studies itself remains contested. However, there is consensus that radicalisation to violence is a social process and that the Internet, particularly social media, provides social spaces that foster the creation of in-groups and out-groups, assist in identity formation, as well as provide platforms for influencers and leaders.

30 Ines von Behr, Anais Reding, Charlie Edwards NS Luke Gribbon (n.d.) "Radicalisation in the digital era", RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
31 Meleagrou-Hitchens and Kaderbhai, "Research Perspectives on Online Radicalisation"

They conclude that "the vast majority of authors argue that, while the Internet plays a facilitating role, in most cases the individual must still also be in contact with real-world networks. An investigation into an individual's trajectory is thus often an investigation into the unique interplay between online and offline interactions."[32] However, more recent research in 2020 by Tinia Gaudette, Ryan Scrivens and Vivek Venkatesh, which relied on in-depth interviews with Canadian former violent extremists, found that "regardless of how individuals are first exposed to violent extremist ideologies and groups, it is the Internet that eventually facilitates processes of violent radicalisation by enabling them to immerse themselves in extremist content and networks – a finding supported by empirical research on the role of the Internet in facilitating an array of violent extremist movements in general and the extreme right-wing movement in particular."[33] This study of Canadian former extremists echoed the findings of Koehler's earlier 2014 study of German ex-extremists and their use of the Internet, which found that, "Compared to other 'socialization institutions', such as offline group activities, music and concerts, rallies and political trainings, the Internet appears as the most important element driving individual radicalization processes, according to the used material."[34]

Another systematic review conducted in 2018 sought to answer what the links between online exposure to violent radicalized content and online or offline violent radical outcomes are by solely reviewing empirical studies. It found that "The Internet's role thus seems to be one of decision-shaping, which, in association with offline factors, can be associated to decision-making." But of the 5,182 studies generated from the systematic review's search, only eleven, a shockingly low figure, were eligible for inclusion[35] – which serves to highlight the lack of empirically based research at the time.

In 2019, another systematic review was conducted that yielded 88 studies for consideration on the role of the Internet in both right-wing and jihadist extremism from a literature search that spanned 2000 to 2019. But these studies focused on the characteristics and content of websites used and not on the Internet habits of the users themselves.[36] The authors concluded from the study that "existing studies have thus far not sufficiently examined the users of available sites, nor have they studied the causal mechanisms that unfold at the intersection between the Internet and its users." There are very few studies that deal with individual users, their usage histories and their motivations and experiences online.

Most recently, in 2020, there was a literature review conducted by Charlie Winter, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino and Johanna Furst on how the Internet is used by violent extremists on both organisational and individual levels and for what purposes.[37] In their review of the

32 Ibid.
33 Tiana Gaudette, Ryan Scrivens and Vivek Venkatesh (2020) "The Role of the Internet in Violent Extremism: Insights from Former Right-Wing Extremists", *Terrorism and Political Violence*, DOI: 10.1080/09546553.2020.1784147
34 Daniel Koehler (2014) "The Radical Online: Individual Radicalization Processes and the Role of the Internet", *Journal for Deradicalization*, vol. Winter 2014/2015 no. 1: https://journals.sfu.ca/jd/index.php/jd/article/view/8/8
35 Ghadya Hassan et al. (2018) "Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Emperical Evidence", *International Journal of Development Science* vol. 12 no. 1–2: pp.71–88
36 Ozen Odog, Anne Leiser and Klaus Boehnke (2019) "Reviewing the Role of the Internet in Radicalisation Processes", *Journal for Deradicalisation* no. 21, https://journals.sfu.ca/jd/index.php/jd/article/view/289
37 Charlie Winter et al. (2020) "Online Extremism: Research Trends in Internet Activism, Radicalization and Counter-strategies", *International Journal of Conflict Violence* vol. 14

literature they found that just as the Internet is of central importance to all individuals, it has "become a primary operational environment, in which political ideologies are realized, attacks planned, and social movements made."[38] It has become so because "much of the time online extremism is simply intuitive usage of the Internet." Extremists use the Internet much in the same way we all do. And while the prevalence of extremist propaganda online and its increased consumption of extremist propaganda online by itself does not lead to radicalisation, online spaces can serve as forums for social engagement and interactions that can contribute to radicalisation and mobilisation to violence.[39] Online spaces are social spaces and function similarly to real-world social spaces in that they can provide identity, validation, community and meaning. The review concludes that, despite being unable to find any causal relationship between Internet technologies and extremism or to draw out structural conclusions, "there is no question that extremist organizations would not be where they are today without their adept use of virtual terrains."

Limitations and Data

These systematic reviews and others like them have been important for understanding the state of the field and the research community's assessments of the role of Internet technologies in violent extremism. However, as many of the literature reviews noted, the literature reviewed was skewed towards the study of jihadist actors because of the prevalence of research in that area. As such, reviews tended to focus less on other ideologies, particularly right-wing ideologies that are now presenting a significant threat across jurisdictions globally and are the subject of an increasing number of emerging research papers.[40] The reviews were also considering research literature conducted and written prior to the pandemic, with its full impact on society and extremism yet to be examined.

Additionally, research conclusions are only as good as the data they rest upon and a literature review is less able to adequately illuminate issues around researcher access to data, which greatly impacts the type and quality of the literature that is being reviewed, and the level of engagement with the technology industry.

Early concerns about the state of terrorism research hinged on the lack of access to data and the lack of data-sharing by governments.[41] But there have been advances in empirically based research[42] and the use of primary data[43] in terrorism and extremism studies since early criticisms around the lack of data-driven research were made about the field.[44] When it comes to the role of technology and extremism, however, even though the Internet is awash with data, as we have seen through many of the literature reviews mentioned above, there

38 Ibid.
39 Department of Security Studies and Criminology, "Mapping Networks"
40 Meleagrou-Hitchens and Kaderbhai, "Research Perspectives on Online Radicalisation"
41 M. Sageman (2014) "The stagnation in terrorism research", *Terrorism and Political Violence* vol. 26 no. 4: pp.565–80, DOI: 10.1080/09546553.2014.895649
42 Sarah Knight and David A. Keatley (2020) "How can the literature inform counter terrorism practice? Recent advances and remaining challenges", *Behavioral Sciences of Terrorism and Political Aggression* vol. 12 no. 3: pp.217–30, DOI: 10.1080/19434472.2019.1666894
43 Bart Schuurman (2020) "Research on Terrorism, 2007–2016 Review of Data, Methods, and Authorship", *Terrorism and Political Violence* vol. 32 no. 5: pp.1,011–26, DOI: 10.1080/09546553.2018.1439023
44 Bart Schuurman and Quirine Eijkman (2013) "Moving Terrorism Research Forward: The Crucial Role of Primary Sources", ICCT Background Note, https://www.icct.nl/app/uploads/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf

remains a lack of data-driven studies on the role of technology and online radicalisation.[45] In "Terrorist Use of the Internet by the Numbers," published in 2017, the authors found that in examining 200 abstracts of research articles on "online radicalisation" only 6.5% used some form of data and a mere 2% of those studies used primary data.[46] The 2018 and 2019 systematic reviews described above had similar findings.

In 2020, Ryan Scrivens, Paul Gill and Maura Conway noted in an updated article around how to make progress researching the role of the Internet in violent extremism that there still remains an issue around access, collection and interpretation of primary data.[47] Their suggestions for progressing knowledge around this issue centre mostly on data. Their five suggestions include "collecting primary data across multiple types of populations" and "making archives of violent extremist online content accessible for use by researchers and on user-friendly platforms."[48]These issues around empirical evidence have inhibited researchers from being able to come to convincing conclusions.[49]

Ironically, just as terrorism research was beginning to incorporate primary data from extremist use of social media platforms, mainstream social media companies began to more consistently and comprehensively deplatform violent extremist actors and more strictly enforce their terms of service. A major reason why the debate about the role of the Internet remains unresolved is due to issues of data access, which remains in the hands the tech companies. Therefore, in order to attempt to contribute to the current understanding of the role of the Internet in extremism and terrorism, particularly around the research community's engagement with the social media platforms that carry most of the data that is relevant to the study of the role technology plays in the radicalisation to violence process, another approach is needed.

45 Gill et al., "Terrorist Use of the Internet by the Numbers"
46 Ibid.
47 Ryan Scrivens, Paul Gill and Maura Conway (2020) "The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research", in T. J. Holt, A. M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_61
48 Ibid.
49 Meleagrou-Hitchens and Kaderbhai, "Research Perspectives on Online Radicalisation"

3 Survey

To compliment past literature reviews on Internet technology and extremism, to gain a current understanding of the research community's findings that may not be included in previously reviewed literature and to understand the academic research community's level of engagement with the tech industry, the Lowy Institute conducted a survey among researchers of terrorism and violent extremism.

A database of researchers was built from a number of sources. The database consisted of researchers and experts who were on the editorial boards of the prominent journals in the field of terrorism and extremism studies: *Studies in Conflict and Terrorism*, *Terrorism and Political Violence*, *Critical Studies on Terrorism*, *Journal for Policing Intelligence and Counterterrorism*, *CTC Sentinel*, *Perspectives on Terrorism*, *Journal of Democracy and Security*, *Journal for DeRadicalization*, *Behavioral Sciences of Terrorism and Political Aggression* and *Dynamics of Asymmetric Conflict*. The database also drew on GNET Associate Fellows and GNET Insight contributors whose work focused on the Internet and extremism. Other experts who were part of recognised research institutes and networks, such as the George Washington University Program on Extremism, Resolve Network, Centre for the Analysis of Radical Right, Vox Pol, Institute for Strategic Dialogue, National Consortium for the Study of Terrorism and Responses to Terrorism, Hadayah, AVERT Research Network, TSAS and others were identified and added to the database. In addition to established career researchers, early career researchers and those focusing on issues around terrorism and technology were identified via research conference programmes such as the TASM Conference on Terrorism and Social Media at Swansea University.

The web-based questionnaire was sent to those individuals in the database. Invitees were also encouraged to share the survey link with others with relevant expertise. Respondents could choose to remain anonymous and they were not required to provide their name or affiliation. Some 158 researchers of terrorism and violent extremism responded to the survey. This report summarises some of the findings of the survey, presenting the results of a number of questions. The entire survey comprised 44 questions; this report summarises most though not all of the responses to the questionnaire.

There are limitations to the expert survey approach. The results reported here are based on a non-random sample and represent only the views of those who responded to the questionnaire. Aside from the criteria described above for building the database of potential respondents, we did not devise a further method to determine individuals' level of engagement with the issues around technology and extremism. Given the fact that many respondents

chose to remain anonymous, we could not identify and verify the level of research expertise and experience involved in answering the survey questions. Additionally, researchers and experts who may have relevant research experience around these issues may not have responded to the survey.

Of the 84 individuals who chose to respond to the prompt "current affiliation", 72% listed university or academia as their primary sector, 12% identifying think tanks or policy institutes as their primary sector and the remaining were scattered among in-house research within technology companies, consulting and non-governmental and civil society organisations. The primary field of discipline for the majority of respondents (n=158) was political science (42%), with sociology, criminology, psychology, communications and history making up majority of the primary fields of the other respondents.

The majority of respondents (n=158) also listed North America (44%) and Europe (48%) as their primary geographic research focus. Respondents also listed the Middle East (23%), Asia (15%) and Oceania (20%) as a geographic research focus (respondents were allowed to identity more than one geographic focus). The focus on North America and Europe is likely due to the fact that a majority of the researchers in the database and thus respondents to the survey are based in or hail from North America and Europe. But this is also likely because the current threat focus of the academic community is now on right-wing extremism from North America, Europe and Oceania, and, to a lesser extent, from Asia.

However, when respondents (n=158) were asked "on which extremist ideology have you conducted research?" and prompted to select all that applied, the same percentage of respondents (79% and 80% respectively) selected "jihadist" and "far right." Lower percentages of respondents selected "racial or ethnically motivated violent extremism" (41%), "far left" (29%), "incel" (22%) and "other" (17%).

Role of the Internet and social media on extremism

The first part of the survey focused on expert views of the role the Internet – particularly social media – has played in extremism. These questions were deliberately worded so as not to solicit opinion or impressions but to have respondents base their answers on "empirically based research" they have either conducted themselves or have read or used in their work.

The first question sought to solicit a view regarding whether online extremist activity satiates desire for real-world action or stokes, encourages or mobilises individuals to take offline action. When asked if Internet-enabled communications and online activity by extremist actors either "support, encourage or mobilise real world harm," "satisfy a desire for action or participation in extremism via virtual activity alone," or "both," the majority of respondents (60%) said either "support, encourage or mobilise real world harm," or both (36%) , with very few respondents saying that strictly online activity satisfied a desire for action or participation in extremism via virtual means alone (less than 1%). Respondents commented that Internet activity facilitates attack planning and execution (e.g. logistics, financing, human resources); motivation or influence to conduct violence; and celebration or amplification of previous attacks that can inspire similar actions by others. A number of respondents also pointed out that the "jihadist videos [for example] on the possession of those arrested and prosecuted for terrorism is one indicator of the [Internet's] support function," as are studies of captured jihadists who indicate that the communications were impactful on them. The view of the majority of survey respondents, that online activity can support, encourage or mobilise real-world harm, is consistent with recent findings of a representative sample in the US that examined "e-participation" more broadly and found that "forms of online expression and interaction [are] associated with greater offline citizen participation."[50]

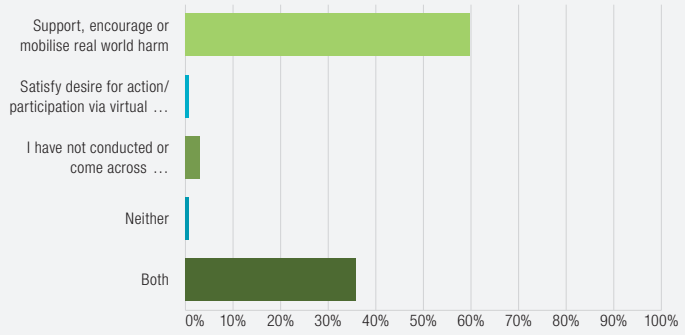
It is interesting to note that the majority of those canvassed concluded that online activity leads to real-world harms, particularly as some research – and some respondents – suggested that some individuals restrict themselves only to online activity and pose no offline risk because their online activity has satisfied their desire to articulate and advocate for their positions and air their grievances.[51] Additionally, previous studies on jihadists found virtual activity can carry similar legitimacy and impact as offline activity, thus potentially mitigating the need for jihadist real-world action. Studies by Akil Awan and others have found that 'virtual jihad' or 'media jihad' serve as legitimate and credible alternative options to real-world militancy.[52] Islamic State's virtual caliphate, for example, was considered as important[53] as the territorial caliphate in Syria and Iraq; the two were in fact intimately intertwined.[54]

50 K. Tai, G. Porumbescu and J. Shon (2020) "Can e-participation stimulate offline citizen participation: and empirical test with practical implications", DOI: 10.1080/14719037.2019.1584233
51 J. Suler (2004) "The online disinhibition effect", *Cyberpsychology and Behavior*, DOI: 10.1089/1094931041291295
52 A. Hoskins, A. Awan and B. O'Loughlin (2011) *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (1st ed.), Routledge, https://doi.org/10.4324/9780203829677
53 Charlie Winter (2015) "The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy", Quilliam, https://www.stratcomcoe.org/charlie-winter-virtual-caliphate-understanding-islamic-states-propaganda-strategy
54 Haroro Ingram and Craig Whiteside (2017) "In Search of the Virtual Caliphate", *War on the Rocks*, https://warontherocks.com/2017/09/in-search-of-the-virtual-caliphate-convenient-fallacy-dangerous-distraction/

Additionally, as technology use becomes more integrated into the functions of daily life the online vs offline dichotomy is diminishing. As one respondent noted, "'real world harm [can] include action in the digital world. Online action does affect the real world. Swatting, trolling, stalking, doxxing, abusing targets online has significant impacts in the real world." Internet-enabled communications and activity have fused digital and physical settings.[55] This fusion points to a need for a more holistic conceptualisation of online vs offline. Other respondents also added caveats to their responses by stating that, while they would support the conclusion that online activity leads to real-world harm, it is not a "linear or unidirectional process. Online and offline dynamics support and co-create one another."

Q7 Based on any empirically based research you have conducted or come across on extremism and technology do you observe that internet enabled communication and online activities

Answered: 134 Skipped: 24



ANSWER CHOICES	RESPONSES	
Support, encourage or mobilise real world harm	59.70%	80
Satisfy desire for action/ participation via virtual activity alone	0.75%	1
I have not conducted or come across research on this topic	2.99%	4
Neither	0.75%	1
Both	35.82%	48
TOTAL		134

This broader question was broken down in subsequent questions relating to extremist use of the Internet to fundraise, recruit, mobilise and plan violent action.

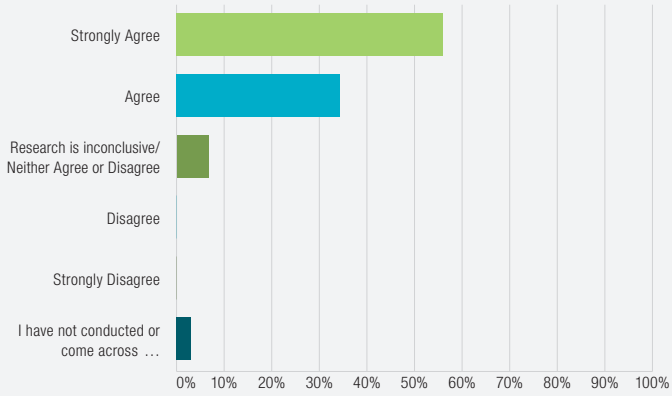
Regarding recruitment and whether Internet-enabled communications have made it easier to recruit individuals to extremist movements, there was broad agreement that this is the case. Some 90% of respondents agreed or strongly agreed. However, even though there

55 D. Valentini, A. M. Lorusso and A. Stephan (2020) "Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization", *Frontiers in Psychology* no. 11: p.524, https://doi.org/10.3389/fpsyg.2020.00524; B. Ducol (2015) "A Radical sociability: in defense of an online/offline multidimensional approach to radicalization", in M. Bouchard (ed.) *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected* (New York, NY: Routledge): pp.82–104

appears to be a broad consensus around this issue, the definition and conceptualisation of 'recruitment' in the online space is not well established. It could mean specific recruitment processes via computer-mediated mechanisms or broader social influence or the creation of communities via strategic communication efforts by extremist groups online. There is also little to no comparative research on the pre- and post-Internet environments when it comes to recruitment but there is broad agreement that the Internet, more than other technologies of the past, has increased the reach of extremist messaging and given extremist groups broader, quicker and more efficient access to potential recruits. As one respondent noted, "A range of research has demonstrated how social media allows for otherwise unconnected individuals to reach and be reached by extremist groups, and removes the reliance on formal organisational structures as a means to recruit."

Q9 The use of the internet enabled communications and/or social media platforms by extremist actors has made it easier to recruit individuals to extremist movements?

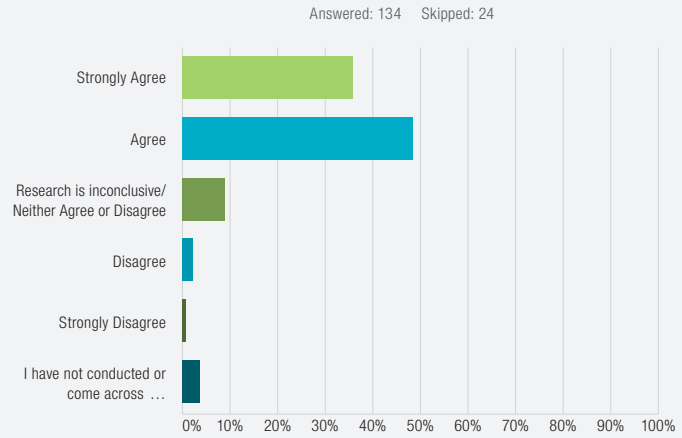
Answered: 134 Skipped: 24



ANSWER CHOICES	RESPONSES	
Strongly Agree	55.97%	75
Agree	34.33%	46
Research is inconclusive/Neither Agree or Disagree	6.72%	9
Disagree	0.00%	0
Strongly Disagree	0.00%	0
I have not conducted or come across research on this topic	2.99%	4
TOTAL		134

Likewise, when asked if the Internet has made it easier to plan attacks or mobilise to violence, the majority of respondents, 84%, agreed or strongly agreed. A respondent summarised the role of the Internet by stating, "the internet and encrypted social media communications in particular have heightened the flow of information, resources, tactical and logistical support and real-time contact which has in turn removed or flattened earlier barriers to mounting attacks." But while the Internet may have made it easier to research, plan and coordinate violence, it has also been a boon for law enforcement. Many plots have been thwarted or prosecuted because of evidence collected on online platforms. Many respondents also gave caveats to their responses by saying that while Internet-enabled communications, particularly encrypted communication, may have made it easier to mobilise, detailed attack planning in fact often occurs offline, particularly for sophisticated plots.

Q10 The use of internet enabled communications and/or social media platforms by extremist actors has made it easier to plan violent attacks/mobilise

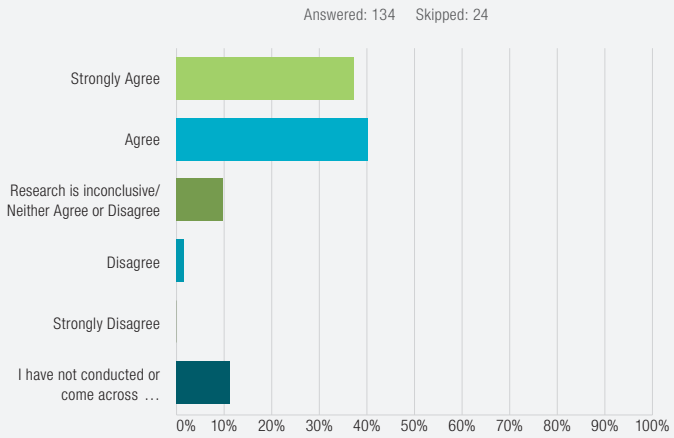


ANSWER CHOICES	RESPONSES	
Strongly Agree	35.82%	48
Agree	48.51%	65
Research is inconclusive/Neither Agree or Disagree	8.96%	12
Disagree	2.24%	3
Strongly Disagree	0.75%	1
I have not conducted or come across research on this topic	3.73%	5
TOTAL		134

Similarly, a majority of respondents agreed or strongly agreed (78%) that Internet-enabled communications have made it easier for extremist actors to fundraise. The Internet has enabled crowdsourced donations, merchandise sales, ad revenue via content channels and the use of crypto-currencies to exchange funds anonymously and securely. One respondent made the point that many extremist groups or individuals actually exist as business enterprises online; they face

"monetary incentives to make the content on their sites as sensational and engaging as possible while remaining vague enough to attract the broadest audience possible."

Q11 The use of internet enabled communications and/or social media platforms by extremist actors has made it easier to fundraise

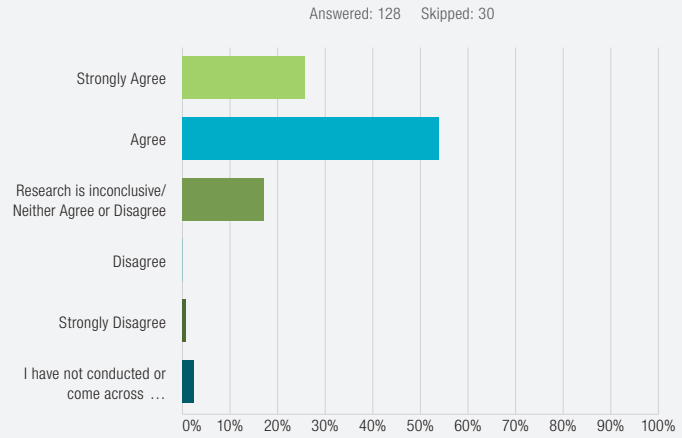


ANSWER CHOICES	RESPONSES	
Strongly Agree	37.31%	50
Agree	40.30%	54
Research is inconclusive/Neither Agree or Disagree	9.70%	13
Disagree	1.49%	2
Strongly Disagree	0.00%	0
I have not conducted or come across research on this topic	11.19%	15
TOTAL		134

When survey participants were also asked more specifically if exposure and engagement with extremist content leads to offline harm, the responses were less decisive. When examining exposure to content specifically, rather than "online activities" more broadly (encompassing communication, fundraising, recruitment, and so on), respondents suggested that engaging with extremist content, as the literature reviews also indicate, can be a contributing factor but not a causal, determinative or sufficient factor. According to one respondent, "There are a lot of predisposing factors before any interaction with extremist content can lead to offline actions, and the causal pathway is not going to be discernible."

However, this consensus may later be challenged, because, as a majority of respondents indicated, the "research was inconclusive." Many respondents noted that "we don't have enough evidence on this," there "simply isn't good enough data," "research uses very limited data," or "very minimal empirical research that clearly shows connection between exposure/interaction with extremist content and offline harm." Again, these responses echo longstanding concerns in the field regarding access to data.

Q13 Online exposure and interaction with extremist content contributes to offline harm?



ANSWER CHOICES	RESPONSES	
Strongly Agree	25.78%	33
Agree	53.91%	69
Research is inconclusive/Neither Agree or Disagree	17.19%	22
Disagree	0.00%	0
Strongly Disagree	0.78%	1
I have not conducted or come across research on this topic	2.34%	3
TOTAL		128

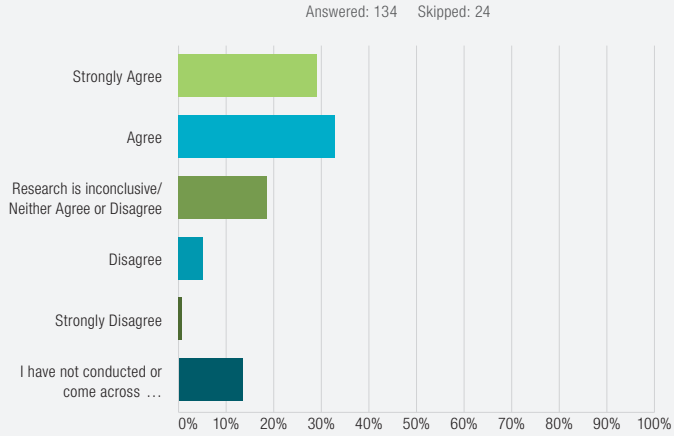
When asked about how certain individuals accessed or were exposed to extremist content, specifically through algorithmic recommendation functions of social media platforms, respondents agreed that algorithmic recommendation played an important role in amplifying content (62% agreed or strongly agreed) but were more circumspect about whether this played a part in an individual's path towards radicalisation – popularly termed as 'going down the rabbit hole.' Many pointed to the fact that research was inconclusive or that there is insufficient research on how algorithmic recommendation factors into the radicalisation process. As one respondent put it, this is an issue "requiring more sophisticated understandings of enmeshed sociality and the social economies of how communities of users actually engage and interact with what they are viewing."

Much of the research on extremist content and algorithmic recommendation focuses on YouTube;[56] one respondent, who indicated that they carried out research on algorithmic recommendation, found that "recommendation algorithms are a key driver for recruitment, radicalization, and propaganda." Another stated

56 Ribeiro et al. (2019) "Auditing Radicalization Pathways on YouTube", *Computers and Society*; Derek O'Callaghan et al. and Tania Bucher suggest a strong connection between algorithms and social behaviour within YouTube.

that "strong evidence suggests that recommender algorithms at the very least can cause desensitization which in turn can lower the viewer's inhibition towards violence … research posits that the immersive nature of social media, including its recommender algorithms, can alter the viewer's perception of reality and can often result in creating a sense of imminence resulting in a feeling that action must be taken immediately."[57]

Q12 Technology platform recommendation algorithms can be an important factor to an individual's path of radicalisation



ANSWER CHOICES	RESPONSES	
Strongly Agree	29.10%	39
Agree	32.84%	44
Research is inconclusive/Neither Agree or Disagree	18.66%	25
Disagree	5.22%	7
Strongly Disagree	0.75%	1
I have not conducted or come across research on this topic	13.43%	18
TOTAL		134

When respondents were asked whether *content moderation – removing or supressing extremist content* – was an effective means of countering extremism and reducing real-world harm, those that were aware of or conducted research around the topic tended to fall into two positions – either "strongly agree/agree" (48%) or "research is inconclusive" (37.5%). A small portion hadn't conducted or come across research on the topic (7.8%). Many of the respondents who did agree that it was an effective means of countering extremism and reducing real-world harm also noted that content moderation was only one means of intervention; as one respondent noted, it is "one puzzle piece in an overall strategy, but by itself, it is probably

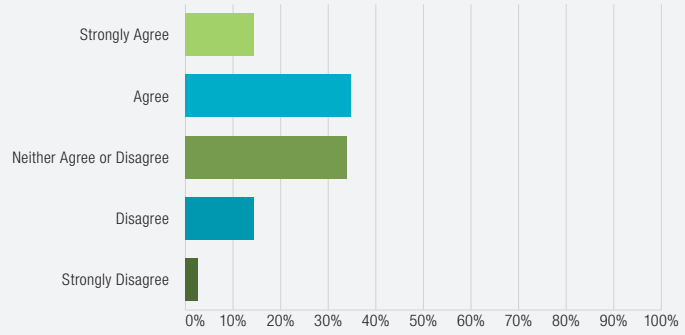
57 J. Berger (2015) "The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion", *Perspectives on Terrorism* vol. 9 no. 4, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/444

not enough to be an effective counter-extremism strategy for the digital sphere."

Some 49% of survey respondents, however, did find that content moderation had an impact on their ability to access data and conduct research on this topic and 34% neither agreed nor disagreed, suggesting that it was not a part of their research. Some respondents said that content moderation has led to a change in research focus and that "content that has been blocked, removed or made inaccessible cannot be studied." Many respondents made the point that there needs to be more systematic archiving of extremist content and accounts. One respondent suggested that "platforms should provide approved researchers with access to moderated content." The Terrorist Content Analytics Platform, developed by Tech Against Terrorism and Public Safety Canada, is one such effort to alert partner tech companies to terrorist content on their platforms both for removal and for archiving in a database of verified terrorist content for research purposes.[58]

Q36 Content moderation and/or deplatforming has affected my access to relevant research data

Answered: 112 Skipped: 46



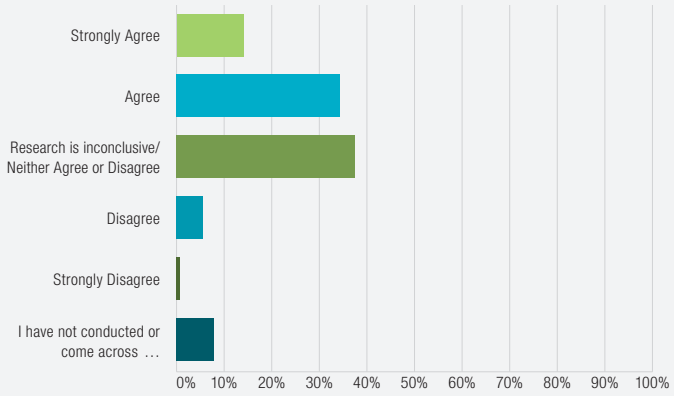
ANSWER CHOICES	RESPONSES	
Strongly Agree	14.29%	16
Agree	34.82%	39
Neither Agree or Disagree	33.93%	38
Disagree	14.29%	16
Strongly Disagree	2.68%	3
TOTAL		112

58 https://www.terrorismanalytics.org/blog/tcap-newsletter-january-2021-jfwmj

As a number of respondents pointed out, content moderation, can be useful in limiting the impact of influencers or the accessibility of information manuals on how to conduct attacks, impeding the establishment of networks and safeguard individuals from accidental or passive exposure to extremist content. However, content moderation does not address drivers of radicalisation to violence and should not be viewed as a singular solution, but one part of a broader strategy of countering violent extremism. One respondent also suggested that content moderation should be on a spectrum: rather than removing content, gradual forms of moderation like demonetisation, making certain content unsearchable, shadow-banning and limiting how users can interact with certain types of content could be more effective.

Q14 Online content moderation- removing or suppressing extremist content – reduces real world violence or harm and/or effective means of countering extremism

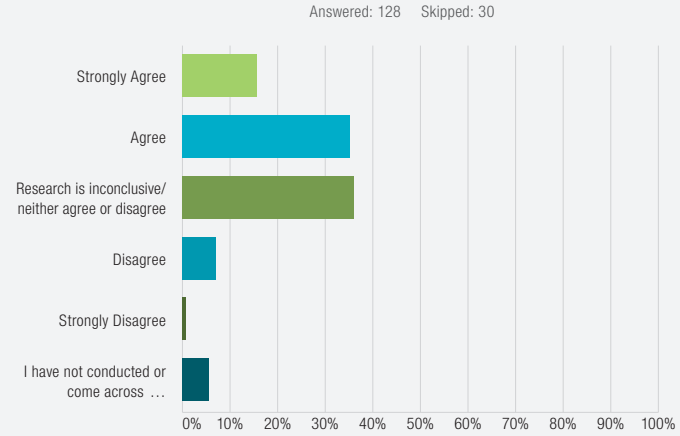
Answered: 128 Skipped: 30



ANSWER CHOICES	RESPONSES	
Strongly Agree	14.06%	18
Agree	34.38%	44
Research is inconclusive/Neither Agree or Disagree	37.50%	48
Disagree	5.47%	7
Strongly Disagree	0.78%	1
I have not conducted or come across research on this topic	7.81%	10
TOTAL		128

With regards to deplatforming extremist actors, just over half agreed or strongly agreed (51%) with the statement that deplatforming extremist actors reduces real-world harms and is an effective means of countering extremism. Some 41% stated that the research was inconclusive or they have not come across research in this area. Only 8% strongly disagreed or disagreed with the proposition that deplatforming is an effective means of countering extremism.

Q15 Deplatforming extremist actors from social media and other technology platforms reduces real world harm and/or effective means of countering extremism



ANSWER CHOICES	RESPONSES	
Strongly Agree	15.63%	20
Agree	35.16%	45
Research is inconclusive/neither agree or disagree	35.94%	46
Disagree	7.03%	9
Strongly Disagree	0.78%	1
I have not conducted or come across research on this topic	5.47%	7
TOTAL		128

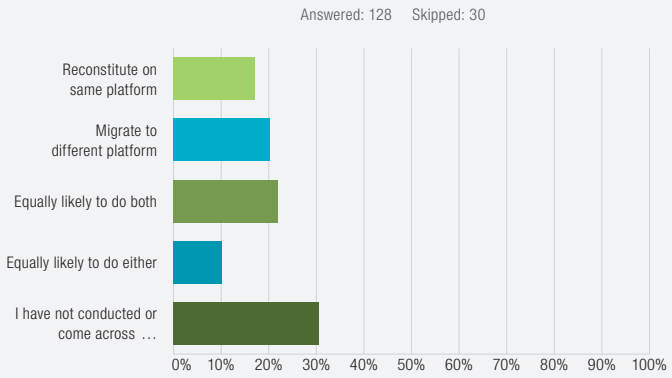
Respondents' comments coalesced around two broad themes. Deplatforming is a useful tool, in that it limits the audience reach of extremist actors, particularly influencers, as they decamp to alt-tech platforms with a lower overall user base. One respondent found that "It seriously impedes their reach, which by default decreases their audience. We also know that even if they come back, they often do not acquire the same [number] of followers again." It also functions to demonetise extremist accounts, limiting funding and income streams. As with content moderation, deplatforming is only one part of a larger effort at countering violent extremism.

Nonetheless, deplatforming can also play into grievances and push extremist actors onto unmoderated, niche and sometimes encrypted platforms, where they can continue to engage with extremist content and networks. When respondents were asked a related question, whether dangerous or extremist actors are more likely to first migrate to another platform or try to reconstitute on the same platform after a suspension (but not final deplatforming), the survey results indicated that we do not yet have enough data or research, with a majority of respondents saying that they have not conducted or come across research on this issue (30%) and the remaining answers spread across the response options.

The comments from some respondents also indicated that this is something that has shifted. Whereas in previous years, deplatformed actors usually attempted to reconstitute a presence on the same platform, more recently deplatformed actors are doing "pre-ban" migrations to other platforms in an attempt to retain their followers. One respondent gave the example of "Alt-Right influencers who had had a couple of 'strikes' strategically broadcast their intentions to migrate prior to being banned. These influencers had large audiences they were trying to 'take with them' as they moved onto platforms like BitChute" so they could retain income streams and give their followers time to adjust to a different platform. Another respondent pointed out that it depended on the platform. While Islamic State eventually gave up on Twitter, it has been more persistent with retaining its presence on Telegram because it finds that platform's features particularly useful.

There is concern that deplatforming could even act as a push factor towards violent radicalisation or serve to solidify extremist views. This concern was mentioned by a number of respondents, but it is potentially contradicted by research by Richard Rogers that found that deplatformed actors who migrate to other platforms become more moderate in their language.[59] It is worth noting, however, that language moderation does not necessarily indicate moderation in views; it could mean these actors are addressing a different communication need.

Q16 Are dangerous/extremist actors more likely to first attempt to reconstitute their social media presence on the same platform when an account has been suspended OR more likely to migrate to a different platform?



ANSWER CHOICES	RESPONSES	
Reconstitute on same platform	17.19%	22
Migrate to different platform	20.31%	26
Equally likely to do both	21.88%	28
Equally likely to do either	10.16%	13
I have not conducted or come across research on this topic	30.47%	39
TOTAL		128

59 R. Rogers (2020) "Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media", *European Journal of Communication* vol. 35 no.3: pp.213–29, https://doi.org/10.1177/0267323120922066

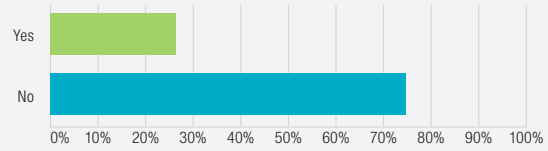
Researcher Engagement with the Tech Industry

The second part of the survey focused on researchers' engagement with the tech industry itself. It sought to gain insight into if and how researchers engaged with the technology. When asked what type and level of engagement a researcher has had with technology companies, the answers varied widely. Responses ran from working closely with technology companies, co-producing research and briefing them on research updates, to no engagement at all. Much of the engagement was through GIFCT or via academic conferences. There were also a number of responses that indicated a cynicism about tech industry engagement with the academic community, with one respondent saying, "Tech companies don't 'engage', they just make it look like they are addressing problems while continuing with many of the same practices until a crisis forces change."

A factor, but certainly not the only one, motivating researchers (47% of the respondents) to engage more with tech companies is a desire for access to data. Yet when asked if they had approached a company to obtain data to inform their research, 75% said no. Of those who had asked, the majority was not able to obtain said data. Some respondents who indicated that they initially did not ask social media companies for data either understood that company policies usually did not allow for this or did not have appropriate channels to approach tech company representatives. When asked if they had clear pathways to appropriate departments in tech companies to discuss research or whether they understood how tech companies might approve research collaboration or access to data, the majority of respondents (46% and 60% respectively) answered no. According to one respondent, the process to enquire about research engagement or data sharing was "highly opaque." Many respondents commented that they were unsure what opportunities for engagement were available, who to contact, how to contact them or simply that engagement with the tech sector was not a priority for them.

Q40 Have you approached a tech company to obtain data to inform your research?

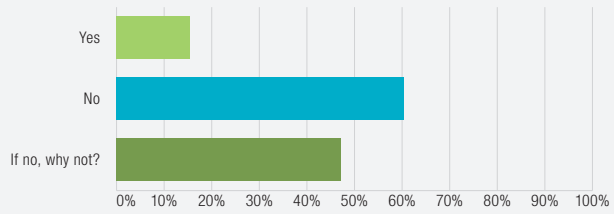
Answered: 91 Skipped: 67



ANSWER CHOICES	RESPONSES	
Yes	26.37%	24
No	74.73%	68
Total Respondents: 91		

Q41 Were you able to obtain this data?

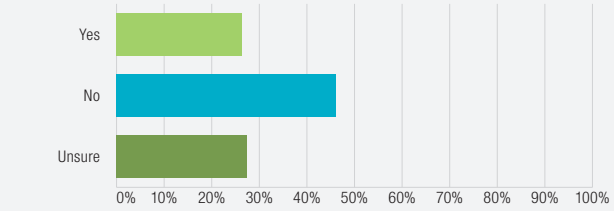
Answered: 91 Skipped: 67



ANSWER CHOICES	RESPONSES	
Yes	15.38%	14
No	60.44%	55
If no, why not?	47.25%	43
Total Respondents: 91		

Q42 Do you have clear pathways into appropriate departments at tech companies that allow you to discuss research?

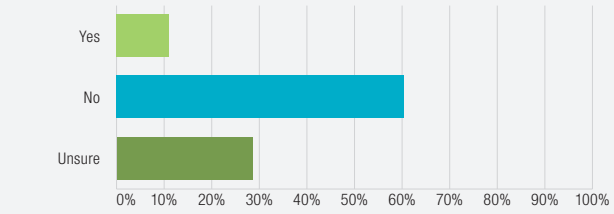
Answered: 91 Skipped: 67



ANSWER CHOICES	RESPONSES	
Yes	26.37%	24
No	46.15%	42
Unsure	27.47%	25
TOTAL		91

Q43 Do you understand the review processes used by tech companies in approving research or access to data?

Answered: 91 Skipped: 67



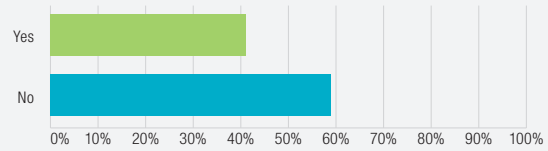
ANSWER CHOICES	RESPONSES	
Yes	10.99%	10
No	60.44%	55
Unsure	28.57%	26
TOTAL		91

When asked about other constraints regarding data, such as whether academic ethics approval processes, legislation and privacy considerations impacted data access, 59% of respondents said no and 41% said yes. Universities in different jurisdictions have differing ethics approval processes and not all researchers work within a university setting, which helps to explain the variation in responses. Obtaining ethics approval was also not the only limitation. Respondents pointed to the fact that certain legislation makes possession of material of relevance to terrorism an offense and that study and/or research of such material is not considered a defence. GDPR legislation was also cited. As one respondent – who said that ethics approval processes and privacy considerations did constrain access to data – noted, the result of this has been to force many researchers to rely on secondary data.

A number of respondents commented on the difficulty in dealing with international review boards (IRB) or ethics committees. One respondent commented, "I have avoided research questions that would result in difficult interactions with IRB committees." Many IRBs provide ethics approval only if data collection respects the terms of service of the platform, which, given the terms of most platforms, has in effect meant that accessing data is not possible. One respondent suggested that IRBs need a better understanding of online data for research because, as respondents indicated, many IRBs have a "too broad definition of private space online" and "Ethics boards don't understand the nature of online research/ extremism research." Additionally, the time it takes for ethics approval has also stymied the ability of researchers either to access data or report on their findings from this data, as by the time ethics approval is given, data may have been removed.

Q32 Have academic ethic approval processes and/or privacy considerations, policies or legislation impacted your ability to access data?

Answered: 112 Skipped: 46



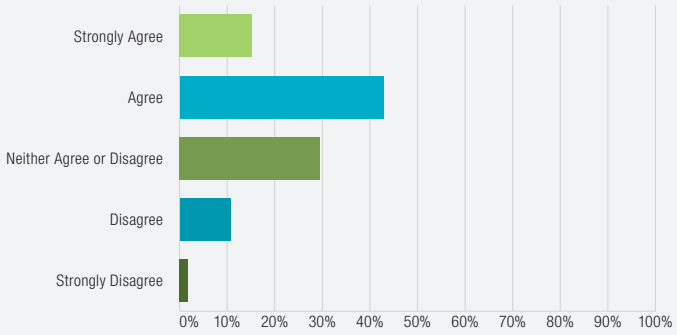
ANSWER CHOICES	RESPONSES	
Yes	41.07%	46
No	58.93%	66
TOTAL		112

Respondents were asked a related question, whether "Academic ethic approval processes and/or privacy considerations, policies or legislation constrain research of extremist/dangerous actors and movements on online platforms" more broadly. The respondents' concerns around ethics approval were also noted in the work of John Morrison, Andrew Silke and Eke Bont, who state that "there have to this point been no objective criteria to assist reviews in their judgement

of the risk or benefits of terrorism research." As a result, they have developed a recently published framework for research ethics in terrorism studies, which can help address this need.[60]

Q31 Academic ethic approval processes and/or privacy considerations, policies or legislation constrain research of extremist/dangerous actors and movements on online platforms

Answered: 112 Skipped: 46



ANSWER CHOICES	RESPONSES	
Strongly Agree	15.18%	17
Agree	42.86%	48
Neither Agree or Disagree	29.46%	33
Disagree	10.71%	12
Strongly Disagree	1.79%	2
TOTAL		112

While many respondents included comments about the difficulties of academic ethics approval processes, a number did also believe that these constraints were appropriate and necessary, stating "They do constrain research – but on the whole these constraints are appropriate" and "It's important to have strict measures when operating in these spaces for ethical reasons and the safety of the researcher themselves. I know of some cases where independent researchers have been threatened as a result of the manner in which they engage with their extremist research subjects."

Privacy considerations, ethics approval processes, platform terms of service and the like have meant that it is very difficult for researchers to study an individual's online activity and/or their engagement with extremist content. When respondents have been able to do so, it was through accessing "court documents relating to cases of terrorist activity" through secondary open-source data, such as newspaper reports, press releases, and so on. Other respondents were able to interrogate an individual's online activity via direct questionnaires administered to lone actors in prison, self-reporting from voluntary participants or focus groups on why and how young people engage with extremist material. There were only a handful of respondents who indicated that they have been able to do in-depth analysis of individuals' online activity and longitudinal studies of individuals,

60 John Morrison, Andrew Silke & Eke Bont (2021) "The Development of the Framework for Research Ethics in Terrorism Studies (FRETS)", *Terrorism and Political Violence*, 33:2, 271–289, DOI: 10.1080/09546553.2021.1880196

tracking their online activity before they became involved in militant activity, as well as comparative studies of the posting behaviour of violent and non-violent extremists. Respondents' answers indicate there are some recently published research in this area and some forthcoming, with one respondent mentioning that they are "involved in the acquisition of big data drawn from various social media platforms in accordance with an approved ethics application. This has provided insights into the activities of individuals online in relation to content associated with violent extremist ideologies."

4 Conclusion

The hope is that this survey will complement literature reviews of the role of Internet technology on violent extremism and form a preliminary point of inquiry into the state of engagement between the tech industry and the research community. A key lesson in the development and synthesis of the survey responses was that parsing the role of technology in violent extremism is incredibly complex, multifaceted and still contested. Empirical research in this area is still limited but growing.

Insights were also gained from what was not asked and questions we received about our approach, in addition to the responses to what was asked. Indeed, a few respondents to this survey highlighted the need for more specificity and precision in the survey question design. While we asked questions generally related to 'extremist actors', many respondents pointed out that their answers depended on the type of actor and movement and that it was not possible to generalise. Additionally, many of the questions posed on the impact of technology, particularly social media, on violent extremism were comparative in nature. However, as one respondent pointed out, there has been little to no research that compares the pre- and post-Internet environment. This is a gap in the research, one that is difficult to fill and will impact how research and survey questions on these topics are designed in future.

In terms of engagement between researchers and the tech industry, this has emerged as a potentially fruitful but also fraught space – much in the same way there remain dilemmas and considerations around collaboration with governments and security agencies among the terrorism research community and concerns around the securitisation of academic research. Some researchers have similar concerns about engaging and collaborating with the tech industry and identified additional ones, such as the ethics of engaging with for-profit companies, the opacity and lack of transparency of major platforms, their reactive nature, differing research priorities to industry and scepticism around how seriously and effectively social media platforms are tackling violent extremism and harmful disinformation. The hope is that the research gaps, challenges and opportunities around engagement between the research community and the tech industry identified in this survey can be further explored and addressed.

Policy Landscape

This section is authored by Lucy Thomas and Constance Woollen, both Research Associates at the Policy Institute based at King's College London. It provides an overview of the relevant policy landscape for this report.

Introduction

In this report, we discuss the policy landscape and legislation in place in nine jurisdictions to fund research into counter-terrorism. Funding comes in different forms and from different sources, such as directly from a government department or indirectly through, for example, a research council, as is the case in the UK and France. Some of the funded research is clearly policy-oriented; the European Commission, New Zealand and the UN each fund research in response to specific counter-terrorism policy needs. In other jurisdictions, like the UK and France, the funding of PhD students might feed less directly into current counter-terrorism strategies but could act as a path to employment for these students in national security agencies. The establishment of networks to share current counter-terrorism research is also common, with five of the nine jurisdictions having made this move in the last decade (Canada, the European Commission, France, New Zealand and the UN).

We conclude with a discussion of the wider ethical challenges implicit in collaborations between researchers and policymakers and describe the steps that might be taken to move towards an ethical countering violent extremism (CVE) research agenda. These include (1) de-emphasising the solutionist paradigm and instead investigating the impact of counter-terrorism on racialised and marginalised communities, and making policy recommendations to alter these policies based on the findings; (2) using CVE research to advocate for policies that seek to redress historical and structural violence; (3) investigating the impact of policies that uplift communities, like greater investment in housing and mental health support, and, as a result, using CVE research to push for a different kind of intervention in pathways to violence.

Government-funded Research into Countering Violent Extremism

Canada

The Canadian government's counter-terrorism and counter-radicalism strategy is expansive, encompassing traditional intelligence and security agency activities, engagement with civil society, collaborative initiatives with industry and community-focused policing. Its strategy, as laid out in its National Strategy on Countering Radicalization

to Violence, has three main strands of direction: to develop counter-messaging with civil society, to support CVE research and to partner with international initiatives and tech companies.[61]

Since investment into research is one of the Canadian government's stated objectives, it follows that their programme of government-funded research is one of the most developed and committed of all the jurisdictions under examination here. Public Safety Canada, Canada's public safety and emergency preparedness directorate, houses the Canada Centre for Community Engagement and Prevention of Violence, which leads the government's CVE response. The Canada Centre, launched in 2017, coordinates a number of CVE activities, including policy guidance, collaboration with stakeholders, supporting initiatives and interventions, and funding and conducting research. Research funded by the Centre includes scholarship intended to "better understand radicalization to violence and how best to counter it, and mobilizing research to front-line individuals working to prevent radicalization to violence".[62]

In conjunction with the Community Resilience Fund, an initiative that works with organisations and local communities, the Centre has funded a range of projects, including resilience against online hate speech, knowledge of the Incel community, families and radicalisation to violence, the far right in Québec, counter-messaging initiatives, and more. Partners and stakeholders included in the funded research include higher education institutions in Canada and overseas, policy actors such as Moonshot CVE, think tanks such as the Institute for Strategic Dialogue, local and civil society actors such as the Boston Children's Hospital, and others.[63] The last Call for Proposals issued covered the 2018–19 period, so it is unclear whether the Canadian government is continuing to fund future research into CVE via this channel.[64]

Additionally, the Canadian Network for Research on Terrorism, Security and Society (TSAS), founded in 2012, supports research and its dissemination relating to "the threat of terrorism, security responses to terrorism, and the impact of both terrorism and securitization on Canadian society".[65] TSAS is an independent academic organisation that often partners with government agencies to carry out research.[66] Its primary objectives are to foster communication and collaboration between academic researchers in multiple disciplines on these topics, to facilitate the interaction and collaboration of researchers and policy officials, and to help to cultivate a new and larger generation of scholars interested in these fields of study.[67]

61 "National Strategy on Countering Radicalization to Violence", Public Safety Canada. Accessed: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx#s7
62 https://www.publicsafety.gc.ca/cnt/bt/cc/index-en.aspx
63 https://www.publicsafety.gc.ca/cnt/bt/cc/fpd-en.aspx
64 https://www.publicsafety.gc.ca/cnt/bt/cc/fnd-en.aspx
65 https://www.tsas.ca/about/
66 https://www.publicsafety.gc.ca/cnt/bt/cc/res-en.aspx See area under "The Canadian Network for Research on Terrorism, Security and Society (TSAS)"
67 Ibid.

European Commission

The European Commission's counter-terrorism strategy sits under the Department of Migration and Home Affairs (DG HOME).[68] The Commission has been funding research into counter-terrorism for around 15 years, first launching research into radicalisation under the 2007–2013 Seventh Framework Programme.[69] More recently, two Communications (policy papers) have been published by the European Commission on preventing radicalisation. These are presented to policymakers across EU institutions. The funding of research into counter-terrorism, and radicalisation in particular, is central to both of these communications, with increasingly policy- and impact-oriented aims.

In 2016, COM(2016) 379 was published in response to the terror attacks seen across Europe,[70] aiming to "support Member States in preventing radicalisation leading to violent extremism in the form of terrorism".[71] In this communication, the Commission argued that recent terror attacks showed "new trends" in the processes of radicalisation that required further investigation. As such, the Commission introduced research priorities to "further bridge the gap between academia and security practitioners in this field".[72] This research, on the root causes of violent radicalisation, which aimed to deliver concrete tools and inform policy interventions,[73] was mobilised under Horizon 2020, "the biggest EU Research and Innovation programme ever" with nearly €80 billion in funding available between 2014 and 2020.[74] The focus of the Commission on involving a wide array of actors in its counter-terrorism strategy is highlighted by the additional establishment of the (now defunct) Radicalisation Awareness Network Centre of Excellence (RANCE), a network of member state actors to share, among other things, knowledge on radicalisation.[75]

A further Commission communication, COM(2020) 795, followed in 2020, outlining a more far-reaching counter-terrorism agenda for the EU.[76] Building on the research funded by the Seventh Framework Programme for Research and Horizon 2020, this agenda set out plans to continue counter-terrorism research. A key aspect of this communication was to fund, specifically, "EU-security research to strengthen early detection capacity and develop new technologies under the Urban Agenda for the EU".[77] This research would be used to strengthen early detection capacity of potential terrorist threats through artificial intelligence and big data projects; addressing radicalisation was once again included in the strategy.[78] Funding for this research will come from Horizon 2020's successor, Horizon Europe, which will run until 2027.[79] While researchers, academics and research agencies are not explicitly named in the communication, it is clear that the EU intends this research to be impact-oriented, deeply integrated in the security policy cycle and a response to the needs

68 https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/radicalisation_en
69 https://ec.europa.eu/transport/themes/research/fp7_en
70 https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-379-F1-EN-MAIN-PART-1.PDF, p.2
71 Ibid., p.3
72 Ibid., p.4
73 Ibid., p.5
74 https://ec.europa.eu/programmes/horizon2020//en/what-horizon-2020
75 https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/COM-2016-379-F1-EN-MAIN-PART-1.PDF, p.5
76 https://ec.europa.eu/home-affairs/sites/default/files/pdf/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf
77 Ibid., p.6
78 Ibid., p.4
79 https://ec.europa.eu/info/horizon-europe_en

of law enforcement.[80] In addition to the research funded by Horizon Europe, the Commission is promoting the sharing of research and knowledge between policymakers, practitioners and researchers on counter-terrorism in this communication. It proposes to establish an EU "Knowledge Hub" on the prevention of radicalisation similar to RANCE.[81] This does not appear to be associated with additional funding opportunities but will point researchers in the direction of funding possibilities under the various EU programmes.[82]

France

In France, the cross-governmental Interministerial Committee for the Prevention of Crime and Radicalisation (CIPDR) has jurisdiction over its counter-terrorism strategy.[83] The committee brings together ministers from the Home and Justice departments, among others,[84] and is led by the Prime Minister.[85] The CIPDR is the source of some direct funding of research. The French government also funds research into counter-terrorism indirectly, through its National Research Agency (ANR). Whilst CIPDR-funded research is intertwined more closely with the French counter-terrorism strategy, ANR research appears to be less policy-oriented.

In 2016, the Second Plan of Action against Radicalisation and Terrorism (PART) was published by the CIPDR as an updated policy for the prevention of radicalisation, based on social as well as security-related considerations.[86] Both PART and its 2014 predecessor, the Counter-Terrorism Plan (PLAT), had prevention at their core, involving detection, training and hands-on intervention in society and the judicial system, and the furthering of research in this field.[87] Specifically, PART included seven broad aims related to radicalisation, with 80 measures split across them.[88] One of these broad aims (with ten associated measures) was to develop applied research by establishing a research network to coordinate and share findings, funding PhD students,[89] and funding private initiatives disseminating a critical discourse on the ideologies of radicalisation or an open discourse of knowledge about Islam.[90]

More recently, in 2018, the CIPDR published the National Plan to Prevent Radicalisation to replace PLAT and PART.[91] This most recent iteration includes one specific measure related to research, of 60 overall, focusing on funding for PhD students,[92] as well as assisting French applications to the European Commission Horizon 2020 funding scheme (see 'European Commission' section above for more detail on counter-terrorism research funding). The research outputs

80 https://ec.europa.eu/home-affairs/sites/default/files/pdf/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf, p.4
81 Ibid., p.9
82 Ibid.
83 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf
84 https://www.cipdr.gouv.fr/pnpr/
85 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf, p.5
86 Ibid.
87 Ibid.
88 https://www.cipdr.gouv.fr/announcement/second-plan-daction-contre-la-radicalisation-et-le-terrorisme-part/
89 https://www.gouvernement.fr/sites/default/files/document/document/2016/05/09.05.2016_dossier_de_presse_-_plan_daction_contre_la_radicalisation_et_le_terrorisme.pdf, p.8
90 Ibid., p.9
91 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf
92 Ibid., p.15

of this CIPDR funding are not named explicitly but are intertwined with the national strategy and, therefore, appear to be policy- and impact-oriented.

The ANR, on the other hand, sits under the French Ministry of Higher Education, Research and Innovation and funds, more generally, project-based research involving collaboration between the public and private sectors.[93] The aims of the ANR are, as a result, more research-related than subject-specific and focus on, for example, funding multi-disciplinary research, rather than motivating research into a particular area like counter-terrorism. As of April 2021, ten pieces of research into "violent extremism" had been funded by the ANR between 2011 and 2020,[94] and three projects on "counter-terrorism" had been funded between 2018 and 2020.[95] Through the ANR, this research has been indirectly funded by the French government but it does not appear to be explicitly policy-oriented or related to the country's counter-terrorism strategy.

Ghana

Although the Republic of Ghana has had little experience of terrorist attacks on its soil and therefore has no national or regional counter-terrorism strategy,[96] there is a clear state approach to policing and intelligence. The Anti-Terrorism Act of 2008, passed in accordance with international legal obligations post-9/11, is "a piece of legislation enacted to combat, suppress and prevent the use of Ghana's territory as a terrorist hub".[97] The act punishes the crime of terrorism and, in line with UN Security Council Resolution 1373, criminalises terrorist financing and materials, possession of terrorist property, incitement and promotion of a terrorist agenda.[98]

The act confers expansive powers to the police and judiciary system to surveil and search suspects of terrorism. Section 24 states that the police can conduct physical searches of a person and "break open premises and forcibly enter" them if it has "reasonable grounds" to suspect there is property used to carry out a terrorist act.[99] Crucially, the police can carry out these physical searches without securing a warrant or placing a suspect under arrest.[100] The act also gives wide-reaching surveillance powers to the state to intercept communications where there is "reasonable suspicion" of a terrorist act being carried out. This legislation laid the foundations for two developments in Ghanaian counter-terrorism strategy: first, a 2012 amendment to the act in which (in line with international best practice) groups designated terrorist were subject to financial sanctions and the freezing of assets,[101] and intertwined immigration control with counter-terrorist strategy.[102]

93 https://anr.fr/en/anrs-role-in-research/missions/
94 https://anr.fr/en/funded-projects-and-impact/funded-projects/?q=violent+extremism&id=1781&L=1
95 Ibid.
96 https://issafrica.org/iss-today/slow-progress-for-west-africas-latest-counter-terrorism-plan
97 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDI07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, p.56
98 Ibid., p.57
99 https://acts.ghanajustice.com/actsofparliament/anti-terrorism-act-2008-act-762/, section 24
100 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDI07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, pp.58–9
101 https://www.mint.gov.gh/wp-content/uploads/2017/06/Anti-Terrorism-Reg-L.-I.-2181.pdf, sections 5 and 6
102 Ibid., section 4

Secondly, and importantly in terms of online violent extremism, tighter counter-terrorism legislation paved the way for the government to introduce the Interception of Postal and Telecommunications Message Bill in early 2016. The bill, dubbed the "Spy Bill", was to legislate to allow "the interception of post and electronic or cyberspace communications for the purpose of protecting national security in the fight against organised crime including terrorism." The Spy Bill was notable in its lack of accountability or oversight, particularly since Section 4(3) allowed the government to defer a court order or warrant for surveillance for 48 hours. This, as well as the lack of oversight mechanism, opened up the door for potential abuses and secret surveillance.[103] Under civil society pressure, the Bill was withdrawn.[104]

Ghana's repressive and abuse-prone counter-terrorism environment is an expression of a wider trend of post-colonial states inheriting paramilitary approaches to policing from their colonial masters – in the case of Ghana, from British colonial authorities.[105] Despite a resource-rich and growing manufacturing and export economy, continuing neo-colonial economic reliance on Western institutions (such as the International Monetary Fund) means that corruption is rife and poverty rates remain high.[106]

In this context, it is perhaps unsurprising that contemporary CVE strategy in Ghana does not include "softer" elements such as government-funded research. Research and initiatives relating to CVE tend to be funded by non-state actors, including regional groups, civil society groups and external governments. For instance, a high-profile workshop addressing the root causes of violent extremism in 2016 was funded by the Kofi Annan International Peacekeeping Training Centre, the African Centre for the Study and Research on Terrorism, and the Spanish government.[107] Counter-terrorism knowledge exchange activities in 2019 and 2020 have been funded by the UN Counter-Terrorism Executive Directorate,[108] and the UN Office on Drugs and Crime with the German government.[109]

Japan

Similar to Ghana above, Japan's domestic approach to CVE is based on criminalisation and policing. One legacy of the Cold War era was that Japanese intelligence activities on domestic soil, centring around combating the ostensible communist threat, are largely coordinated by law enforcement agencies. Prefectural police (overseen by the National Police Agency) and the Public Security Intelligence Agency (Japan's national intelligence agency) lead intelligence-gathering and counter-terrorism efforts on Japanese soil.[110]

103 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDl07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, pp.60–61

104 https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Spy-Bill-withdrawn-from-Parliament-451805

105 https://journals.sagepub.com/doi/pdf/10.1177/1461355716638114

106 See Walter Rodney (2018) *How Europe Underdeveloped Africa* (London: Verso Books); https://www.imf.org/en/News/Articles/2015/09/14/01/49/pr15159; https://www.tandfonline.com/doi/abs/10.1080/01900692.2011.598272; https://www.unicef.org/ghana/media/531/file/The%20Ghana%20Poverty%20and%20Inequality%20Report.pdf

107 https://caert.org.dz/Reports/Final%20Report%20for%20CVE%20Workshop_7-8Nov2016.pdf

108 https://www.un.org/sc/ctc/news/2019/10/04/cted-conducts-follow-visit-republic-ghana/

109 https://www.unodc.org/westandcentralafrica/en/2020-09-28-ghana-counter-terrorism.html

110 Ken Kotani (2013) "A Reconstruction of Japanese Intelligence: Issues and Prospects", in Philip H. J. Davies & Kristian C. Gustafson (eds.), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington D.C.: Georgetown University Press): pp.181–99.

In terms of domestic terror activity online, traditional policing and security architectures are mobilised.[111] Innovative technological developments are a hallmark of Japanese scientific research and export trade, and this is also reflected in its security strategy. The Japanese government has invested heavily in AI-led solutions, including large-scale facial recognition, biometric authentication and behaviour detection systems.[112] These solutions suggest a governance model centred around early detection and prevention, operationalised through traditional police and security tactics.

In response to a hostage crisis in which two Japanese citizens were killed by Islamic State in Syria, Japan launched a counter-terrorism unit in 2015, staffed by its foreign and defence ministries, the NPA and the Cabinet Intelligence and Research Office.[113] The unit suggests a move toward strengthening national intelligence and security capabilities. Indeed, the former prime minister Shinzo Abe forced a "brutal"[114] anti-terror bill through parliament in mid-2017.[115] The legislation criminalises planning to commit over 270 "serious crimes" that include sit-in protests and music copyright infringements; its enforcement extends to social media.[116] Civil rights activists have voiced concern about the law, given its scale and the power it grants law enforcement in Japan to surveil and police online activity.[117]

With regard to counter-terrorism activities internationally, Japan's approach diverges dramatically from its domestic emphasis on criminalisation. Its overseas counter-terrorism efforts are regional, capacity-building and cooperative. The Association of Southeast Asian Nations (ASEAN) is the forum through which many of Japan's overseas counter-terrorism efforts are funnelled,[118] which issued a set of declarations. These declarations commit the signatories to "prevent, disrupt and combat international terrorism through information exchange, intelligence sharing and capacity building", establishing a precedent for regional cooperation to CVE and terrorism.[119] Japan has hosted the annual ASEAN-Japan Counter Terrorism Dialogue twice and has engaged in bilateral talks with a range of global actors.[120] For example, in late 2019, Japan and the UK held discussions on "the current situation of international terrorism, domestic measures to counter terrorism, and also on current counter-terrorism capacity building cooperation particularly in third [*sic*] countries."[121]

111 https://www.mofa.go.jp/files/000156881.pdf, section on "Domestic Counter-Terrorism Measures"
112 The Government of Japan, "All is Ready for a Safe and Secure Tokyo Games", https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html; "NEC Becomes a Gold Partner for the Tokyo 2020 Olympic and Paralympic Games", NEC Corporation, 2015, https://www.nec.com/en/press/201502/global_20150219_01.html; Kyodo News (29 January 2018) "Kanagawa police eye AI-assisted predictive policing before Olympics", https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html
113 https://www.voanews.com/east-asia/japan-launches-anti-terrorism-unit-ahead-summit-olympics
114 B. Allen-Ebrahimian (16 June 2017) "Japan Just Passed a 'Brutal,' 'Defective' Anti-Terror Law'", *Foreign Affairs*, https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/
115 The Bill passed via "the unusual step of skipping a vote in the Upper House Committee on Judicial Affairs". Japan Federation of Bar Associations (15 June 2017) "Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy", https://www.nichibenren.or.jp/en/document/statements/170615.html
116 J. McCurry (15 June 2017) "Japan passes 'brutal' counter-terror law despite fears over civil liberties", *The Guardian*, https://www.theguardian.com/world/2017/jun/15/japan-passes-brutal-new-terror-law-which-opponents-fear-will-quash-freedoms; J. Adelstein (15 June 2017) "Japan's Terrible Anti-Terror Law Just Made 'The Minority Report' Reality", *The Daily Beast*, http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality
117 Japan Federation of Bar Associations, 'Statement on the Enactment of the Bill"
118 "Japan: Extremism & Counter Extremism", Counter-Extremism Project, https://www.counterextremism.com/countries/japan
119 "ASEAN-Japan Joint Declaration for Cooperation to Combat International Terrorism", ASEAN, https://asean.org/?static_post=asean-japan-joint-declaration-for-cooperation-to-combat-international-terrorism-2
120 "Japan: Extremism & Counter Extremism"
121 Ministry of Foreign Affairs of Japan (4 December 2019) "The 4th Japan-the UK Counter-Terrorism Dialogue", https://www.mofa.go.jp/fp/is_sc/page1e_000297.html

In this context, it is not clear that the Japanese government funds research into CVE along with civil society or academic partners in terms of domestic online violent extremist activity. In keeping with the national-international split, however, Japan has funded research and workshops in conjunction with the UN. For example, Japan partnered with the UN Office on Drugs and Crime to publish international guidance to prevent child recruitment and exploitation by violent extremist groups,[122] and with UN Women to understand the gendered dynamics of violent extremism.[123] These activities boost the international profile of Japan as cooperative and progressive in terms of CVE governance. But in order to protect its citizens' freedom and privacy effectively, Japan should commission research and shape policy with these concerns in mind.

New Zealand

The overarching response to countering terrorism in New Zealand involves coordination between several different government departments, communities and private sector organisations. High-level governance is provided through the Cabinet External Relations and Security committee and the Security and Intelligence Board. New Zealand's overarching strategy is outlined in its Counter-Terrorism Strategy plan, released in February 2020.[124] The Christchurch attack in March 2019 led to various responses in counter-terrorism in New Zealand, including the international Christchurch Call and the New Zealand-specific Royal Commission Report, in which research is frequently discussed.

The Christchurch Call summit, a global response to the March 2019 mosque attack, saw world leaders and Internet companies come together for a summit in Paris focused on tackling terrorist use of the Internet.[125] The event, co-chaired by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron,[126] set out a four-phase strategy to counter extremist content, one of which was "Understanding, mapping and analysing research (conducted or identifying the gaps) on violent extremism online",[127] due to the paucity of research and progress in mapping and understanding online extremism.[128] By signing the Christchurch Call to Action, governments agreed to accelerate research and development of tools to prevent, detect and remove uploads of terrorist and extremist content, drawing on expertise from academia, researchers and civil society.[129] As such, the Christchurch Call could be seen as widening the reach of New Zealand's community- and civil society-centred approach to counter-terrorism, compared to countries like the UK and France that signed the Call and tend towards more traditional models.

In terms of specifically New Zealand-centric counter-terrorism funding, the Report of the Royal Commission of Inquiry into the terrorist

122 https://www.unodc.org/unodc/en/frontpage/2019/March/unodc--japan-gather-countries-from-asia--the-middle-east-and-north-africa-to-protect-children-affected-by-terrorism-and-violent-extremism.html
123 https://thediplomat.com/2018/03/japan-helps-explore-the-gender-dynamics-of-violent-extremism/
124 Government of New Zealand, Officials' Committee for Domestic and External Security Coordination, Counter-Terrorism Coordination Committee (February 2020) "Countering terrorism and violent extremism national strategy overview", https://dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf
125 https://www.gov.uk/government/news/pm-joins-christchurch-call-to-action-on-online-terror
126 Ibid.
127 https://www.orfonline.org/research/one-year-since-the-christchurch-call-to-action-a-review/
128 https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/christchurch-call-to-eliminate-terrorist-and-violent-extremist-content-online
129 Ibid.

attack on the Christchurch mosque on 15 March 2019,[130] released to the public on 8 December 2020,[131] included 44 recommendations to the government. Recommendation 16 of the report involves the funding of independent research on the causes of and measures to prevent violent extremism and terrorism.[132] The research described appears to be policy-oriented, given that, according to the associated provisions for funding, the (proposed) national intelligence and security agency should be provided with a multi-year appropriation for research funding and research priorities and grant recipients should be selected by a panel comprising officials from the new national intelligence and security agency.[133] A further recommendation was made to establish an information-sharing network on CVE and terrorism, between relevant central and local government agencies, communities, civil society, the private sector and researchers.[134] The government formally accepted all recommendations made in the report. However, implementation appears to have been slow; in a speech on 8 December 2020, Jacinda Arden apologized on behalf of the government for the lapses in implementation.[135] In her speech, the prime minister did not refer to the implications of funded research directly but said the government would act on some recommendations immediately, while others would be considered in partnership with parliament and New Zealanders.[136] What is clear is that the research that will be funded is policy-oriented and, if carried out in line with the Royal Commission recommendations, will involve close ties to the national security agencies. The measures proposed in the Royal Commission therefore appear to encompass conventional security and intelligence structures as well as initiatives that bring together civil society, academia and policymakers in their counter terrorism strategy.

United Kingdom

In the UK, the Home Office is tasked with counter-terrorism legislation and policy, while the National Security Council (NSC), chaired by the prime minister, is the main forum for collective discussion of the government's objectives for national security.[137] The NSC, in turn, sets the priorities of the Government Communications Headquarters (GCHQ).[138] The UK government funds research into counter-terrorism both directly and indirectly, via these various bodies. That funding is made available (mostly) indirectly and research outputs are published through independent agencies is not surprising given the UK's more traditional CVE strategy. There appear to be four main ways in which the UK funds research into counter-terrorism, which are described from most to least directly-funded.

The Conflict, Stability and Security Fund (CSSF), launched in 2015 as a catalyst for a more integrated UK government response to fragility and conflict, is a £1.26 billion annual cross-government fund that

130 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf
131 https://christchurchattack.royalcommission.nz/the-report/download-report/download-the-report/
132 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf, p.26
133 Ibid.
134 Ibid., p.27
135 https://www.tvnz.co.nz/one-news/new-zealand/full-statement-jacinda-ardern-apologises-agrees-all-recommendations-in-christchurch-attack-report
136 Ibid.
137 https://www.gov.uk/government/groups/national-security-council
138 https://www.gchq.gov.uk/section/mission/overview

includes the Home Office and Cabinet Office.[139] As part of the CSSF, the Counter Terrorism Programme Fund (CTFP) was established, with the Enablers Programme as one its modes of operating. The Enablers Programme was intended to support research that improves the government's understanding of terrorism and violent extremism.[140] While the nature of the research undertaken is not made clear online, it can be assumed that it is related to counter-terrorism, given that this part of the CTFP is designed to support delivery of aspects of the overseas elements of CONTEST.[141]

CONTEST, the UK's Strategy for Countering Terrorism, which was updated in 2018 by the Home Office,[142] makes several references to research, particularly in relation to one of its "tried and tested" strategic work strands, "Prevent".[143] Prevent is underpinned by "continuous research and evaluation".[144] This underpinning is, again, not described in detail but involves, for example, collaboration with research organisations and engagement with academics to better understand how terrorists use the Internet to radicalise vulnerable individuals.[145] Also described in the Strategy is the foundation of counter-terrorism work in "science, technology, analysis and research",[146] and the Home Office's future plans to "enhance collaboration with academia and the private sector to ensure [they] can access and exploit the most advanced technology, advice and solutions for counter-terrorism".[147]

Less explicitly funded by the UK government is the Centre for Research and Evidence on Security Threats (CREST), the UK "hub for behavioural and social science for national security".[148] CREST received government funding both directly and indirectly, from the UK intelligence and security agencies and the Home Office,[149] and the Economic and Social Research Council (ESRC), part of the public body responsible for supporting research and knowledge exchange at higher education institutions in England.[150] Since October 2015, CREST has received nearly £12.5 million,[151] to bring together six partner universities across the UK to "deliver a world-class, interdisciplinary portfolio of activity that maximises the value of social science to countering threats to national security".[152] As a part of the most recent grant, seven PhD students will also be trained by CREST.[153] Projects are varied, with topics ranging from "Understanding & Countering Online Behaviour" to an evaluation of the efficacy of CVE.[154] Made clear in these grant reports are the close ties between CREST and academic partners, rather than the UK government. That CREST receives funding directly from the Home Office (and indirectly from the government via the ESRC) means, however, that connections with the UK government and its counter-terrorism policy cannot be denied.

139 https://www.gov.uk/government/organisations/conflict-stability-and-security-fund/about
140 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875951/CTPF_Enablers_Programme_Summary.odt
141 Ibid.
142 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
143 Ibid., p.9
144 Ibid., p.32
145 Ibid., p.33
146 Ibid., p.8
147 Ibid., p.80
148 https://www.lancaster.ac.uk/people-profiles/paul-j-taylor
149 https://crestresearch.ac.uk/about/
150 https://www.ukri.org/about-us/who-we-are/
151 https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview; https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
152 https://www.ukri.org/news/uk-hub-for-research-into-security-threats-awarded-5-3m-funding/; https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview
153 https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
154 https://crestresearch.ac.uk/projects/

The Home Office works closely with the National Cyber Security Centre (NCSC), the UK's independent authority on cyber security.[155] The NCSC is not tasked specifically with CVE, but it is part of GCHQ, the priorities of which are set in line with the National Security Council and the National Security Strategy,[156] where counter-terrorism plays a central role. The NCSC has been sponsoring PhD students to undertake cyber security-related research since 2012,[157] through 19 universities recognised as Academic Centres of Excellence in Cyber Security Research.[158] These universities are jointly recognised by the NCSC and the Engineering and Physical Sciences Research Council, an indirect stream of government funding. Just as France funds PhD students to carry out research into counter-terrorism, so does the UK, albeit less directly. While this link may appear slightly tenuous, it is a well-established funding stream for future academics that may also act as a direct path to employment at NCSC or GCHQ,[159] feeding into the UK counter-terrorism policy.

United Nations Counter-Terrorism Committee Executive Directorate

The UN Counter-Terrorism Committee Executive Directorate (UN CTED) was established by UN Security Council Resolution 1535 (2004) as an expert body in support of the Security Council's Counter-Terrorism Committee (CTC).[160] Its initial aim was to assess UN Member States' implementation of Security Council resolutions on counter-terrorism and support their efforts through dialogue.

In 2015, CTED launched its Global Counter-Terrorism Research Network (GRN). The GRN brings together more than 100 research institutions across the world, aiming to inform CTED of emerging terrorism trends and to identify and share good practices in the implementation of the relevant Security Council resolutions by Member States.[161] The value of the GRN was later recognised in a 2017 UN resolution (2395), alongside CTED's relationships with relevant experts in academia and think tanks.[162] While it is not clear whether research shared by the GRN is funded by CTED or another UN body, the GRN publishes regular reports online, including longer pieces of analysis, for example on the impact of the coronavirus pandemic on terrorism, counter-terrorism and CVE,[163] and shorter "Trends Alerts". These alerts are published to "to increase awareness, both within the CTC and among United Nations agencies and policymakers",[164] and include research from across the GRN.[165] Like the European Commission-funded research, the GRN has policy and impact at its core.

155 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
156 https://www.gchq.gov.uk/section/mission/overview
157 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
158 https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
159 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
160 N. Chowdhury Fink (2012) "Meeting the challenge: A guide to United Nations counterterrorism activities", International Peace Institute: p.45, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf
161 https://spark.adobe.com/page/hMGmYTiTbbEag/
162 https://www.un.org/sc/ctc/news/2021/01/05/virtual-roundtable-global-research-network-20-years-research-emerging-threats-trends-developments-terrorism-counter-terrorism/
163 https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf
164 https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf, p.2
165 Ibid.

The UN Development Programme, although not directly related to CTED, also released an action plan to address radicalisation and violent extremism in 2016, with two agendas, one of which is centred around "Research, Policy and Advocacy".[166] This research agenda "will be steered by the [UN] Oslo Governance Centre and conducted in collaboration with the regional hubs and in partnership with academic and research institutions".[167] The agenda also discusses the role of the RESOLVE research network, which is separate to the GRN, which aims to provide "an evidence base for Countering Violent Extremism programs and policies",[168] and organises an annual conference to share international CVE research. While no mention is made of the associated funding streams, as the agenda title suggests, research outputs are, again, expected to be policy-oriented.

United States

Under the Trump administration, the United States' CVE activities and budget were slashed. The Countering Violent Extremism Task Force, established in 2011 to unify efforts and activities across agencies during the Obama administration, was restructured in 2017,[169] and shuttered in late 2018.[170] Funding for activities engaging with communities and civil society, such as Life After Hate, an initiative that works with individuals to leave white supremacist and neo-Nazi groups,[171] was halted.

Despite these budget cuts, the level of CVE funding to law enforcement – particularly the Department of Homeland Security (DHS) – tripled, from $764,000 to $2,340,000.[172] The DHS's Science and Technology Directorate commissioned a number of research roadmaps to take stock of current CVE research and stakeholders, as well as make recommendations for future lines of research.[173] Federal government research into CVE focuses on "emerging social, psychological, economic, legal, political, and cultural issues" as well as "risk factors that lead to violent extremism to help partners create more effective and efficient CVE programs."[174]

Although some commentators claim that the Trump administration "could have been worse" in terms of its CVE policy, citing the expansion of DHS research funding as a positive development,[175] it is clear that these research programmes have targeted specific communities and bolstered policing and surveillance efforts within them. The Brennan Center for Justice, a public policy and law institute, analysed the Trump administration's CVE grants, and found that "at least 85% of CVE grants, and over half of CVE programs, now

166 https://www.undp.org/content/dam/norway/undp-ogc/documents/Discussion%20Paper%20-%20Preventing%20Violent%20Extremism%20by%20Promoting%20Inclusive%20%20Development.pdf, p.33
167 Ibid.
168 Ibid., p.34
169 J. Ainsley et al. (3 February 2017) "Exclusive: Trump to focus counter-extremism program solely on Islam – sources", *Reuters*, https://www.reuters.com/article/idUSKBN15G5VO?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social
170 P. Beinart (29 October 2018) "Trump Shut Programs to Counter Violent Extremism", *The Atlantic*, https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/
171 Life After Hate, "About Us", https://www.lifeafterhate.org/about-us-page
172 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
173 See: https://www.dhs.gov/science-and-technology/developing-local-capabilities and in particular https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf
174 https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf, p.11
175 https://www.brookings.edu/blog/order-from-chaos/2020/04/07/on-cve-the-trump-administration-could-have-been-worse/

explicitly target minority groups, including Muslims, LGBTQ Americans, Black Lives Matter activists, immigrants, and refugees."[176] Over half of the programmes target schools and students, some as young as five years old.[177] Many CVE grants were awarded to law enforcement agencies operating in non-white areas, such as "Minneapolis and its Somali enclaves; the Alameda County Sheriff's Office, which includes Oakland, California."[178]

The use of federal funding for this type of activity is insidious: under the cover of community outreach and research, law enforcement agencies are able to "gather intelligence, to identify possible targets for sting operations, or to identify possible informants for recruitment".[179] This is reminiscent of the controversial Prevent programme in the United Kingdom, which has encouraged surveillance of British Muslim communities.[180] These activities contribute to the racial profiling of certain communities, creating a climate of fear and policing freedom of expression and privacy.

The incoming Biden administration's strategy on CVE remains to be seen. Considering Biden's vice presidency during the Obama administration, it may be that his counter-terrorism strategy is informed by the militaristic approach abroad that Obama favoured.[181] If Biden is keen to disavow the racist policies expanded by Trump, abandoning the CVE grant programme would be a step in the right direction. Funding that has previously been used for harmful CVE research could be channelled instead into chronically neglected and under-funded communities to address basic needs.

Policy Relevancy, Research and the State: Ethical Considerations

In developing and executing CVE policy, there are three main groups of stakeholders: academia, policymakers/practitioners and the technology industry. Lydia Khalil's survey findings above focus on researcher engagement with the tech industry, finding a varied level of engagement with companies. This subsection examines researcher engagement with policymakers and practitioners of CVE, exploring some of the wider ethical challenges implicit within collaborations between academia and policymakers.

Prior to the bombings in London in July 2005, counter-terrorism strategy had focused on security threats from international terrorism, particularly groups such as al-Qaeda. Given that three of the four London bombers were born in Britain, the UK began to focus on "homegrown extremism" and domestic terrorism threats. The Prevent strategy, launched in 2003 by the UK Home Office, targeted individuals deemed to be "vulnerable" to radicalisation, intervening in the so-called radicalisation pathway before any criminal activity could take place.[182]

176 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
177 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
178 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/
179 Ibid.
180 See previous GNET report,"Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities" https://gnet-research.org/wp-content/uploads/2021/01/GNET-Report-Researching-Extremist-Content-Social-Media-Ethics.pdf, pp.32–7
181 https://www.cfr.org/election2020/candidate-tracker, section on counter-terrorism
182 Prevent Strategy HM Government, June 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

The strategy was particularly notable for its "whole-of-society" approach: civic institutions such as schools, registered childcare providers, universities, colleges, prisons, probation services, healthcare, social services and immigration enforcement were all implicated in the strategy. These institutions were obliged to anticipate, monitor and intervene in possible instances of radicalisation by identifying specific suggestive markers of radicalisation and reporting them. This approach dislocated counter-terrorism strategy and policing from traditional security and intelligence apparatuses and into community spaces and multiple state agencies. Spearheaded by the UK, the Prevent strategy approach has since been implemented in many Western states.[183]

This whole-of-society and multi-agency approach to counter-terrorism has come to be described by the term CVE. CVE encompasses a range of activities "on the ground" to intervene in the radicalisation pathway, informed and underpinned by ideological, psychological or cultural understandings of radicalisation.[184] Community engagement projects, such as education or mentoring programmes – often with youths or with particular communities – and programmes designed to bolster trust in and engagement with the police are typical of CVE strategy.[185]

The United States' Department of Homeland Security's Office for Targeted Violence and Terrorism Prevention (TVTP; formerly the Countering Violent Extremism Task Force) encapsulates the tenets of CVE strategy well. TVTP's activities are focused on "proactive measures" to prevent terrorism and acts of targeted violence that are focused on communities.[186] These measures are said to "empower communities and individuals" and build resilience to "violent messaging and recruitment". They include public awareness, community engagement and support services.[187]

Crucially, CVE strategy and prevention frameworks are centred around a threat assessment and management paradigm. According to TVTP, this means recruiting "educators, psychologists, faith leaders, medical personnel, law enforcement, and others" into the counter-terrorism effort in a whole-of-society approach.[188] This approach has been heavily criticised by human rights groups concerned with the ways in which this form of community surveillance and policing functions to entrench harmful assumptions about which communities and racial groups are "vulnerable" to radicalisation and violence, as well as creating a climate of fear and hostility within communities.[189] In prioritising threat assessment and management, CVE strategy is dependent upon being backed up by "hard" law enforcement and security apparatuses to criminalise particular behaviours.

183 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, footnote 18
184 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, p.3
185 Ibid., p.5 and https://www.tandfonline.com/doi/full/10.1080/18335330.2015.1028772?casa_token=4VBOXUOQT3UAAAAA%3ABeegdWY62rzDh376WJQuY3Ssw6Z99i4QiU6NZkRWzkypPQ4OQ5Q9PkBzslOXsdnrAVFp07xAQE4
186 See: https://www.dhs.gov/tvtp
187 Ibid.
188 https://www.dhs.gov/tvtp, section Local Prevention Framework
189 See, for example, Liberty: https://www.libertyhumanrights.org.uk/fundamental/prevent/

In the policy overview of jurisdictions above, we examined the role of federal funding in the US to operationalise this whole-of-society approach between law enforcement, policymakers and academia. We found that "at least 85% of CVE grants, and over half of CVE programs, now explicitly target minority groups, including Muslims, LGBTQ Americans, Black Lives Matter activists, immigrants, and refugees."[190] Over half of the programmes target schools and students, some as young as five years old.[191] Many CVE grants were awarded to law enforcement agencies operating in non-white areas, such as "Minneapolis and its Somali enclaves; the Alameda County Sheriff's Office, which includes Oakland, California."[192]

A particularly striking example of the collaboration between law enforcement, federal agencies and academic researchers is shown in a CVE grant awarded to the Seattle Police Department. The $409,389 award funded overtime for police officers to develop and execute "Micro Community Policing Plans" that bring "together community engagement, crime data and police services". These plans are targeted at Seattle's "African American, East African, Filipino, Korean, Latino, Muslim/Sikh Arab, Native American, and South East Asian communities", particularly refugee women and their families, five- to 18-year-olds and "disenfranchised populations".[193] The grant brings together Seattle law enforcement, with a rehabilitation centre, schools, city, faith and community-based organisations, as well as researchers from Seattle University. Researchers "will evaluate the program through community surveys that measure 'perceptions of police'" and other factors.

In partnering with a policing programme directly targeted at particular groups, the example above shows a dangerous side of researcher collaborations with CVE policymakers and practitioners. It raises thorny ethical questions relating to complicity with problematic state surveillance, repressive policing and the continuance of racial profiling, contributing to the overpolicing of racialised groups.

Richard Jackson, founding editor of *Critical Studies on Terrorism*, wrote that the "war on terror" launched after the 11 September 2001 attacks in the US has "killed and injured over a million people … caused incalculable suffering to millions more … and is one of the most effective tools of hegemonic domination by Western states in the present era." He goes onto argue that "the global counter-terrorism regime is, in its philosophy, practice, and effects, inherently violent, oppressive, and life-diminishing" and that "In such conditions … it can be argued that working directly with state counterterrorism is akin to medical professionals who collaborate with torturers in an effort to improve prisoner welfare."[194]

Research funded by or partnered with state agencies, such as the DHS-funded grant with Seattle Police Department and Seattle University above, is highly constrained in its scope. Writing from a perspective as a leading critical terrorism professor, Jackson

190 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
191 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
192 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/
193 https://www.dhs.gov/sites/default/files/publications/EMW-2016-CA-APP-00236%20Full%20Application.pdf
194 https://www.tandfonline.com/doi/pdf/10.1080/17539153.2016.1147771?needAccess=true, pp.121–2

contends that critical terrorism "scholars have warned and criticised and made alternative suggestions for years now, without any measurable effect; [they], by and large, have no voice in the current counterterrorism system." He goes on to argue that researchers called upon to consult and advise with the government are in reality "primarily … utilised by the state to legitimise already decided courses of action and to bolster its public reputation."[195] Since the scope of enquiry of academic partnerships with government is limited to the intellectual legitimisation of state practice, independent critical analysis of the counter-terrorism regime or specific practices within it is shifted further and further away from the centre of state power and decision-making.

In the survey findings above, it is noted that ethics approval processes and privacy considerations, such as compliance with General Data Protection Regulation (GDPR) legislation and with social media companies' terms of service, have been major obstacles in CVE research. These obstacles, which cause significant delays to research and available data, have, according to the survey findings analysis, "force[d] many researchers to rely on secondary data."

In such a research climate where primary source analyses are difficult to produce and can serve to legitimise harmful state counter-terrorism practices, how can CVE research be ethically policy relevant? First, CVE research could employ a different mode of enquiry at its core. Jackson contends that research seeking to be policy relevant in the orthodox way "pushes us towards asking particular kinds of questions and looking for particular kinds of questions. Primarily, it frames the research question in a 'problem-solving' mode," which drives research to conform with the way in which policymakers articulate the "problem" and define the range of solutions.[196] An ethical research agenda that de-emphasises the solutionist paradigm could instead investigate the impact of counter-terrorism and CVE on racialised and marginalised communities, and make policy recommendations to alter these policies based on the findings. This would help to work towards an understanding of policy relevance as research that not simply legitimises state policy, but that is relevant directly to the communities which it targets.

Secondly, research that sheds light on historical, structural and societal – rather than individual, ideological and racial – explanations for violence against citizens and the state would form another strand of an ethical CVE research agenda. In expanding the range of enquiry to take into account violence against communities traditionally understood as being "vulnerable to radicalisation", CVE research can advocate for policies that seek to redress historical and structural violence. For example, in understanding the detention and deportation regime as institutional harm against particular communities, CVE research can begin to advocate for the dismantling of such institutions and for the development of migration management policies.

195 Ibid., p.123
196 Ibid.

Lastly, and in developing a research agenda that centres and uplifts those impacted by counter-terrorism strategies, CVE research could advocate for a move away from a whole-of-society approach that encourages over-policing of these communities. In this way, CVE research could investigate the impact of policies that uplift communities – for instance, greater investment in housing, mental health support, healthcare and employment opportunities. In advocating for basic needs such as these and reducing police presence in communities, in conjunction with an understanding of structural violence, CVE research can push for a different kind of intervention in pathways to violence.

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.

© GNET