HM Prison & Probation Service

The Internet and radicalisation pathways: technological advances, relevance of mental health and role of attackers

Dr Jonathan Kenyon – HMPPS
Dr Jens Binder – Nottingham Trent University
Dr Christopher Baker-Beall – Bournemouth University

Ministry of Justice Analytical Series
2022

His Majesty's Prison and Probation Service is committed to evidence-based practice informed by high-quality social research and statistical analysis. We aim to contribute to the informed debate on effective practice with the people in our care in prisons, probation and youth custody.

Disclaimer

The views expressed are those of the authors and are not necessarily shared by the Ministry of Justice (nor do they represent Government policy).

First published 2022

Any enquiries regarding this publication should be sent to us at National.Research@noms.gsi.gov.uk

This publication is available for download at http://www.justice.gov.uk/publications/research-and-analysis/moj

ISBN 978 1 84099 988 4

The authors

Dr Jonathan Kenyon is a BPS Chartered and HCPC Registered Psychologist. He currently works as a National Specialist Lead within the HMPPS Counter Terrorism Assessment and Rehabilitation Centre (CT-ARC). His research interests include pathways to lone-actor terrorism and exploring the role of the Internet in radicalisation and extremist offending. Previous publications include Lone-actor terrorism – A systematic literature review (Kenyon et al., 2021a) and The Role of the Internet in Radicalisation and Offending of Convicted Extremists in England and Wales (Kenyon et al., 2021b).

Dr Jens Binder is Associate Professor of Psychology at Nottingham Trent University. His research focuses on cybersecurity and safety, social media engagement and user wellbeing as well as cognitive factors in online communication. He draws on perspectives from cyberpsychology, cognitive psychology and human-computer interaction and uses predominantly quantitative methods. His work has been published in high profile journals including American Psychologist, Computers in Human Behavior, New Media & Society and Journal of Personality and Social Psychology. He regularly supervises projects at PhD level and leads on a specialist Postgraduate degree in Cyberpsychology.

Dr Christopher Baker-Beall is Senior Lecturer in Crisis and Disaster Management at Bournemouth University. His research focuses on European Union security policy, the issue of ‘radicalisation’, and the merging of migration, border control and counter terrorism. His publications include The European Union’s Fight Against Terrorism: Discourse, Policies, Identity (Manchester University Press, 2016) and the edited collections Counter Radicalisation: Critical Perspectives (Routledge, 2015).

Contents

List of tables

List of figures

1. Executive Summary

Introduction and aims

This study explored the role of the Internet in radicalisation pathways of convicted extremist offenders in England and Wales, continuing the work previously reported in Kenyon et al. (2021b). Specific considerations included technological advances and changes in online activities, exploring the relevance of mental health including specific types of difficulties and disorders, and focusing on the sub-group of convicted extremist offenders identified as attackers.

Methodological approach and interpreting findings

The study built on an existing data set of 269 individuals from the study by Kenyon et al. (2021b) but expanded the numbers substantially by adding those with a completed initial Extremism Risk Guidance (ERG22+) report from January 2018 to December 2021. This resulted in a data set of 490 individuals who had been convicted of an extremist offence, equating to nearly all offenders who have been subject to either a Structured Risk Guidance (SRG) or initial ERG22+ report from October 2010 up to December 2021. The analysis focused on 437 individuals who were identified as 'Radicalised Extremists' following a review of all reports. Online behaviours commonly associated with radicalisation, demographic information and offence characteristics were coded for all cases. Professional ratings for overall levels of engagement, intent and capability to commit violent extremist acts were also included. Future offence data was obtained for all individuals by accessing up-to-date offending information and reviewing their current location. Statistical analyses were used to compare three radicalisation pathway groups: those who primarily radicalised online; those who primarily radicalised offline; and those subject to radicalising influences in both the online and offline domain.

Limitations that should be borne in mind when interpreting findings include the potential for lack of honesty from offenders, missing data as the purpose of reports is not to detail all online behaviours, that some individuals who have committed extremist offences may not be included, such as those who evaded arrest or were

killed in the commission of their offences, and the comparatively smaller number of non-Islamist extremists and females within the data set.

Key findings

The study identified ten key findings and six recommendations for counter-terrorism policy and practice moving forward.

First, when considering initial ERG22+ reports from 2018 to 2021 for convicted extremist offenders, the previously reported trend of the Internet playing an increasingly prominent role in radicalisation processes has continued, in line with online activity by society generally over the time period investigated. Radicalisation was found to now take place primarily online, as was evident for those sentenced in 2019–2021, although it remains at present uncertain to what extent this may be due to the onset of the COVID-19 pandemic and associated restrictions.

Second, the most marked increase in prominence of the Internet in radicalisation pathways over time was found for convicted women and the older generation. The Internet was also increasingly prominent over time in pathways for Islamist Extremists, those affiliated with the Extreme Right Wing and Other Political groups. Animal Rights activists were the exception, with in-person contact remaining a key feature of their radicalisation over time.

Third, the types of websites, platforms and applications used by convicted extremists had changed over time, with a steady decline in use of specific extremist websites/homepages and standard communication applications/platforms, and an increase in use of forums/chatrooms, open social media platforms and encrypted applications. Use of the dark web was reported infrequently, as were new developments such as online gaming and use of imageboards. No individuals reported they had livestreamed their attacks online.

Fourth, the internet-related behaviours found to differentiate those who primarily radicalised online from those who primarily radicalised offline were general online activities relating to extremism, namely learning from online sources, interacting with

others online, and use of open social media platforms. Those who primarily radicalised online could be differentiated from those radicalised via online and offline influences as they were more likely to generate their own extremist propaganda and use open social media platforms.

Fifth, pathway groups were markedly different in terms of their recorded demographic profile, offending history and socialisation. Those who primarily radicalised online were most likely to have committed a non-violent offence, most likely to have committed extremist offences solely online, least likely to be socially connected in the context of the offence and most likely to display signs of mental health issues, neurodivergence[1] or personality disorder/difficulties. Those reported as being primarily radicalised offline were most likely to be older and have a convicted offending history, including prior convictions for violence. Index offences were most likely to be violent, with individuals most likely to be part of a group of four or more people and least likely to follow an Islamist extremist ideology. Those reported as being radicalised via online and offline influences were most likely to have committed a previous Terrorism Act (TACT) or TACT-related[2] offence and most likely part of a small cell, consisting of two or three people.

Sixth, a third of the sample were reported as having mental health issues, neurodivergence or personality disorder/difficulties. Disorders most commonly reported across all three pathway groups were Autism Spectrum Condition (ASC), depression and personality disorder/difficulties. However, these were most common for those who primarily radicalised online.

Seventh, for attackers, reported online planned action behaviours differed between pathway groups. Those who primarily radicalised online or by online and offline means were more likely than those who primarily radicalised offline to engage in

---

1 The term 'neurodivergence' refers to divergence in mental or neurological function from what is considered typical or normal. This term is frequently used with reference to autistic spectrum condition, but also includes learning difficulties and disabilities, and other conditions such as attention deficit hyperactivity disorder etc.).

2 TACT-related offences include those that are more recently defined as TACT-connected offences following definitional changes applied from September 2020 to align with legislative changes since 2009. Definitions can be found within Appendix A.

attack preparation online. Those radicalised via online and offline means were more likely than those who primarily radicalised offline to identify targets online, and those who primarily radicalised online were more likely to signal attacking intent online than those who primarily radicalised offline.

Eighth, the recorded nature and success of plots by attackers differed between pathway groups. Whilst those who primarily radicalised online devised plots with the potential to cause serious harm, their plots were least likely to have progressed beyond the planning stage and most likely to have been foiled.

Ninth, differences were found in assessed levels of reported engagement, intent and capability, with those who primarily radicalised online considered the least identified with an extremist group or cause, and least willing and able to perpetrate violent extremist acts.

Tenth, in terms of future proven offending outcomes, based on the methodology used for this study, results indicated that 7 per cent of individuals were subsequently convicted for further TACT or TACT-related offences. The pathway group most likely to be convicted for further TACT offences were those reported as being radicalised by both online and offline influences.

Conclusions and recommendations

This study explored the role of the Internet in radicalisation pathways of convicted extremist offenders in England and Wales and findings need to be considered in light of the limitations set out earlier. To conclude, findings suggest that the Internet has become increasingly prominent in radicalisation pathways and offending over time for convicted extremists in England and Wales. Technological advances have led to changes in the types of applications/platforms used over time. Mental health issues, neurodivergence and personality disorder/difficulties were relevant for a sizable proportion of the sample, with ASC, depression and personality disorder/difficulties recorded as the most common types of disorders, particularly for those who have primarily radicalised online. For attackers specifically, those exposed to online influences in their radicalisation pathway were more likely to use the online domain

for attack planning behaviours, including target identification and signalling attacking intent. Those attackers reported as being primarily radicalised online were found to be the least successful in plotting attacks and most likely to see their plots foiled at the planning stage.

Based on the findings of this study, six recommendations are proposed relevant for both Ministry of Justice (MoJ) policy and practice in prison, along with wider counter-terrorism policy and practice:

1. Online responses should remain a key focus of counter-terrorism efforts, accounting for the heterogeneity of the audience
2. Research should investigate emerging platforms and applications, establishing how they are used and best ways to respond
3. Multi-platform responses are recommended to counter terrorism, with tech companies being transparent in their approach
4. Those vulnerable to online radicalisation may benefit from specialist input concerning ASC, depression and personality disorder, along with support during transitional periods[3] in their life
5. Offline activities of those identified as potential extremists should be closely monitored, acting upon concerns of potential attack planning at an early stage
6. Intervention developers should consider risk and protective factors across individuals and contexts, with consideration also given to diversionary solutions at point of sentencing, or potentially at point of arrest, for those active solely online and considered as having a peripheral role.

[3] Examples of transitional periods include relocation or change in cultural environment, losses or separation, changes to employment or work life, conflicts with others or traumatic events.

2. Context

The Internet has long been a source of concern regarding extremism, with the online domain becoming increasingly important for extremists around the world (Meleagrou-Hitchens & Kaderbhai, 2017). It has now been established that online communities play a key role in radicalisation processes towards extremist offending and that all mainstream social media and file-sharing platforms have been touched by extremist activism to some extent. The Internet is considered a primary operational environment in which ideologies are realised, attacks planned, and social movements made (Winter et al., 2020).

This study updated previous work reported by Kenyon et al. (2021b),[4] which involved analysis of a data set of 267 Extremism Risk Guidance (ERG22+)[5] reports and two Structured Risk Guidance (SRG) reports (the predecessor to the ERG22+) compiled on convicted extremists in England and Wales from October 2010 up to December 2017. Within the previous study, the role of the Internet in radicalisation and offending of convicted extremists were compared across three radicalisation pathway groups: those who primarily radicalised online; those who primarily radicalised offline; and those radicalised through both online and offline influences. Within this updated study, the same approach was taken by comparing the three pathway groups, but an additional 221 individuals have been incorporated, including all that have been subject to an initial ERG22+ report completed by His Majesty's Prison and Probation (HMPPS) staff from 2018 to 2021. This resulted in a greatly expanded data set from 269 to 490 individuals within the overall sample.

The inclusion of more recent initial ERG22+ reports from 2018 to 2021 provides an opportunity to establish whether trends identified in the previous study, on reports up to 2017, have continued or moved in new directions. In the previous study, the

[4] This study was published as a research report on gov.uk as part of the Ministry of Justice analytical series on 16th September 2021 (Exploring the role of the Internet in radicalisation and offending of convicted extremists (publishing.service.gov.uk).

[5] The ERG22+ is an assessment framework based on Structured Professional Judgement (SPJ) that helps inform overall decisions about risk and identify areas that can be targeted through intervention for those who have committed extremist offences (see Lloyd & Dean, 2015 for further information on the ERG22+).

Internet was found to have played an increasingly prominent role in radicalisation pathways over time of those subsequently convicted of extremist offences. This was true for both males and females, and across younger and older generations. Other key findings from the previous study included changes in the types of online applications/platforms used by extremist offenders over time, most notably a move away from specific extremist websites/homepages towards an increased use of open social media platforms. Differences were also found between the three radicalisation pathway groups in relation to their online activities, socio-demographics and offending histories. Particularly noteworthy was that those who primarily radicalised online were assessed by professionals as having the lowest levels of engagement to an extremist group or cause at the time of offending, and the lowest levels of intent and capability to commit extremist offences causing serious and significant harm.

In addition to revisiting and updating previous analyses, this current study provided a more in-depth investigation in a number of areas of interest. First, this study intended to use more recent reports to review the types of online activities being undertaken, as well as the applications/platforms being used currently by convicted extremists. The literature refers to the ever-changing online space, with extremists no different from members of the public in taking advantage of new technologies and the latest platforms on offer. Examples of this include accounts of extremists having livestreamed their attacks and the ‘gamification’ of violent extremism, with fears that online gaming and associated platforms are being used for the purposes of propaganda, radicalisation and recruitment (Lakhani, 2021). Gaming references and language in contemporary extremist milieus is also reported as commonplace (Schlegel, 2021). Others have called for greater attention to be given to use of the dark web by extremists, suggesting this space, due to a lack of monitoring and regulation, is used to radicalise, recruit and obtain illicit goods (Malik, 2018).

Other new online activity developments reported in the literature include use of anonymous imageboards (also known as chanboards) among extremists and concerns these online environments may act as echo chambers, contributing to radicalisation (Crawford et al., 2020). The use of imageboards and livestreaming by extremists were heavily publicised following the Christchurch mosque shooting by Brenton Tarrant in 2019 after he was found to have announced his violent intentions

on 8chan, before livestreaming the attack on Facebook to share his actions with a large audience and affect political outcomes (Macklin, 2019). Based on these reported developments of online activities within the literature, this study compared pathway groups in terms of reported use of the dark web, relevance of online gaming and associated platforms, use of imageboards, and whether livestreaming was a feature of attacks.

Second, this study considered profile and vulnerability factors of pathway group members to a greater depth than the previous study. The increased sample size enabled investigation into the relevance of the 22 individual factors comprising the ERG22+, organised across the three domains of engagement, intent and capability, as a way of determining pathway group membership. Engagement domain factors account for an individual's involvement and growing identification with an extremist group, cause or ideology, whilst intent domain factors evidence an individual's readiness to support and/or use illegal means, and/or violence to further the goals of an extremist group, cause or ideology. Capability factors are those that enable an individual to cause harm, offend or perpetrate violence on behalf of an extremist group, cause or ideology. Comparing pathway groups at the factor level offered insights into what characteristics make individuals vulnerable to becoming engaged in extremist groups or causes through online or offline influences, along with factors that fuel intent or support capability to commit violent extremist acts.

Related to profile and vulnerability factors is the focus on the role of mental health and neurodivergence in relation to terrorism within academic literature, but also by policymakers and the media. However, comparatively little research exists on the mental health needs of those convicted of extremist offences in the UK (Copeland & Marsden, 2020). Autism Spectrum Condition (ASC) in particular has attracted recent interest, with some studies reporting an overrepresentation of autistic people among extremist offenders, specifically lone actors, compared to the general population (Corner et al., 2016; O'Driscoll, 2018). In the media, recent reports have claimed a 'staggeringly high' proportion of people with autism on the UK Prevent scheme (Grierson, 2021). Due to this attention on the relevance of mental health and neurodivergence, this current study identified the most common types of mental health issues, neurodivergence and personality disorder/difficulties relevant to each

pathway group to offer insights into whether those with certain types of mental health issues or disorders are more likely to radicalise in online settings, offline settings or a combination of both.

Third, this study focused on those who assumed the role of an attacker within the context of their offending. Attackers are defined as those who have either committed an extremist attack themselves on another person or property, or where there is sufficient evidence based on their conviction (i.e., being convicted for 'engaging in conduct in preparation for committing acts of terrorism') that they would have done had they not been disrupted prior to such. This group often receive the most publicity (Chermak & Gruenewald, 2006), cause most concern to the public (Ritchie et al., 2019) and may also pose the greatest challenges to professionals in relation to rehabilitation efforts. When considering the relevance of radicalisation pathways to risk, a recent study of 439 jihadist-inspired attackers across eight Western countries found that those who radicalised mostly offline were more likely to complete their attacks than those who radicalised online (Hamid & Ariza, 2022).[6] Those who radicalised offline were also reported as being better at evading detection by security officials and more likely to complete a terrorist attack successfully. Similarly, Whittaker (2021)[7] in his study of 231 Islamic State terrorists in the U.S. reported that those who used the Internet were less successful in achieving their goal than those who stayed offline. To test whether such findings are relevant for convicted extremists in England and Wales, this study compared attackers across pathway groups in terms of online behaviours related to planned action, as well as the types of plots formulated, plot implementation and success, and reasons for plot failure.

Fourth, to supplement the analysis of risk assessments of offenders in terms of their engagement, intent and capability at time of offending, in this study, future offending outcome data were examined and compared across pathway groups to provide

[6] This sample was drawn from existing databases in the literature on terrorist attacks, with further attacks/plots identified through open-source research. For some cases this included access to court documents and interviews with police investigators, family members, friends, lawyers and other individuals.

[7] This sample was drawn from several existing databases/reports in the literature, with case files created through access to U.S. court documents, data from academic and grey literature, and from journalistic data via news search engines.

further insights as to whether differences exist between pathway groups in the likelihood of further offending (both TACT and TACT-related). Figures provided by MoJ in response to a parliamentary question on re-offending by TACT offenders in England and Wales showed a proven re-offending rate of 3 per cent of those subsequently convicted for a further terrorism-related offence between the period January 2013 and December 2019 (MoJ, 2020).

2.1 Research aims and questions

One of the key aims of this study was to provide an update to analyses conducted previously using a substantially expanded data set with more recent cases included. Previous analyses were revisited and updated with reference to the most recent initial ERG22+ reports completed from January 2018 up to December 2021. Another key aim was to provide more in-depth analysis, made possible in large parts by the enlarged sample size, within five areas of interest.

To achieve these aims, this study investigated whether:

1. The trends of Internet use among extremist offenders had continued or changed since 2017. This included a breakdown of sex, age and ideological affiliation.
2. The differences identified in Internet use by convicted extremists when radicalisation pathways were compared in the previous study still held and what new insights emerged when considering new technological advancements.
3. The differences identified in offender demographics and offence-type variables when radicalisation pathways were compared in the previous study still held and what new insights emerged, particularly when considering the most common offences committed, the 22 factors comprising the ERG22+, the mental health status of individuals and when focusing specifically on attackers.
4. The differences identified in professional assessments of overall levels of engagement to an extremist group or cause, along with overall levels of intent and capability to perpetrate violent extremist acts still held when using the expanded data set
5. Future offending outcomes differed between radicalisation pathway groups in terms of the likelihood of individuals committing further TACT or TACT-related offences.

3. Approach

3.1 Sample

The updated data source consisted of 488 ERG22+ reports and two SRG reports. As way of an introduction to the ERG22+, this assessment framework has been used throughout HMPPS in England and Wales since September 2011 to assess individuals convicted of extremist offences. The ERG22+ is regarded as a promising risk and need formulation framework for use with extremist offenders based on the construct validity and internal consistency of the measure (Powis et al., 2019a), and its inter-rater reliability (Powis et al., 2019b).

As with the previous study, only initial ERG22+ reports were included as they feature an assessment of all individuals in terms of each of the 22 factors and overall levels of engagement, intent and capability at the time of committing their offence. Report subjects were those convicted of primarily terrorist or terrorist-related offences in England and Wales, with a total sample of 490 individuals. The reports included all that were available to the MoJ that were completed from October 2010 to December 2021. Report authors were either Registered Psychologists or qualified Probation Officers who had undertaken a standardised two-day national training to learn how to conduct the assessment. Authors typically have access to a number of restricted information sources when completing reports, including direct interviews with the offender in the majority of cases. Within this sample, 81 per cent of report subjects had directly contributed to the completion of the report via interview. The average length of reports was 20 pages, the longest comprising 146 pages and the shortest four pages.

Consistent with the previous study, the analysis focused on those identified as 'Radicalised Extremists'[8] prior to coming into custody. Of the 490 individuals, this applied to 450 (92%), making up the vast majority of the data set. As with the original study and consistent with previous research (see Reinares et al., 2017), individuals

[8] 'Radicalised Extremists' are defined as those individuals considered to have entered prison already holding extremist views and who have engaged in extremist actions in the outside world (Silke, 2014). See section 3.2 Procedure for a full description of variables and how they were coded.

were categorised into one of three groups to reflect their radicalisation pathway based on Internet use (where this could be identified). This was possible as both the SRG and ERG22+ are formulation-guided assessments, where authors describe an individual's pathway to extremist offending, including when the development of extremist beliefs occurred. The three pathway groups included:

- Primarily radicalised online ('internet' group)
- Radicalised through a combination of online and offline influences ('hybrid' group)
- Primarily radicalised offline ('face-to-face' group)

The following analysis focuses on those 437 (97%) of the 450 'Radicalised Extremists' where the radicalisation pathway could clearly be identified based on the content of the report. As with the previous study, the radicalisation pathway was determined by reading each report in its entirety, paying particular attention to offence and background details for each case, along with the narrative account of the offending pathway. The basic demographics for individuals included within the analysis are detailed in Table 1.

Table 1. Basic demographics for the 437 individuals included in the analysis

Demographic		Percentage (%)
Sex	Male	89
	Female	11
Age (at time of sentencing)	Mean age = 29 years old, Range = 15 – 63 years old	-
	Up to and including 25	44
	Over 25	56
Place of birth[a]	UK	70
	Non-UK	30
Ideology/cause	Animal Rights	4
	Extreme Right Wing	18
	Islamist Extremist	72
	Other Political	6

[a] Based on 424 individuals as place of birth could not be identified in 13 cases

3.2 Procedure

The same procedure was followed as in the previous study. The lead researcher manually reviewed initial ERG22+ reports for an additional 221 individuals and added these to the existing data set.[9] After examining each new report, variables of interest were extracted for each case relating to online activities associated with online radicalisation, demographic information and a number of offence-type variables. Furthermore, individual factor ratings from the ERG22+ assessment were extracted, as were the professional ratings of overall levels of engagement, intent and capability relevant to the time of offending (for a full description of variables and how they were coded, see Appendix B). Future offence data was obtained for all individuals by accessing up-to-date offending information and reviewing their current location (e.g., in prison or in the community). The coding frame from the previous study was updated to include a number of new variables to reflect technological advancements online and reported changes in the way extremist offenders are using the Internet according to the literature.

Once the lead researcher had applied the coding frame to all new initial ERG22+ reports, two other coders[10] independently coded all variables of interest for a selection of test cases to ensure clarity and ease of use of the updated coding frame. Any differences in coding between the three coders were resolved collaboratively through discussion and reaching a consensus. The aim of these discussions was to further refine the coding frame in order to strengthen variable definitions and examples. The modified instrument was then used by the lead researcher to finalise codings.

3.3 Analysis

As with the previous study, a quantitative research design was used involving analysis of coded information within the data set. As the previous study only featured reports completed up to December 2017, the prominence of the three pathway

[9] This updated study received approval from the National Research Committee (NRC) as the data related to convicted offenders in England and Wales.

[10] These additional coders were university-based researchers with domain expertise and familiarity with the coding technique.

groups over time was compared for the full time period, to consider established trends and novel developments. This included consideration of the prominence of internet use in radicalisation pathways of males, females, younger and older individuals, and those affiliated with various ideological groups. Subsequent analyses were clustered to compare pathway groups in terms of their online activities, demographic and offence-type variables, individual factors within the ERG22+, plot-related factors relevant to those identified as attackers, and overall engagement, intent and capability ratings at the time of offending, provided by professionals.

The data-analytical approach in this study was similar to that applied in the previous study, with the main differences concerning additional sub-group analyses of attackers and being able to separate the internet group from the hybrid group when predicting pathway group membership due to greater number of cases overall. Relative frequencies and percentages of all variables of interest were compared for each radicalisation pathway group. Where possible, Pearson's chi-squared tests were conducted to test for statistically significant relationships between pathway groups and variables of interest, with Fisher's exact test used as an alternative where the statistical assumptions for chi-squared tests were not met. Multinomial logistic regression analysis was used to test whether coded internet behaviour variables could predict pathway group classification, and to what extent. The same analysis was employed to test whether any of the 22 factors within the ERG22+ could predict pathway group membership. The Kruskal-Wallis test was used to determine whether statistically significant differences existed between pathway groups when comparing overall ratings of engagement, intent and capability at time of offending from the ERG22+ assessments.

3.4 Limitations

General limitations to the study approach have been identified previously and should be taken into account for the present work, namely that some internet activities may have been missed given the purpose of SRG and ERG22+ reports is not to detail all online behaviours. In addition, some individuals who have committed extremist offences in England and Wales would not be included in the sample, such as those killed in the commission of offences or those who avoided arrest. Other limitations

include the difficulties distinguishing between missing data and variables that could reliably be coded as not present, the varied length and level of detail of reports in the sample, potential lack of honesty from offenders, the subjectivity of interpretations placed by authors on information provided and the smaller number of non-Islamist extremist offenders in the sample. There were also comparatively fewer females (48 individuals, equating to 11% of the sample), so caution is necessary when interpreting comparisons based on sex.

The data set used in this study covers approximately 20 years of internet use.[11] It is recognised that online technology and the services and applications available have changed and evolved during this time. Whilst the analyses capture offenders' use of the technology, they do not directly account for the technological changes and developments that have occurred over time. There is also a growing awareness of internet-related challenges surrounding radicalisation, which means that more attention is being paid to these issues in more recent initial ERG22+ reports. As the present work is an extension of the previous study reported in Kenyon et al. (2021b), caution is required when comparing findings due to the overlap between the two data sets.

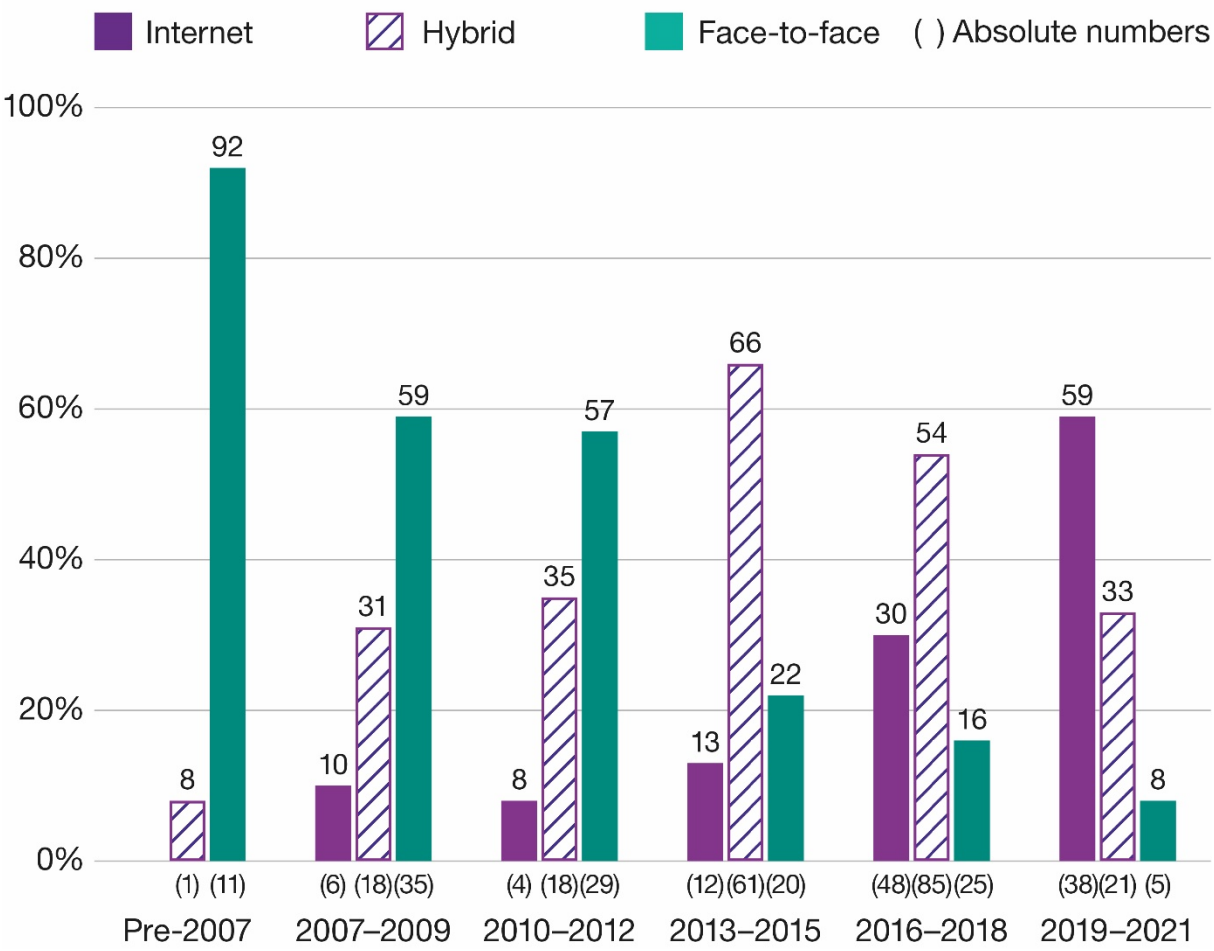
[11] 99 per cent of individuals within the sample had sentencing dates between 2000 and 2021.

4. Results

4.1 Prominence of the Internet in radicalisation over time

As expected, the Internet has continued to increase in prominence in the radicalisation of convicted extremists in England and Wales based on the most recent reports. From the period before 2007 up to 2021, there was an increase in the proportion of individuals subject to some degree of online radicalisation, including those who primarily radicalised online and those radicalised via online and offline influences (92% in 2019–21, 84% in 2016–18, 79% in 2013–15, 43% in 2010–12, 41% in 2007–09 and 8% in pre-2007, see Figure 1). As reported in the previous study, this trend reflects the increase in general online activity within society, with internet use now ubiquitous and multi-faceted. To support this assertion, self-reported internet use among adults has increased from 12.1 hours per week in 2007 to over 28 hours per week by April 2020 (Ofcom, 2020).

Figure 1. Percentages and frequencies of individuals showing the primary method of radicalisation for 'Radicalised Extremists' over time



NB: Values are percentages, with values in parentheses referring to absolute numbers.

Researchers have previously argued that the distinction between online and offline radicalisation is a "false dichotomy" and "plotters regularly engage in activities in both domains" (Gill et al., 2015, p. 35; see also Whittaker, 2021). Contrary to this argument, our data show that radicalisation primarily through online means is most common for those sentenced in 2019–21. Whilst the hybrid pathway, via online and offline influences, was most prominent for those sentenced in 2013–15 and 2016–18, this no longer appears to be the dominant pathway in 2019–21. As way of an explanation, the early months of 2020 coincided with the onset of the COVID-19 pandemic and lockdown restrictions, which is reported to have further exacerbated the time that people were spending online (see the synthesis of evidence on use of digital technology in the context of COVID-19 pandemic by Pandya & Lodha, 2021). It is possible that the dominance of the internet group during 2019–2021 may at least

in part be explained by the on-set of the pandemic, although the available case numbers are inconclusive.[12]

Consistent with the previous study, the Internet was found to have played an increasingly prominent role in radicalisation for both males and females, along with younger and older individuals. The Internet was also increasingly prominent in radicalisation for Islamist Extremists and those in both the Extreme Right Wing and Other Political sub-groups, but not Animal Rights activists (see Appendix C for sex, age and ideology sub-group analysis).

4.2 Changes in applications/platforms used over time

The three pathway groups were compared on their use of applications/platforms over time. The types of platforms and means of communication investigated included use of specific extremist websites/homepages, standard communication applications/platforms, forums/chatrooms, open social media platforms and encrypted applications. Consistent with findings of the previous study, the expanded data set showed that the types of applications/platforms used has changed markedly over time, from 2007 to 2021.

A more detailed analysis of trends in use of applications/platforms over time is provided in Appendix D, with a comparison across pathway groups and reference to the specific applications and platforms reported. To summarise, a reduction in use of specific extremist websites/homepages and use of standard communication applications/platforms was found for all three pathway groups over time. Over the same period, increased use of forums/chatrooms, open social media platforms and encrypted applications was evident for all three pathway groups. For those sentenced between 2019 and 2021, 67 per cent of forum/chatroom users were supporting an Extreme Right Wing ideology, with the more popular forums reported including ‘Iron March’ and ‘Fascist Forge’. The use of ‘Discord’ was also noteworthy as this was an application originally designed for gamers, where chat communities

[12] Of the 64 cases sentenced between 2019–21, 22 (34%) were sentenced from March 2020, coinciding with the first national lockdown. If allowing six months for arrest, investigations and court case following the commencement of the first national lockdown, 11 (17%) cases were sentenced from October 2020 onwards.

are organised into ‘servers’, each containing numerous text and voice channels. Very few cases were reported to have used the dark web specifically, and use of online computer games for extremist purposes featured most commonly for those who primarily radicalised online or had radicalised through both online and offline influences. Use of chanboards was reported in very low numbers, and no cases were reported as having live-streamed attacks online.

4.3 Differences in online activity depending on radicalisation pathway

Statistically significant associations were found when predicting pathway group membership from eight variables assessing online activities: learning from online sources, interaction with co-ideologues online, generating own extremist propaganda, use of extremist websites/home pages, use of forums/chatrooms, use of open social media platforms, use of standard communication applications/platforms, and use of encrypted chat applications.

Using the internet group as a reference category for both the hybrid and the face-to-face groups showed distinct patterns of association, over and above the results from the first study (see Table 2 in Appendix E). When comparing the face-to-face group with the internet group, three statistically significant predictors were found, namely learning from online sources, interacting with co-ideologues online, and use of open social media platforms. When learning from online sources was present, the odds of belonging to the face-to-face group were reduced by 99.7 per cent in favour of belonging to the Internet group.[13] Similarly, interacting with co-ideologues online reduced the odds by 94 per cent, and the use of open social media platforms reduced the odds by 90 per cent. It should be noted that these estimates come with considerable variability given the large confidence intervals obtained for odds ratios.

Comparing the hybrid group to the internet group showed two predictors to be statistically significant: generating own extremist propaganda online and use of open

[13] Whilst it would be expected that individuals within the face-to-face group would engage in lower levels of online activity within their radicalisation pathway, learning from online sources would also cover knowledge acquired via the Internet to support attack planning.

social media platforms. For individuals who had generated their own extremist propaganda online, the odds of belonging to the hybrid group were reduced by 45 per cent in favour of belonging to the internet group. When use of open social media platforms was present, the odds of belonging to the hybrid group were reduced by 60 per cent in favour of belonging to the internet group.

4.4 Profile and vulnerability factors depending on radicalisation pathway

As with the first study, extremist offenders within each radicalisation pathway group were found to be markedly different in demographic profile, offending history and socialisation, a pattern supplemented by additional variables in the present analysis. Statistically significant associations were found between several profile and vulnerability factors and primary method of radicalisation (see Table 3 in Appendix F). For some demographic and offence-type variables, the percentages show a general similarity between those who primarily radicalised online and those radicalised through both online and offline influences. Both these groups contrast to the group that primarily radicalised offline. Post hoc tests allow for some detailed characterisation as follows.

Five characteristics set apart those who primarily radicalised online from the other two pathway groups. These included whether the index offence was violent or non-violent, the role taken within the context of offending, whether the index offence was committed fully online, the degree of social connection to other co-ideologues offline and presence of mental health issues, neurodivergence or personality disorder/difficulties. Those who primarily radicalised online were more likely to have committed a non-violent index offence (84%) and by virtue were less likely to have held the role of attacker (16%). Members of this pathway group were also most likely to have committed their index offence solely within the online domain (57%). Those who primarily radicalised online were most likely to be classed as lone (85%) and least likely to have wider connections within a group (5%) compared to the other two pathway groups. Those who primarily radicalised online were also more likely to show a strong presence of mental health issues, neurodivergence or personality disorder/difficulties (42%) compared to the other two pathway groups.

Individuals who primarily radicalised offline were more likely than the other two pathway groups to be older and were more likely to have a convicted offending history, including violent offending. Those in this pathway group were most likely to have been convicted of a violent index offence and assumed the role of an attacker, and least likely to have committed an online-only index offence, compared to the other pathway groups. Those who primarily radicalised offline were also least likely to follow an Islamist extremist ideology and were most likely to have been part of a group of other extremists offline.

Those radicalised by both online and offline influences were most likely to have committed either a TACT offence or TACT-related offence prior to the index offence when compared with the other pathway groups. Individuals within this pathway group were also the most likely to have been members of a small cell, comprising two or three people. No significant differences were found between pathway groups in relation to sex, country of birth and whether members were reported as having a brain or head injury.

Further analysis identified which offence types were most common for those within each pathway group (see Table 4 in Appendix G). For those who primarily radicalised online, the most common offences were dissemination of terrorist materials/distributing materials to stir up racial hatred/encouraging and/or inciting acts of terrorism (42 individuals), engaging in conduct in preparation for terrorist acts (31 individuals) and possession of terrorist materials (18 individuals). For those primarily radicalised offline, the most common offences included arson/making explosives/conspiracy to cause explosion (22 individuals), murder/conspiracy to murder/attempted murder/soliciting to murder/manslaughter (21 individuals) and robbery/GBH/ABH/violent disorder (17 individuals). For those radicalised by online and offline means, the most common offences included engaging in conduct in preparation for terrorist acts (88 individuals), dissemination of materials/distributing materials to stir up racial hatred/encouraging and/or inciting acts of terrorism (39 individuals) and possession of terrorist materials (18 individuals).

4.4.1 ERG22+ factors and pathway membership

To investigate which individual factors from the ERG22+ were most closely associated with pathway membership, a stepwise multinomial logistic regression was carried out predicting radicalisation pathway from all 22 factors. This was based on 363 individuals where all factors had been assigned a rating by the report author. A forward stepwise procedure was chosen in the interest of parsimony since it was expected that only a sub-group of all 22 factors would be diagnostic of pathways. The resulting model retained eight factors. A full prediction model run for comparison reasons did not show any additional significant factors and was only marginally better at explaining pathway membership (Nagelkerke's R^2 = .47 for the full model and .41 for the condensed model; Chi square difference = 18.85, df = 28, ns), with both models explaining just under half of the variability in pathway membership. The eight factors retained comprised of five related to engagement (susceptibility to indoctrination, family and/or friends supporting extremism, transitional periods, group influence and control, and mental health issues), one related to intent (harmful end objectives) and two for capability (access to network, funding and equipment, and criminal history).

Full analysis and the regression outputs are provided in Table 5 in Appendix H. In sum, mental health issues and transitional periods increased the likelihood of falling into the internet group whereas access to networks, funding and equipment decreased the likelihood, compared to both the face-to-face and hybrid group. Group influence and control, susceptibility to indoctrination and criminal history allowed for an additional differentiation between the face-to-face and internet groups whereas family and/or friend support and harmful objectives served to differentiate the hybrid and internet group.

4.4.2 Mental health issues, neurodivergence or personality disorder/difficulties relevant to radicalisation pathways

For the 437 'Radicalised Extremists' where the radicalisation pathway could be identified, 143 (33%) were reported as having mental health issues, neurodivergence or personality disorder/difficulties. In comparison, it is estimated that 1 in 6 adults in England have a common mental disorder, and 1 in 8 people aged 16 or over screened positive for any type of personality disorder (McManus et al., 2016). Having

established that those who primarily radicalised online were most likely to show the presence of mental health issues, neurodivergence or personality disorder/difficulties compared with the other pathway groups (see Table 3 in Appendix F), a more detailed analysis of the type or mental health issue or disorder relevant for each pathway group was conducted.

For those who primarily radicalised online, the three most common types of mental health issue or disorder included diagnoses or assessments of ASC and associated traits, depression and personality disorder/difficulties (see Figure 2 in Appendix I). This was also found for those who primarily radicalised offline and those who radicalised via both online and offline influences, but frequency counts for these pathway groups were smaller.

4.4.3 Comparing attackers across radicalisation pathway groups

For the 437 'Radicalised Extremists' in the data set where the radicalisation pathway could be established, 137 (31%) were reported to have assumed the role of an attacker in the context of their offending and committed either a TACT or TACT-related index offence. In terms of demographics of this group, the majority were male (90%), over 25 (55%), and where place of birth could be identified, 73 per cent were born in the UK. In relation to ideology, 64 per cent were Islamist Extremist, 19 per cent were Extreme Right Wing, 10 per cent were Other Political and 7 per cent were Animal Rights activists.[14]

Having previously established that those who primarily radicalised online were significantly less likely to be an attacker than members of other pathway groups, and those radicalised primarily offline were significantly more likely to be an attacker (see Table 3 in Appendix F), it was investigated whether differences existed in online planned action behaviours by attackers across pathway groups. For undertaking attack preparation online, significant differences were found across pathway groups ($\chi^2 = 17.34$, $p < 0.01$). Attackers who primarily radicalised online and those

[14] It should be noted that for all Islamist Extremists and all Extreme Right Wing individuals, attackers made up 28% and 34% of these sub-groups respectively. For those in the Other Political group and Animal Rights activists, attackers made up 53% and 48% of these sub-groups respectively.

radicalised through online and offline influences were significantly more likely to engage in online attack preparation than those who primarily radicalised offline (as established by Bonferroni-corrected post-hoc tests). For online target identification, significant differences were found between pathway groups ($\chi^2 = 7.34$, $p < 0.05$), with those radicalised via online and offline influences significantly more likely to identify targets online than those who primarily radicalised offline. For signalling intent to attack online, significant differences were found between pathway groups ($\chi^2 = 14.67$, $p < 0.01$), with those who primarily radicalised online significantly more likely to signal their intent online than those who primarily radicalised offline.

The three pathway groups were then compared on the types of plots that attackers engaged in, the progress and success of these plots, and when plots were disrupted, how this occurred (see Table 6 in Appendix J). For those who primarily radicalised online, the most common types of plots included use of an Improvised Explosive Device (IED, 65%), a bladed weapon (24%) or a vehicle (12%). Only the minority of plots moved from planning to the execution stage (29%), with 18 per cent of plots successfully completed. For this pathway group, all thwarted plots were disrupted by the Police/security services (100%), suggesting that the online traces of those who primarily radicalised online make it more difficult for them to progress substantially in their attacks and bring them to the attention of the Police/security services more readily. This interpretation is also supported by the finding that attackers who primarily radicalised online were most likely to signal their attacking intent compared to the other pathway groups. These findings also counter the popular notion that the Internet helps create an undetectable threat of lone actors.

In contrast, those who primarily radicalised offline were most commonly involved in plots that either involved an IED (49%), unarmed assault (15%) or vandalism/criminal damage (13%). The majority of plots progressed to the execution stage (66%) with most successfully completed (58%). This adds some credence to the suggestion that members of extremist groups are more camouflaged from detection by authorities when primarily involved in offline extremist activity. It is also possible that the lack of online attack planning behaviours by this pathway group may have assisted members in avoiding detection. Of the thwarted plots, the majority were disrupted by the Police/security services (87%), but other reasons included the IED failing to

detonate (9%) and the attacker losing their nerve (4%). For those radicalised via online and offline influences, most plots involved either an IED (60%), a bladed weapon (31%), a firearm (8%) or vehicle (8%). When compared to those who primarily radicalised online, more plots escalated to the execution stage (39%) and were successfully completed (22%), but less on both counts when compared with attackers who primarily radicalised offline. The Police/security services were responsible for most thwarted plots for this pathway group (84%), but other reasons included the IED failing to detonate (4%) and missing the intended target (12%).

4.5 Differences in engagement, intent and capability to act depending on radicalisation pathway

The three radicalisation pathway groups were found to differ in terms of overall ratings by professionals in relation to levels of engagement with an extremist group, cause or ideology, levels of intent and levels of capability to commit violent extremist offences from the ERG22+ at the time of offending (see Figures 3 and 4 in Appendix K).

The engagement domain refers to factors that may account for an individual's involvement and growing identification with an extremist group, cause or ideology. As was the case in the first study, based on 29 individuals in the internet group, it was found that those who primarily radicalised online have the lowest overall engagement levels, this time based on 108 individuals (of which 91 had an overall engagement rating reported). This suggests that these individuals are generally less involved or identified than those on other radicalisation pathways. Consistent with findings from the first study, the expanded data set showed that those radicalised by a both online and offline influences had the highest overall engagement levels, highlighting the important role of offline contacts in strengthening involvement and deepening a sense of identity with an extremist group, cause or ideology.

The intent domain refers to factors evidencing an individual's readiness to support and/or use illegal means, and/or violence to further the goals of an extremist group, cause or ideology. Consistent with the first study, the expanded data set showed that those who primarily radicalised online had the lowest overall levels of intent, whilst those radicalised by online and offline influences had the highest overall levels of

intent. Therefore, not only do offline contacts play an important role in strengthening involvement and deepening a sense of an extremist identity, they also appear to play an important role in making individuals more willing or prepared to offend on behalf of an extremist group, cause or ideology. This combination effect of exposure to online and offline influences may further reinforce views and beliefs, eventually leading to a hardening of resolve to act.

The capability domain refers to factors that enable an individual to cause harm, offend or perpetrate violence on behalf of an extremist group or cause. Assessors are instructed to consider an individual's capability to commit offences that may cause serious and significant harm. Consistent with findings from the first study, the expanded data set showed that those who primarily radicalised online had the lowest overall levels of capability. Those who primarily radicalised offline had the highest overall capability levels, highlighting the value of offline contacts in providing individuals with the knowledge, skills and networks to take violent action in support of a group or cause.

4.5.1 Future offending outcomes for members of radicalisation pathway groups

Whilst acknowledging that many factors impact on future offending outcomes, the pathway groups were compared on whether individuals subsequently re-offended in custody or the community leading to a new conviction or their death whilst committing the offence. Unlike more typical approaches to recidivism studies, such as MoJ official reoffending statistics, where specific time periods are reviewed for evidence of some form of criminal justice sanction, such as a conviction or caution (MoJ, 2022), these future offending outcomes are caveated by unequal length of 'at risk' time as individuals were sentenced and released on licence into the community at different points in time. The sample also included cases where re-offending outside prison could not have occurred as they were still serving their original sentences at time of analysis. For these reasons, a more rigorous statistical consideration of time span was not possible and results must be viewed as indicative.

In total, 31 (7%) individuals from the sample of 'Radicalised Extremists' were subsequently convicted for further TACT or TACT-related offences. When comparing

pathway groups based on 351 individuals having excluded re-offending for non-TACT offences or licence breaches not resulting in conviction, those radicalised by online and offline influences were significantly more likely (p = 0.03 Fisher's Exact Test) to have committed a further TACT offence (10%) than those radicalised primarily offline (2%). As a comparison, 3 per cent of those primarily radicalised online committed a further TACT offence. This supports professional assessments that those in the hybrid group are typically most engaged with an extremist group or cause, with highest levels of intent to commit terrorist acts, and may be more resistant to rehabilitation efforts given higher recidivism rates for TACT offences. No significant differences were found between pathway groups in terms of likelihood of committing TACT-related offences.

5. Implications/Conclusions

5.1 Conclusions drawn from study findings

This study found that use of the Internet has continued increasing in prominence in the radicalisation of convicted extremists in England and Wales when considering those sentenced from 2018 to 2021. Although this is unsurprising given the ubiquity of Internet use across society, what is interesting is that radicalisation for convicted extremists is now taking place primarily within the online domain, as was evident for those sentenced in 2019–2021. This contradicts some of the more recent assertions in the literature that a distinction between online and offline radicalisation is a "false dichotomy" and "plotters regularly engage in activities in both domains" (Gill et al., 2015, p. 35; see also Whittaker, 2021). This change in direction may in part be accounted for by the restrictions on movement during the COVID-19 pandemic, which resulted in increased time spent online and reduced opportunities for in-person contact with others.

Sub-group analyses demonstrated that the most marked increase in prominence of the Internet in radicalisation pathways was for convicted females, and for the older generation, who in the past may have been more likely to associate with other extremists offline than their younger counterparts. When separating individuals by ideological affiliation, the increasingly prominent role of the Internet was most marked for Islamist extremists, but this pattern was also observed for the Extreme Right Wing and Other Political sub-groups.

It was apparent that a number of changes had occurred over time in the types of platforms and applications used by convicted extremists. As was found with the previous study, the use of specific extremist websites/homepages had fallen over time for all pathway groups. It may be that the availability of such sites has reduced given their comparative visibility to security services. The same was found for use of standard communication applications/platforms. This suggests that extremists now favour more secure forms of communication to avoid detection and communicate with one another more securely. As major open social media platforms become increasingly inhospitable to extremist groups through their disruption efforts,

extremists are likely to access lesser-known platforms and applications such as specialised chatrooms for some of their activities.

As was found within the previous study, the use of open social media platforms has continued to grow over time, despite increased disruption efforts on such platforms. The highest percentage of open social media platform use within both the internet and face-to-face pathway groups was found by individuals sentenced in 2019–21. The literature suggests that due to account suspensions and faster removal of extremist content, the ways in which such platforms are used has changed over time. Examples include posting links on such sites to re-direct followers to file-sharing sites where extremist content can be found (Macdonald et al., 2019), or to platforms offering greater levels of user privacy (Clifford & Powell, 2019). There are also reports of open social media platforms being used as a way of approaching sympathisers, who are then invited to more secure recesses of the Internet for further interaction and indoctrination (Berger, 2015). In this study, an increase in encrypted application use, particularly Telegram, was found from 2013–15 onwards by those who primarily radicalised online and through both online and offline influences. It has been suggested that encrypted platforms are not used for mass recruitment given their privacy and inaccessibility, but instead are often used for attack planning purposes, providing a virtual meeting ground where communications may encourage recruits to carry out attacks, often with minimal training or experience (Malik, 2018). There is some suggestion that the November 2019 takedown of Daesh channels and pro-Daesh accounts on Telegram co-ordinated by EU Member States and Europol may have resulted in messaging and supporter networks becoming dispersed across multiple smaller online platforms (EUROPOL Policy Brief, 2020), however this was not reflected in the findings of this study.

In terms of new technological advancements referenced in the literature, online gaming was reported as relevant for 7 per cent of all individuals, largely accounted for by those who had primarily radicalised online and those radicalised by both online and offline influences. First-person shooter games or those featuring a war theme were typically those that were reported. Other developments, such as use of the dark web and use of imageboards were only reported as relevant for a very small number of individuals, and none were found to have attempted to livestream an attack.

In terms of offence characteristics, those who primarily radicalised online were more likely to have committed a non-violent index offence and most likely to have committed extremist offences solely online. This was supported by finding that the most common offence for this pathway group involved either disseminating terrorist materials or encouraging/inciting others to commit terrorist acts. In relation to social connectedness, those who primarily radicalised online were most likely to be classed as lone and least likely to have wider connections within a group compared to the other pathway groups. When exploring the relevance of individual factors of the ERG22+ for pathway groups, it was found that those who primarily radicalised online were more likely to suffer from severe mental health issues, neurodivergence or personality disorder/difficulties. It was also apparent that this pathway group was more likely to experience periods of transition in their lives that contributed to trajectories towards extremist offending. When compared to those where internet use was not considered relevant to their pathway, those who primarily radicalised online are found to be generally more susceptible to influence and persuasion.

Having explored the prevalence of specific mental health issues and disorders, the three most common types across all three pathway groups were ASC (and associated traits), depression and personality disorder/difficulties. Rates for all three disorders were highest for those who primarily radicalised online. For individuals with ASC, the online domain is considered particularly attractive as written communication is free from the social and sensory demands of the offline world (Al-Attar, 2020). Online, content is typically visual and spelt out, which speaks to the strengths of those with ASC. Individuals with ASC are also provided with opportunities to curate their extremist identity online, incorporating their specific interests, and as a consequence they can find it easier to connect with others and establish a sense of kinship and community connection. Those with ASC may also be more able to assume leadership or influencer roles within extremist groups online, where such roles may be more difficult to hold in offline settings as, according to Al-Attar (2020), the domains demand different skills. When considering depression, links with vulnerability to radicalisation have previously been reported in the literature (Bhui et al., 2014). As depression has been linked to social adversity and marginalisation, this may explain why depression rates were highest for those who primarily radicalised online given this group were less socially connected to other extremists offline than

members of other pathway groups. In terms of personality disorder/difficulties, the literature provides mixed evidence of relevance, although narcissistic, paranoid, antisocial and sadomasochistic traits have previously been associated with terrorists (Lloyd & Kleinot, 2017; Weatherston & Moran, 2003), as have dependent, avoidant and emotionally unstable traits for suicide bombers specifically (Merari et al., 2009).

Those who primarily radicalised online were least likely to take on the role of an attacker. Whilst plots were devised with the potential to cause serious harm, including the use of IEDs, knives or vehicles, their plots were least likely to have progressed beyond the planning stage and were also the least successful. These findings provide support for the study by Hamid and Ariza (2022) focusing on attackers across eight Western countries, in which those radicalised offline were found to be three times more likely than those who radicalised online to complete an attack successfully and were 18 times more lethal. It is suggested that for attackers who primarily radicalised online in this study, their online activities likely brought them to the attention of the Police/security services at an earlier stage. Establishing that this pathway group were the most likely to signal their attacking intent online supports the argument that this group provide more opportunities for detection. It also suggests that those hardest to detect and often have the most success are those who tend to limit their extremist activity to the offline domain.

As with the previous study, those who primarily radicalised online were typically less engaged with an extremist group or cause, with lower levels of intent and capability to commit offences likely to cause serious or significant harm. Coupled with the findings that this group were most likely to have committed a non-violent index offence, least likely to take on the role of attacker, most likely to have committed extremist offences solely online, and with comparatively low levels of recidivism for TACT offending, it can be assumed that those who primarily radicalise online present a lower level of risk overall. Even for the few individuals who primarily radicalised online and assumed the role of an attacker in this study, only 18 per cent of plots were successfully completed and their willingness to signal their intent online may have resulted in the majority of plots being disrupted by the Police/security services. When considering that from 2019, the most prominent radicalisation pathway for convicted extremists was found to be primarily online, this may provide evidence that

the overall threat of serious and significant harm from terrorist offending in England and Wales is starting to diminish.

Those who radicalised through both online and offline influences were assessed as being the most engaged and presented with the highest levels of intent at the time of offending. The additional indicative analysis provided within this study in respect of future offending outcomes provides support for the greater risk posed by those radicalised by both online and offline influences as this pathway group were most likely to be convicted for another offence under terrorism legislation. This suggests that members of this pathway group may present additional challenges and also be more resistant to rehabilitation efforts. It may also be the case that risk management strategies utilised in the community are not as robust for managing individuals within the hybrid group due to their history of engaging in extremist activities in both the online and offline domain. However, it is important to note that the hybrid pathway, from being the most prominent radicalisation pathway in 2013–2015, has been at a lower level from 2019 to the end of 2021 than during other time periods, and from 2019, the most prominent radicalisation pathway for convicted extremists is primarily online. This may be accounted for, at least in part, by the effects of the COVID-19 pandemic and consequently, the hybrid pathway may return to being the most prominent route to radicalisation as associated restrictions have now been lifted.

5.2 Recommendations for informing counter-terrorism policy and practice

Based on the findings of this study, six recommendations are proposed to inform future MoJ policy and practice in prison, and wider counter-terrorism policy and practice future:

1. The Internet continues to play an increasingly prominent role in radicalisation processes for convicted extremists and online radicalisation was found to be the most prominent pathway for those sentenced in 2019–21. This highlights the need for online measures and responses to be front and centre of counter-terrorism efforts in England and Wales. Online counter-terrorism measures are applicable to males, females, younger and older individuals, and those expressing an interest in a range of ideologies and causes. For this reason, we

recommend that new online counter-terrorism measures should be designed and developed with consideration given to the heterogeneity of the target audience.

2. Extremist content can be found on mainstream sites and ‘alt-tech’ platforms that have been created or co-opted for the unconventional needs of their users. In recognition of the rapidly changing online technological landscape, we recommend that future research aims to investigate emerging platforms and applications to better understand how these are being used, which ultimately should inform methods that companies employ to respond to extremist content on their platforms.
3. It is now understood that extremists use multiple platforms for their online activity, in what has been described as an online ecosystem (Macdonald et al., 2019). For this reason, we recommend a multi-platform response and co-operation between private social media companies to counter terrorist exploitation of the Internet. One example of a multi-platform response is the Global Internet Forum to Counter Terrorism (GIFCT) (BSR, 2021) founded by Microsoft, Facebook, Twitter and YouTube, but now with 14 further members, which maintains a database of known extremist content that has been removed, preventing the same content being re-uploaded onto any of the participating platforms. In addition, we recommend that technology companies are more transparent about their ongoing efforts to counter terrorism on their platforms as a way of demonstrating accountability and to protect the public.
4. In the previous study, we recommended that individuals identified as particularly vulnerable to online radicalisation and susceptible to online extremist rhetoric would likely benefit from support to develop their social networks to reduce isolation, along with referrals to mental health or personality disorder services where appropriate. Based on the findings of this study, we recommend that specialist input by those familiar with ASC, depression and personality disorder/difficulties is likely to be particularly important. We also recommend that support is offered during times of transition in the lives of those considered vulnerable to online radicalisation to avoid such events becoming a catalyst to increasing engagement with an extremist group or cause. Where concerns also exist in terms of potential offline influences, this should be reflected in risk assessments and the levels of resource and support allocated to individuals given the marked differences in levels of engagement and intent between those

who primarily radicalised online and those radicalised by online and offline influences.

5. The analysis of attackers in the data set suggests that those most likely to carry out a successful attack and prove the hardest to detect are those that conduct the majority of their extremist activities offline. For this reason, we recommend that offline activities of those identified as potential extremists are closely monitored by the Police and security services, and that reasonable concerns relating to potential attack planning are acted upon and investigated at an early stage. For individuals who do use the Internet in the course of their radicalisation pathway, the analysis provides encouragement that online footprints are left that Police and security services can find, which in turn aids in apprehending potential terrorists and supports ongoing investigations. There is also a tendency for individuals who use the Internet in the course of radicalisation to disregard operational security by signalling their intent to commit violent extremist acts.
6. Following the previous study, we recommended that further work was needed to determine how radicalisation pathways can inform the development of interventions and general rehabilitation efforts with extremist offenders within custodial and community settings. It was highlighted that differences found in overall engagement, intent and capability ratings between radicalisation pathway groups provide a more nuanced understanding to potentially inform decisions on appropriate response measures. The current study supports this view and provides additional evidence based on future offending outcome data to suggest these pathway groups present different levels of offending risk, with some individuals potentially more resistant to intervention efforts than others. This may be the case for those who radicalised by both online and offline influences as they were found to be the most likely to commit further TACT offences. With this in mind, we recommend that those involved in the development and implementation of counter-terrorism interventions take account of which risk and protective factors are typically more common across a range of individuals and contexts, and which tend to vary depending on pathway, to ensure effective targeting of areas to reduce risk. We also recommend that differing levels of risk found between pathway groups is considered at point of sentencing, or possibly even at point of arrest, with diversionary solutions offered for some individuals where extremist involvement was only peripheral and took place solely online.

References

Al-Attar, Z. (2020). Autism spectrum disorders and terrorism: how different features of autism can contextualise vulnerability and resilience. *The Journal of Forensic Psychiatry & Psychology, 31*(6), 926–949.

Berger, J. M. (2015). Tailored Online Interventions: The Islamic State's Recruitment Strategy. *CTC Sentinel 8*(10), 19–23.

Bhui, K., Everitt, B., & Jones, E. (2014). Might depression, psychosocial adversity, and limited social assets explain vulnerability to and resistance against violent radicalisation? *PLoS ONE, 9*. Retrieved from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0105918

BSR (2021). *Human Rights Assessment: Global Internet Forum to Counter Terrorism*. Retrieved from: https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf

Chermak, S. M., & Gruenewald, J. (2006). The Media's Coverage of Domestic Terrorism. *Justice Quarterly, 23*(4), 428–461.

Clifford, B., & Powell, H. (2019). Encrypted Extremism: Inside the English-speaking Islamic State ecosystem on Telegram. *Program on Extremism, The George Washington University. Retrieved from:* https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf

Copeland, S., & Marsden, S. (2020). Extremist risk assessment. *Centre for Research and Evidence on Security Threats (CREST) Report*. Retrieved from: https://crestresearch.ac.uk/resources/extremist-risk-assessment/

Corner, E., Gill, P., & Mason, O. (2016). Mental Health Disorders and the Terrorist: A Research Note Probing Selection Effects and Disorder Prevalence. *Studies in Conflict & Terrorism, 39*(6), 560–568.

Crawford, B., Keen, F., & Suarez de-Tangil, G. (2020). Memetic Irony and the Promotion of Violence within Chan Cultures. *Centre for Research and Evidence on Security Threats (CREST) Report.* Retrieved from: https://crestresearch.ac.uk/resources/memetic-irony-and-the-promotion-of-violence-withinchancultures/

EUROPOL (2020). *The terrorism situation in Europe: Impacts of the COVID-19 pandemic and online trends – Policy Brief*. Retrieved from: https://h2020-infinity.eu/sites/default/files/2021-11/ct_europol_v2.pdf

Gill, P., Corner, E., Thornton, A. & Conway, M. (2015). What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists. *EU FP7 VOX-Pol report*. Retrieved from: http://voxpol.eu/what-are-the-roles-of-the-internet-interrorism.

Grierson, J. (2021, Jul 7). 'Staggeringly high' number of autistic people on UK Prevent scheme. *The Guardian*. Retrieved from: https://www.theguardian.com/uk-news/2021/jul/07/staggeringly-high-number-of-people-with-autism-on-uk-prevent-scheme

Hamid, N., & Ariza, C. (2022). Offline versus online radicalisation: Which is the bigger threat? *Global Network on Extremism & Technology*. Retrieved from: https://gnet-research.org/wp-content/uploads/2022/02/GNET-Infographic-Offline-Versus-Online-Radicalisation.pdf

HM Government (2015). *Revised Prevent Duty guidance: for England and Wales.* Retrieved from: https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales#f-glossary-of-terms

HM Prison and Probation Service (2019). *Extremism Risk Guidance (ERG) 22+ – Structured professional guidelines for assessing risk of extremist offending – Manual* (version 1.2). Interventions Services (Internal document).

Kenyon, J., Baker-Beall, C., & Binder, J. (2021a). Lone-actor terrorism – A systematic literature review. *Studies in Conflict and Terrorism*, 1–24. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/1057610X.2021.1892635

Kenyon, J., Binder, J., & Baker-Beall, C. (2021b). Exploring the role of the Internet in radicalisation and offending of convicted extremists. *Ministry of Justice Analytical Series.* Retrieved from: https://www.gov.uk/government/publications/exploring-the-role-of-the-internet-in-radicalisation-and-offending-of-convicted-extremists

Lakhani, S. (2021). Is it just a game? Exploring the intersection between (violent) extremism and online video-gaming. *VOX-Pol Blog*. Retrieved from: https://www.voxpol.eu/is-it-just-a-game/

Lloyd, M., & Dean, C. (2015). The development of structured guidelines for assessing risk in extremist offenders. *Journal of Threat Assessment and Management, 2*, 40–52.

Lloyd, M., & Kleinot, P. (2017). Pathways into terrorism: The good, the bad and the ugly. *Psychoanalytic Psychotherapy, 31*(4), 367–377.

Macdonald, S., Grinnell, D., Kinzelm A., & Lorenzo-Dus, N. (2019). Daesh, Twitter and the Social Media Ecosystem – A Study of Outlinks Contained in Tweets Mentioning Rumiyah. *The RUSI Journal, 164*(4), 60–72.

Macklin, G. (2019). The Christchurch Attacks: Livestream terror in the viral video age. *CTC Sentinel, 12*(6). Retrieved from: https://ctc.usma.edu/christchurch-attacks-livestream-terror-viral-video-age/

Malik, N. (2018). *Terror in the Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies.* Henry Jackson Society. Retrieved from: http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

McManus, S., Bebbington, P., Jenkins, R., & Brugha, T. (2016). *Mental health and wellbeing in England: Adult Psychiatric Morbidity Survey 2014*. Leeds: NHS Digital. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/556596/apms-2014-full-rpt.pdf

Meleagrou-Hitchens, A., & Kaderbhai, N. (2017). *Research Perspectives on Online Radicalisation: A Literature Review 2006–2016.* N.p.: VOX-Pol. Retrieved from: http://icsr.info/2017/05/icsr-vox-pol-paper-research-perspectives-online-radicalisation-literature-review-2006-2016

Merari, A., Diamant, I., Bibi, A., Broshi, Y., & Zakin, G. (2009). Personality characteristics of 'self martyrs'/'suicide bombers' and organizers of suicide attacks. *Terrorism and Political Violence, 22*(1), 87–101.

Ministry of Justice (2020). *Terrorism: Prisoner's Release – Question for Ministry of Justice*. Retrieved from: https://questions-statements.parliament.uk/written-questions/detail/2020-01-27/HL782

Ministry of Justice (2022). *Guide to proven reoffending statistics*. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1094532/Guide-to-proven-reoffending-Jul22_Final.pdf

O'Driscoll, D. (2018). *Violent extremism and mental health: K4D helpdesk report*. Institute of Development Studies. Retrieved from: https://assets.publishing.service.gov.uk/media/5c700673ed915d4a3e8266e7/476_Violent_Extremism_and_Mental_Disorders.pdf

Ofcom (2020, June 24). *Online Nation – 2020 Summary Report*. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/196408/online-nation-2020-summary.pdf

Pandya, A. & Lodha, P. (2021). Social connectedness, excessive screen time during COVID-19 and mental health: A review of current evidence. *Frontiers in Human Dynamics, 3*, 684137. Retrieved from: https://doi.org/10.3389/fhumd.2021.684137

Powis, B., Randhawa, K. & Bishopp, D. (2019a). An examination of the structural properties of the Extremism Risk Guidelines (ERG22+); a structured formulation tool for extremist offenders. *Terrorism and Political Violence, 33*(6), 1141–1159. Retrieved from: http://www.tandfonline.com/doi/full/10.1080/09546553.2019.1598392

Powis, B., Randhawa-Horne, K., Elliott, I. & Woodhams, J. (2019b). Inter-rater reliability of the Extremism Risk Guidelines 22+ (ERG22+). *Ministry of Justice Analytical Series.* Retrieved from: https://www.gov.uk/government/publications/inter-rater-reliability-of-the-extremism-risk-guidelines-22-erg-22

Reinares, F., García-Calvo C., & Vicente, A. (2017). Differential association explaining jihadi radicalisation in Spain: A quantitative study. *CTC Sentinel 10*(6), 29–34.

Ritchie, H., Hasell, J., Appel, C., & Roser, M. (2019). Terrorism. *Our World in Data*. Retrieved from: https://ourworldindata.org/terrorism

Schlegel, L. (2021). The gamification of violent extremism and lessons for P/CVE. *RAN External Report.* Retrieved from: https://ec.europa.eu/home-affairs/system/files/2021-03/ran_ad-hoc_pap_gamification_20210215_en.pdf

Silke, A. (2014). Risk assessment of terrorist and extremist prisoners, in A. Silke (Ed.) *Prisons, terrorism and extremism: Critical issues in management, radicalisation and reform* (pp.108–121). London: Routledge.

Weatherston, D, & Moran, J. (2003). Terrorism and mental illness: is there a relationship? *International Journal of Offender Therapy and Comparative Criminology, 47*(6), 698–713.

Whittaker, J. (2021). The online behaviors of Islamic state terrorists in the United States. *Criminology and Public Policy, 20*(1), 177–203. Retrieved from: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1745-9133.12537

Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, Johanna. (2020). Online extremism: Research trends in Internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence, 14*(2), 1–20. Retrieved from: https://www.ijcv.org/index.php/ijcv/article/view/3809

Appendix A

Note on terminology

Extremist offending – defined as “any offence committed in association with a group, cause, and/or ideology that propagates extremist views and actions and justifies the use of violence and other illegal conduct in pursuit of its objectives” (HM Prison and Probation Service, 2019, p. 8).

Radicalisation – defined as “the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups” (HM Government, 2015, p. 21).

TACT offence – an offence that falls under terrorism legislation.

TACT-related offence – an offence that falls under other legislation but was either part of a counter terrorism investigation or deemed by the investigating force to have an extremist motivation.

TACT-connected offence – an offence that falls under other legislation but the sentencing court has determined has a ‘terrorist connection’.

The following categories referred to within this study reflect the ideological persuasion of individuals within the sample:

Animal Rights – A category to reflect a number of individuals who claim to support animal rights and used this to justify their actions.

Extreme Right Wing – A category to reflect a number of individuals inspired by extreme right wing ideology and used this to justify their actions.

Islamist Extremist – A category to reflect a number of individuals inspired by an Islamist extremist ideology and used this to justify their actions.

Other Political – A category to reflect a number of individuals described as anti-establishment or supporting a far-left ideology, along with those affiliated with nationalist or separatist movements.

Appendix B

Variables of interest

The first variable of interest related to the four types of prison-based extremist identified by Silke (2014).

Type of prison-based extremist – Categories included: 'Radicalised extremist,' considered to be an individual who entered prison already holding extremist views and who had engaged in extremist actions in the outside world; 'Affiliate,' an individual who had been convicted of involvement in extremism or terrorism, but with good reasons to suggest they were not radicalised when they did so; 'Prison Recruit,' described by Silke (2014) as 'ordinary decent' individuals who had been radicalised within prison, possibly as a result of contact with extremist prisoners; and 'Vulnerable,' described by Silke (2014) as 'ordinary decent' individuals who, whilst not yet radicalised, may be assessed as vulnerable to joining the 'spectacular few' in the right circumstances. When the development of extremist beliefs occurred was generally referenced within the formulation section of the SRG and ERG22+ reports, which provided a narrative account for how someone came to be engaged with an extremist group, cause and/or ideology. When a formulation was not included within the report, the onset of extremist beliefs was at times referenced within the summary of offending section of the report or within the scoring of the factors comprising the assessment.

The second variable of interest related to the radicalisation pathway undertaken by individuals.

Primary method of radicalisation – This variable related to identifying the primary method of radicalisation based on evidence contained within the SRG/ERG22+ report. Categories included 'internet' for those who primarily radicalised online, 'face-to-face' for those who primarily radicalised offline, and 'hybrid' for individuals where both online and offline influences were considered significant. Examples of coding this variable are as follows: if there was a lack of reference within the report to the individual having engaged in offline interactions or meetings with other extremists,

yet they were reported to have participated in online activity or exchanges with other extremists, this would be coded as ‘internet’. In another example, if an individual reported having initially been exposed to extremist materials and discussions online, but also shared their views had later been reinforced having met with other co-ideologues in offline settings, this would be coded as ‘hybrid’. If the radicalisation pathway was unclear from available information, ‘Not clear’ was used.

Information was coded relating to internet activities and behaviours commonly associated with online radicalisation. For individuals where internet use was relevant, the following internet activity variables were coded dichotomously (e.g., ‘Yes’ or ‘No evidence’), unless stated otherwise:

Learnt from online sources – This variable related to whether an individual had learnt from online sources.

Interact with co-ideologues online – This variable related to whether an individual had communicated with co-ideologues online.

Generate their own extremist propaganda online – This variable related to whether an individual had generated their own extremist propaganda online. Examples included if an individual had designed their own extremist image or posted comments of an extremist nature online. However, if they had posted a link to extremist material on another platform that others had generated, this would not be included.

Use of specific extremist websites/homepages – This variable related to whether an individual had accessed specific extremist websites or home pages online. Examples included if an individual had set up their own website to promote extremist ideology or published details of animal testing companies on an animal rights activist website. However, if they had accessed extremist content online but only through open social media platforms, this would not be included.

Use of forums/chatrooms – This variable related to whether an individual had accessed specific forums or chatrooms online (e.g., Fascist Forge, Iron March, Incel.co).

Use of standard communication applications and platforms – This variable related to whether an individual had used standard communication applications and platforms online. Standard communication applications and platforms are those where the intended standard use is generally for more restricted/targeted communication to others (e.g., E-mail, Skype and MSN messenger).

Use of open social media platforms – This variable related to whether an individual had used open social media applications or platforms online. Open social media applications or platforms are those where the intended standard use is generally made for increased openness and wider sharing or distribution of content to others (e.g., Facebook, Twitter and YouTube).

Use of encrypted applications – This variable related to whether an individual had used encrypted applications online (e.g., Telegram, Viber and WhatsApp – from 2016 when end-to-end encryption introduced).

Use of dark web – This variable related to whether an individual was reported to have used the dark web.

Use of online computer/video games – This variable related to whether online computer games were reported as having contributed to an individual's involvement with extremism or pathway to offending.

Use of imageboards – This variable related to whether an individual had used anonymous imageboards (aka chanboards), a specific type of online forum (e.g., 4chan, 8chan, 8kun and Endchan).

Livestreaming attacks – This variable related to whether an individual was reported to have livestreamed their attack online. This did not include those who are reported

to have recorded themselves committing their offence with the intention of uploading onto the Internet afterwards.

To obtain demographic and offence type information for all individuals within the data set, the following variables were created by applying the coding scheme:

Age – This variable related to the age of an individual at time of sentencing, with categories of ‘Up to (and including) 25’ and ‘Over 25’.

Sex – Coded as ‘Male’ or ‘Female’.

Place of birth – Coded as ‘UK’ or ‘Non-UK’.

Prior offending history – This variable related to convicted offences only. Coded as ‘Yes’ or ‘No’.

Prior violent offending history – This variable related to convicted violent offences only. Coded as ‘Yes’ or ‘No’.

Prior TACT or TACT-related offending history – This variable related to convicted offences that fall under terrorism legislation (TACT) and convicted offences that fall under terrorism legislation but where the motivation was considered extremist (TACT-related). Coded as ‘Yes’ or ‘No’.

Presence of mental health issues/neurodivergence/personality disorder – This variable related to whether an individual had mental health difficulties, neurodivergence and/or personality disorder/difficulties based on ratings from the corresponding factor within the ERG22+ assessment.

Reported brain/head injury – This variable related to whether an individual was reported to have a brain or head injury. Coded as ‘Yes’ or ‘No evidence’.

Violent or non-violent index offence – This variable related to whether an individual was violent or non-violent based on the nature of their index offence. This

was included to distinguish between those who only espoused radical beliefs and those prepared to commit acts of extremist-related violence. For the purposes of coding, a strict definition of 'Violent' was used: those convicted of any act which constituted, or any potential act which, if carried out would constitute, Murder, Attempted Murder, Manslaughter, Assault, and/or real injury to another, and/or cause serious and significant structural damage. Therefore, the 'Violent' sub-category included some individuals who were arrested prior to having conducted an act of violence but were convicted on the basis there was sufficient evidence they would have committed the act had they not been disrupted. Individuals who had knowingly exhibited non-violent behaviours that could facilitate violence conducted by others (e.g., by disseminating extremist materials online) would fall within the 'Non-violent' sub-category.

Online-only index offence – This variable related to whether an individual was solely convicted for extremist offences that took place online as part of the index offence. Coded as 'Yes' or 'No'.

Role in event – This variable related to the role taken by an individual within the index offence. Categories included 'Attacker', where an individual had either committed an extremist attack themselves on another person or property, or there was sufficient evidence (based on their conviction) they would have done had they not been arrested/disrupted; 'Traveller', where an individual had either travelled to other countries to pursue extremist goals, or there was sufficient evidence (based on their conviction) they would have done had they not been arrested/disrupted; 'Financer', where an individual had provided financial support either to others with extremist views or to an extremist group/organisation; and 'Facilitator', where an individual had provided direct or indirect support (other than financial) to others with extremist views or to an extremist group/organisation. This also included those who may have provided some level of direct support to others (e.g., supporting others involved in extremist activity) or those who provided indirect support through inspiring others through their actions (e.g. through disseminating extremist material online).

Degree of social connection – This variable related to an individual's degree of social connection with other extremists in an offline setting during the lead up to and

around the time of the index offence. Categories included ‘Lone’, ‘Small cell’ (2–3 people) and ‘Group’ (4 people or more).

Ideology – This variable related to the specific ideology supported by an individual, with categories of ‘Islamist Extremist’, ‘Extreme Right Wing’, ‘Other Political’ and ‘Animal Rights’.

A number of variables included within the study were specific only to attackers within the data set. For attackers where internet use was relevant, the following three ‘online planned action behaviour’ variables were coded dichotomously (e.g., ‘Yes’ or ‘No evidence’), unless stated otherwise:

Attack preparation online – This variable related to whether an individual had used the Internet for attack preparation purposes (e.g., accessing poison recipes, bomb-making instructions, purchasing chemicals online, purchasing body armour and/or equipment etc.).

Target identification online – This variable related to whether an individual had used the Internet to select a target(s) when attack planning (e.g., researching specific individuals, military facilities, religious buildings, government buildings etc.).

Signalling intent to attack online – This variable related to whether the individual had used the Internet to signal their attack plans to others (e.g., could be vague such as telling others to watch the news as they would feature, or more specific regarding the necessity of targeting a particular place or individual).

For attackers within the data set, the following plot-related variables were also coded:

Type of plot – This variable related to the type of plot that attackers had developed based on weapon choice/manner of attack. Coding options included: Improvised Explosive Device (IED), arson, firearm, bladed weapon, vandalism/criminal damage, vehicle or unarmed assault.

Moved to execution stage – This variable related to whether the plot had progressed beyond planning to being executed (even if execution had only reached the early stages). Coded as ‘Yes’ or ‘No’.

Completed plot – This variable related to whether the plot was executed to completion. Coded as ‘Yes’ or ‘No’.

How plot was thwarted – For those plots that were foiled or disrupted, this variable related to the reasons why they were ultimately unsuccessful. Coding options included: Police/security services, IED did not detonate, attacker lost nerve or attacker missed target.

In terms of variables specific to the ERG22+ assessment, the ratings provided by the assessor for all 22 individual factors were recorded (see Table 7 in Appendix L for ERG22+ factors and domains). These were obtained from either the ERG22+ scoring grid attached to each report or where factor ratings were referenced within the body of the report. These variables were coded based on the corresponding rating provided (either Not Present, Partly Present, Strongly Present or Omitted). Other variables specific to the ERG22+ assessment included overall ratings for engagement, intent and capability. These were obtained from either the ERG22+ scoring grid attached to each report or where overall ratings for engagement, intent and capability were referenced within the body of the report. These variables were coded based on the corresponding rating provided:

Overall engagement rating – This variable related to the summary score for ‘engagement’, based on the scoring of 13 engagement items forming part of the ERG22+ assessment. This scale is not summative, so the number of individual engagement factors endorsed does not correspond with the strength of the individual’s overall level of engagement. Instead, this is an overall judgement by the assessor (in terms of Low, Low-Medium, Medium, Medium-High or High) to reflect the individual’s level of engagement to the extremist group, cause and/or ideology (and motivation to offend) at the time of offending.

Overall intent rating – This variable related to the summary score for ‘intent’, based on the scoring of 6 intent items forming part of the ERG22+ assessment. This scale is not summative, so the number of individual intent factors endorsed does not correspond with the strength of the individual’s overall level of intent. Instead, this is an overall judgement by the assessor (in terms of Low, Low-Medium, Medium, Medium-High or High) to reflect an individual’s mental state of readiness to commit extremist offences that could cause serious and significant harm at the time of offending.

Overall capability rating – This variable related to the summary score for ‘capability’, based on the scoring of 3 capability items forming part of the ERG22+ assessment. This scale is not summative, so the number of individual capability factors endorsed does not correspond with the strength of the individual’s overall level of capability. Instead, this is an overall judgement by the assessor (in terms of Minimal, Minimal-Some, Some, Some-Significant or Significant) to reflect the individual’s level of capability to commit extremist offences that could cause serious and significant harm at the time of offending.

Appendix C

Comparing variables of sex, age and ideology in terms of the prominence of the Internet in radicalisation over time

The Internet was found to have played an increasingly prominent role in radicalisation for both males and females, along with younger and older individuals. This increase was most marked for females, with a 100-percentage point increase from those sentenced in 2007–09, where all females had primarily radicalised offline, to 2019–21, where all females had either primarily radicalised online or by both online and offline influences. For males, a 48-percentage point increase was found over the same time period (43% to 91%). However, in contrast to the first study, the increasingly prominent role of the Internet in radicalisation was most evident for older rather than younger individuals. The older generation experienced a 54-percentage point increase where internet use contributed to radicalisation for those sentenced in 2007–09 to those sentenced in 2019–21 (40% to 94%), whereas a 47-percentage point increase was found for members of the younger generation over the same time period (43% to 90%). When explaining this finding, it is clear that there has been a considerable increase in internet use by older individuals since 2018 (17-percentage point increase, 77% to 94%) to levels similar to that of the younger age group in 2019–2021 (91%).

When considering a breakdown by ideological affiliation, the Internet was found to have played an increasingly prominent role in radicalisation for Islamist Extremists. A 53-percentage point increase was found for individuals where internet use contributed to radicalisation when comparing those sentenced in 2007–09 to those sentenced in 2019–21 (39% to 92%). For the Extreme Right Wing group, a 9-percentage point increase was observed over the same time period (83% to 92%). For both ideological groups, only small numbers of those sentenced from 2013 onwards were primarily radicalised offline. With the Other Political group, a 50-percentage point increase was found between 2007–09 and 2019–21 (50% to 100%). For Animal Rights activists, in-person contact with others has remained a key feature of their radicalisation over time.

Appendix D

Detailed analysis of changes in use of applications/platforms over time

Specific extremist websites/homepages have seen a steady decline in use when comparing proportion of use in 2007–09 with that in 2019–21. For those who primarily radicalised online, a 29-percentage point decrease was found, whilst an 11-percentage point and 44-percentage point decrease was found for those who primarily radicalised offline and those subject to online and offline influences respectively.

All three pathway groups also demonstrated a reduction in use of standard communication applications and platforms over time (Starting in 2007–09 and extending to 2019–21, face-to-face = 14-percentage point decrease, hybrid = 17-percentage point decrease). Unlike the other two pathway groups, the first evidence of standard communication applications and platforms by those who primarily radicalised online was for those sentenced in 2013–15. A 12-percentage point decrease was found in use of standard communication applications/platforms, compared with those sentenced in 2019–21. The most common standard communication applications/platforms mentioned in reports were WhatsApp (pre-2016, prior to end-to-end encryption being introduced, 25 individuals), E-mail (23 individuals), Paltalk (11 individuals) and Skype (6 individuals).

Increased use of forums/chatrooms was found for all three pathway groups from 2007–09 up to 2019–21 (internet = 22-percentage point increase, face-to-face = 17-percentage point increase, hybrid = 2-percentage point increase). However, for most individuals where forum/chatroom use had been reported, the specific site was not mentioned. Where specific forums or chatrooms were referenced, the most common were Discord (3 individuals), Fascist Forge (2 individuals), Iron March (2 individuals) and several others were mentioned for 1 individual only (i.e., Stormfront, Revolution Muslim, Incels.co).

Consistent with the previous study, an increase was found in number of individuals using open social media platforms across all three pathway groups from 2007–09 up

to 2019–21 (internet = 54-percentage point increase, face-to-face = 60-percentage point increase, hybrid = 52-percentage point increase). Where specific open social media platforms were reported, the most popular were YouTube (115 individuals), Facebook (90 individuals), Twitter (66 individuals) and Instagram (14 individuals).

For cases within the sample, use of encrypted applications was most evident for those sentenced from 2013–15 onwards. This is consistent with the onset of disruption efforts and suspensions of accounts promoting extremist material across mainstream open social media platforms. For example, with Twitter, disruption efforts gathered pace from mid-2014 (Berger & Morgan, 2015). When comparing convicted extremists sentenced in 2013–15 with those sentenced in 2019–21, an increase was found in use of encrypted applications[15] across all three pathway groups (internet = 45-percentage point increase, face-to-face = 15-percentage point increase, hybrid = 61-percentage point increase). Where encrypted applications were referenced, the most popular were Telegram (65 individuals), WhatsApp (38 individuals, from 2016 onwards when default end-to-end encryption was introduced), Surespot (6 individuals), KIK messenger and Viber (5 individuals each).

In relation to use of the dark web, this was only reported for 11 individuals from those sentenced in 2013–15 onwards. Those who primarily radicalised online were found to have used the dark web most frequently (6% of pathway group members), followed by those who radicalised by both online and offline influences (2% of pathway group members). No individuals who primarily radicalised offline were found to have used the dark web.

Across 437 ‘Radicalised Extremists’, the use of online computer games was reported for 31 (7%) individuals, with varying degrees of suggestion by authors that these contributed to their radicalisation pathway. Of these 31 individuals, the vast majority were made up of those who primarily radicalised online (48%) and those radicalised by both online and offline influences (48%). Online computer game use was most prevalent for those sentenced from 2013–15 onwards. Whilst specific games played

[15] Some applications referred to in the ‘encrypted applications category’ are default end-to-end encrypted (e.g., WhatsApp), whilst some are not (e.g., Telegram).

were only mentioned for a small minority of individuals, the most common were first-person shooter games and/or those centred on a war theme with online capabilities. This included Call of Duty (8 individuals), Medal of Honour (1 individual), Battlefront (1 individual) and Grand Theft Auto (1 individual). This preference for first-person shooter games and those based on a war theme is in line with studies on how extremist organisations employ the appearances of gaming. Daesh are reported to have used footage from video games such as Call of Duty and imitated the aesthetics and viewpoint of first-person shooter games within propaganda videos filmed with helmet cameras (Schlegel, 2021). As referenced previously, but related to online gaming, the most common forum/chatroom referenced in reports was Discord (3 individuals), an application originally designed for gamers.

In terms of other recent developments in internet use by extremists reported within the literature (see Crawford et al., 2020), use of imageboards was only reported as relevant for 4 individuals from those sentenced from 2016–18 onwards. The use of imageboards was most frequently reported for those radicalised by both online and offline influences (3 individuals), followed by those who primarily radicalised online (1 individual). Whether individuals had livestreamed attacks online was also investigated, but this was found to be not relevant for all cases within the data set.

Appendix E

Online activity variables as predictors for pathway group classification

Table 2. Online activity variables as predictors for pathway group classification

Predictor	B	SE(B)	Odds Ratio
Predicting face-to-face against internet group			
Intercept	6.25	0.96	
Learnt from online sources	-5.69***	0.92	0.003 [0.001, 0.020]
Interact with co-ideologues online	-2.80***	0.81	0.06 [0.01, 0.30]
Generate own extremist propaganda online	0.95	0.70	2.59 [0.66, 10.12]
Use of extremist websites/home pages	0.53	0.60	1.69 [0.52, 5.51]
Use of forums/chatrooms	-0.54	1.07	0.59 [0.07, 4.73]
Use of open social media platforms	-2.34***	0.61	0.10 [0.03, 0.32]
Use of standard communication applications/platforms	0.06	0.82	1.06 [0.21, 5.30]
Use of encrypted applications	-0.60	0.77	0.55 [0.12, 2.50]
Predicting hybrid against internet group			
Intercept	0.35	0.99	
Learnt from online sources	1.26	0.95	3.51 [0.55, 22.57]
Interact with co-ideologues online	-0.11	0.36	0.90 [0.45, 1.81]
Generate own extremist propaganda online	-0.60*	0.29	0.55 [0.31, 0.97]
Use of extremist websites/home pages	0.49	0.35	1.62 [0.83, 3.19]
Use of forums/chatrooms	-0.40	0.33	0.67 [0.35, 1.28]
Use of open social media platforms	-0.91**	0.29	0.40 [0.23, 0.72]
Use of standard communication applications/platforms	0.33	0.34	1.39 [0.71, 2.71]
Use of encrypted applications	-0.18	0.28	0.83 [0.48, 1.44]

NB: Multinomial logistic regression coefficients predicting pathway group membership for the face-to-face group (top half) and the hybrid group (bottom half) using the internet group as reference category. Nagelkerke's R^2 = .68. ***significant at p < .001, *significant at p < .05. Numbers in parentheses refer to 95% confidence intervals.

Appendix F

Percentages of profile and vulnerability factors across pathway groups

Table 3. Percentages of profile and vulnerability factors across pathway groups

Profile and vulnerability factors (n = 437 unless specified)		internet (n = 108) Percentage (%)	hybrid (n = 204) Percentage (%)	face-to-face (n = 125) Percentage (%)
Age at sentencing***	Up to + including 25	44‡	53†	29†‡
	Over 25	56‡	47†	71†‡
Sex	Male	89	90	87
	Female	11	10	13
Place of birth (n = 424)	UK	68	70	71
	Non-UK	32	30	29
Prior offending history*** (n = 434)	Yes	28‡	30†	52†‡
	No	72‡	70†	48†‡
Prior violent offending history*** (n=433)	Yes	15‡	17†	35†‡
	No	85‡	83†	65†‡
Prior TACT or TACT-related offending history***	TACT offence	0‡	6†‡	2†
	TACT-related offence	4‡	18†‡	3†
	No evidence	96‡	75†‡	96†
Presence of mental health issues/ neurodivergence/ personality disorder *** (n = 415)	Strongly present	42†‡	13†	7‡
	Partly present	9	15	12
	Not present	49†‡	72†	80‡
Reported brain/head injury	Yes	7	3	1
	No evidence	93	97	99
Violent/non-violent index offence***	Violent	16†‡	32†♯	51‡♯
	Non-violent	84†‡	68†♯	49‡♯
Role in offence***	Attacker	16†‡	32†♯	51‡♯
	All other roles	84†‡	68†♯	49‡♯
Online only index offence***	Yes	57†‡	22†♯	6‡♯
	No	43†‡	78†♯	94‡♯
Degree of social connection*** (n = 435)	Lone	85†‡	9‡	6†
	Small cell (2–3)	10‡	22†‡	9†
	Group	5†‡	69†♯	86‡♯
Ideology***	Islamist extremist	75‡	79†	58†‡
	All other ideologies	25‡	21†	42†‡

NB: Chi-squared tests were used for overall associations, except for prior TACT/TACT-related offending and reported brain/head injury where Fisher's exact test was used due to low expected cell count.

***significant association with radicalisation pathway at $p < .001$.

†,‡,♯: significant pairwise post hoc comparisons, Bonferroni-adjusted, at $p < .05$; in each row, same indices indicate a difference in proportions.

Appendix G

Most common offences committed by each pathway group

Table 4. Frequency count of most common offences committed by pathway groups

Pathway group	Type of offence	Frequency count
internet (108 individuals)	Dissemination of terrorist materials/distributing materials to stir up racial hatred/encouraging terrorism/inciting another to commit acts of terrorism	42
	Engaging in conduct in preparation for terrorist acts	31
	Possession of terrorist materials	18
hybrid (204 individuals)	Engaging in conduct in preparation for terrorist acts	88
	Dissemination of terrorist materials/distributing materials to stir up racial hatred/encouraging terrorism/inciting another to commit acts of terrorism	39
	Possession of terrorist materials	18
face-to-face (125 individuals)	Arson/making explosives/conspiracy to cause explosion	22
	Murder/conspiracy to murder/attempted murder/soliciting to murder/manslaughter	21
	Robbery/GBH/ABH/violent disorder	17

Appendix H

Multinomial Logistic Regression Summary for ERG22+ factors, with detailed analysis

Table 5. ERG22+ factors as predictors for pathway group classification

Predictor	B	SE(B)	Odds Ratio
Predicting face-to-face against internet group			
Intercept	0.20	0.49	
Susceptibility to indoctrination	-0.51*	0.23	0.60 [0.38, 0.95]
Family and/or friends support extremism	0.42	0.22	1.52 [0.99, 2.33]
Transitional periods	-0.69**	0.25	0.50 [0.31, 0.82]
Group influence and control	0.76**	0.28	2.15 [1.25, 3.68]
Mental health/neurodivergence/PD	-1.20***	0.25	0.30 [0.18, 0.50]
Harmful end objectives	0.33	0.28	1.40 [0.80, 2.43]
Access to networks, funding and equipment	0.91***	0.28	2.49 [1.45, 4.27]
Criminal history	1.23***	0.46	3.41 [1.91, 6.12]
Predicting hybrid against internet group			
Intercept	-0.32	0.46	
Susceptibility to indoctrination	0.13	0.21	1.14 [0.75, 1.74]
Family and/or friends support extremism	0.82***	0.20	2.27 [1.54, 3.34]
Transitional periods	-0.53*	0.23	0.59 [0.37, 0.93]
Group influence and control	0.27	0.25	1.31 [0.80, 2.13]
Mental health/neurodivergence/PD	-0.96***	0.20	0.38 [0.26, 0.57]
Harmful end objectives	0.60*	0.25	1.82 [1.11, 2.98]
Access to networks, funding and equipment	0.75**	0.25	2.12 [1.29, 3.48]
Criminal history	0.47	0.29	1.60 [0.91, 2.82]

NB: Multinomial logistic regression coefficients predicting pathway group membership for the face-to-face group (top half) and the hybrid group (bottom half) using the internet group as reference category. Forward stepwise entering of variables was used. Nagelkerke's R^2 = .41. ***significant at p < .001, *significant at p < .05. Numbers in parentheses refer to 95% confidence intervals.

Comparing internet and face-to-face pathways, the likelihood of belonging to the face-to-face group increased by 115 per cent with every unit increase in assessed group influence and control (B = .76, SE = .28, OR = 2.15, 95% CI [1.25, 3.68], p < .01), by 149 per cent with every unit increase in assessed access to networks, funding and equipment (B = .91, SE = .28, OR = 2.49, 95% CI [1.45, 4.28], p < .001) and by 241 per cent with every unit increase in assessed criminal history (B = 1.23, SE = .30, OR = 3.41, 95% CI [1.91, 6.12], p < .001). In contrast, the odds of face-to-

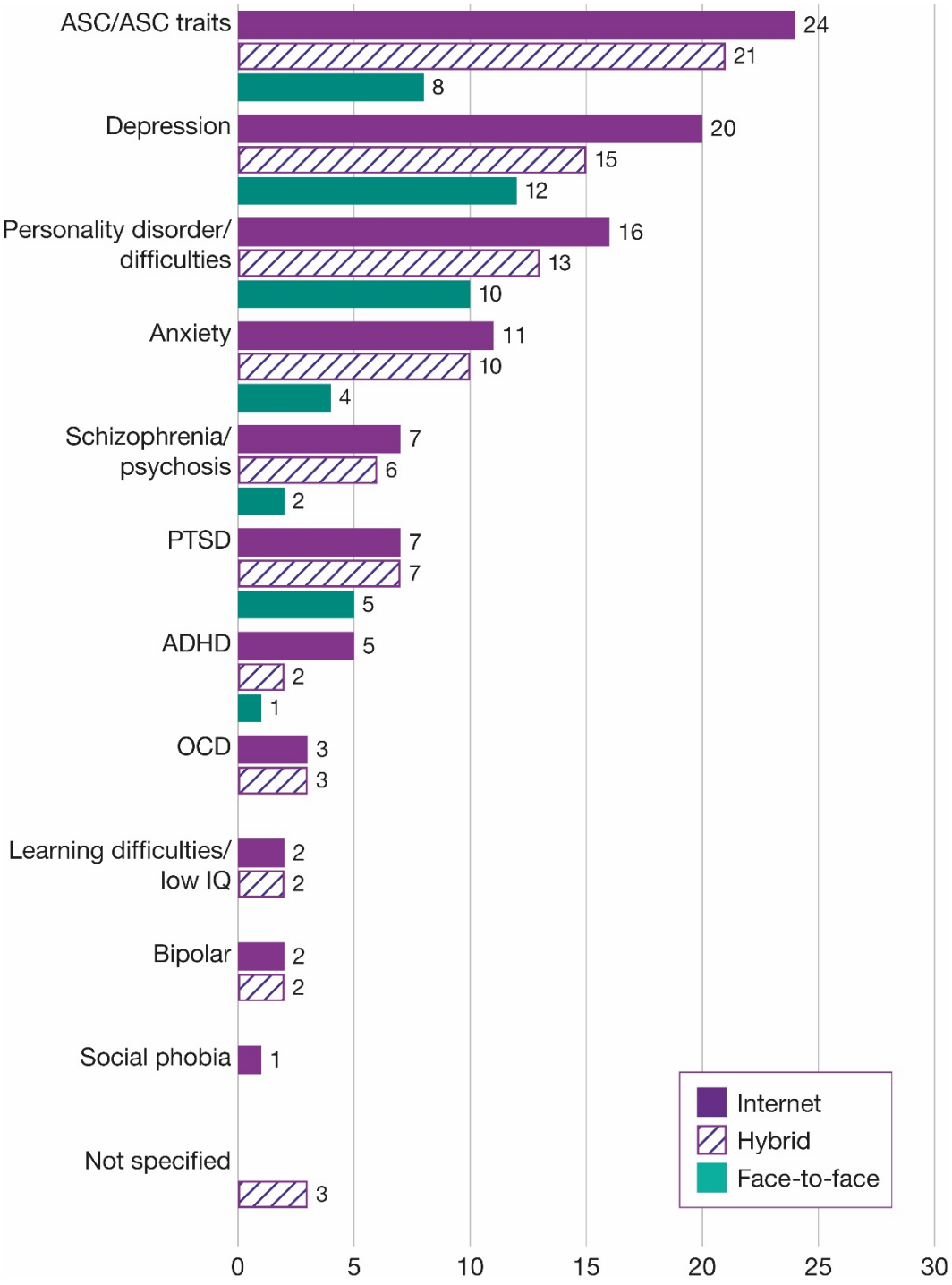
face pathway membership decreased by 40 per cent with every unit increase in assessed susceptibility to indoctrination (B = -.51, SE = .23, OR = 0.60, 95% CI [.38, .95], p < .05), by 50 per cent with every unit increase in assessed transitional periods (B = -.69, SE = .25, OR = 0.50, 95% CI [.31, .82], p < .01) and by 70 per cent with every unit increase in assessed mental health issues, neurodivergence or personality disorder/difficulties (B = -1.20, SE = .25, OR = 0.30, 95% CI [.18, .50], p < .001).

Comparing hybrid and internet pathways, a modified pattern emerged. The likelihood of belonging to the hybrid group increased by 127 per cent with every unit increase in assessed family and/or friends' support of extremism (B = .82, SE = .20, OR = 2.27, 95% CI [1.54, 3.34], p < .001), by 82 per cent with every unit increase in assessed harmful end objectives (B = .60, SE = .25, OR = 1.82, 95% CI [1.11, 2.98], p < .05), and by 112 per cent with every unit increase in assessed access to networks, funding and equipment (B = .75, SE = .25, OR = 2.12, 95% CI [1.29, 3.48], p < .01). In contrast, the odds of hybrid group membership decreased by 41 per cent with every unit increase in assessed transitional periods (B = -.53, SE = .23, OR = 0.59, 95% CI [.37, .93], p < .05), and by 62 per cent with every unit increase in assessed mental health issues, neurodivergence or personality disorder/difficulties being present (B = -.96, SE = .20, OR = 0.38, 95% CI [.26, .57], p < .001).

Appendix I

Frequency counts of types of mental health issue/neurodivergence/ personality disorder across primary method of radicalisation

Figure 2. Frequency counts of types of mental health issue/neurodivergence/ personality disorder across primary method of radicalisation



NB: For 45 (31%) of the 143 individuals, co-morbidity was relevant with more than one type of mental health issue/neurodivergence/personality disorder identified.

Appendix J

Percentages of attacker plot-related variables across pathway groups

Table 6. Percentages of attacker plot-related variables across pathway groups

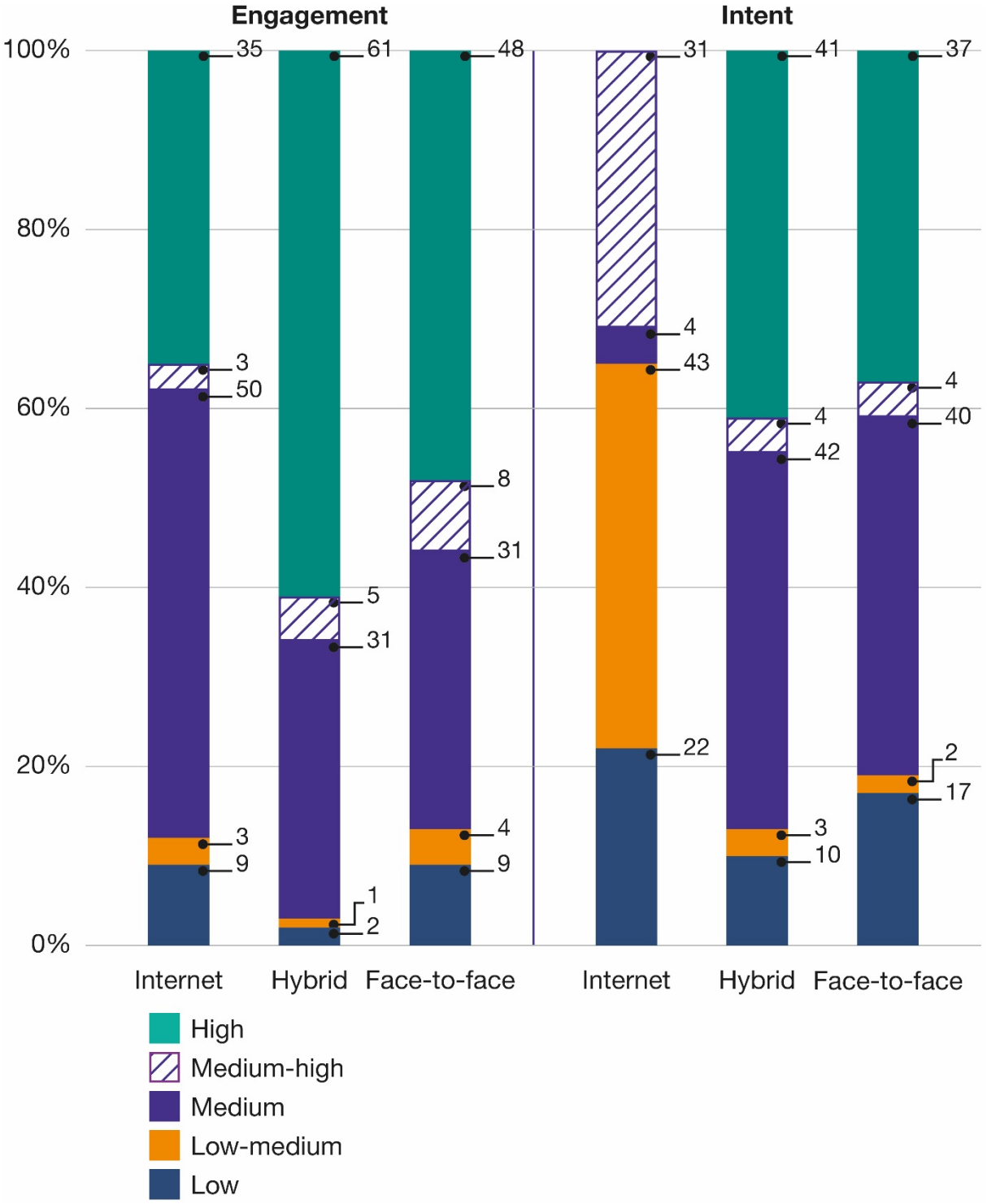
Attacker variables (n = 137 unless specified)		internet (n = 17) Percentage (%)	hybrid (n = 65) Percentage (%)	face-to-face (n = 55) Percentage (%)
Type of plot*	IED	65	60	49
	Arson	0	6	9
	Firearm	6	8	4
	Bladed weapon	24	31	11
	Vandalism/crim damage	0	2	13
	Vehicle	12	8	2
	Unarmed assault	0	5	15
Moved to execution stage		29	39	66
Completed plot		18	22	58
How plot was thwarted	Police/security services	100	84	87
	IED did not detonate	0	4	9
	Lost nerve	0	0	4
	Missed target	0	12	0

NB: *Percentages under ‘type of plot’ equate to the percentage of plots against the overall number of plots that involved each type of weapon (as some plots involved multiple weapons).

Appendix K

Percentages for overall engagement and intent ratings from the ERG22+ across primary method of radicalisation at time of offending

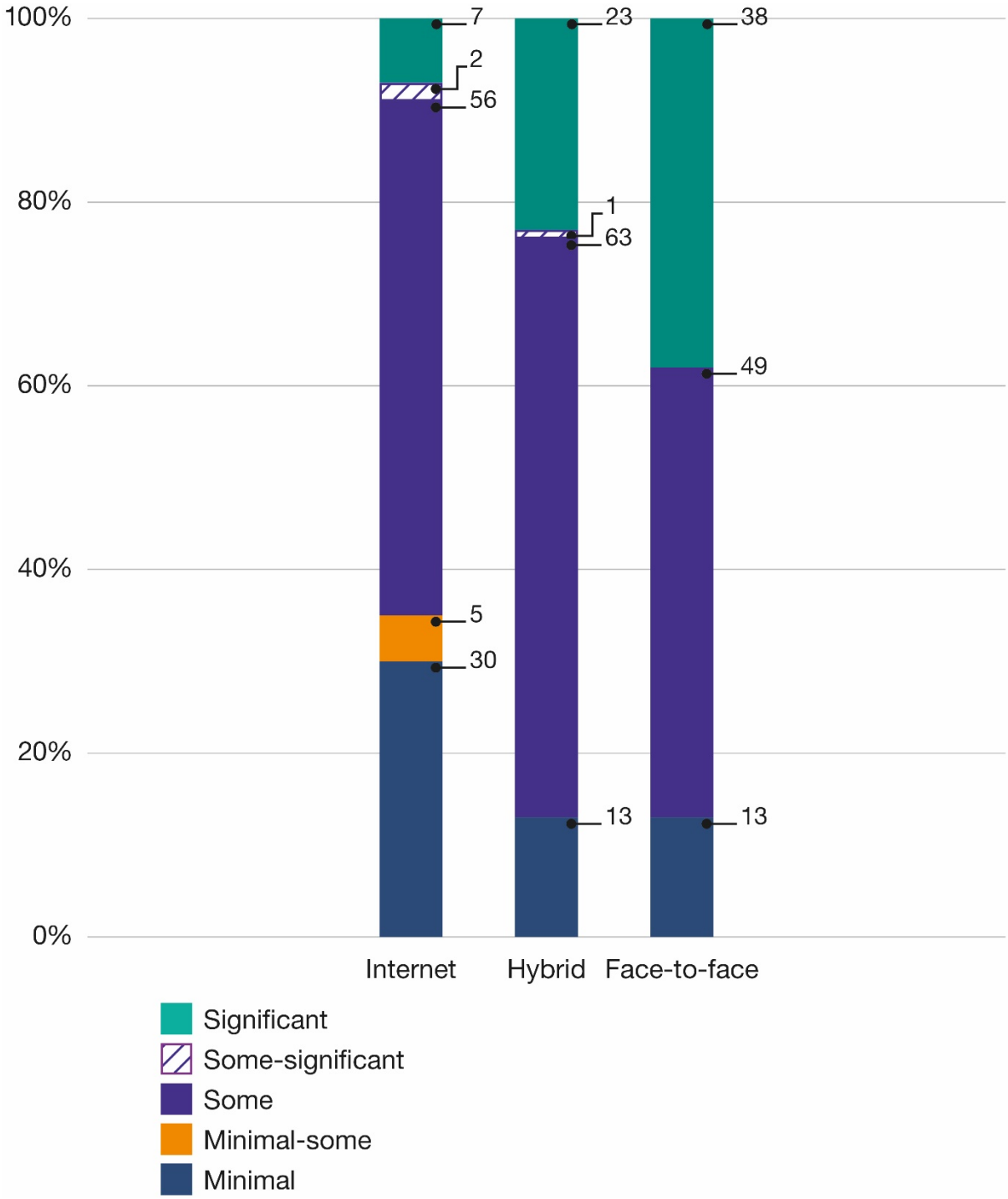
Figure 3. Percentages for overall engagement and intent ratings from the ERG22+ across primary method of radicalisation at time of offending



NB: Statistically significant relationships were found between both overall engagement and intent ratings and primary method of radicalisation at $p < .001$, using the Kruskal-Wallis test.

Percentages for overall capability ratings from the ERG22+ across primary method of radicalisation at time of offending

Figure 4. Percentages for overall capability ratings from the ERG22+ across primary method of radicalisation at time of offending



NB: A statistically significant relationship was found between overall capability ratings and primary method of radicalisation at $p < .001$ using the Kruskal-Wallis test.

Appendix L

ERG22+ Factors and Domains

Table 7. ERG22+ factors and domains

Engagement	Intent	Capability
1. Need to redress injustice and express grievance	14. Over-identification with group, cause or ideology	20 Personal knowledge, skills, competencies
2. Need to defend against threats	15. Them and Us thinking	21. Access to networks, funding, equipment
3. Need for identity, meaning and belonging	16. Dehumanisation of the enemy	22. Criminal history
4. Need for status	17. Attitudes that justify offending	
5. Need for excitement, comradeship and adventure	18. Harmful means to an end	
6. Need to dominate others	19. Harmful end objectives	
7. Susceptibility to indoctrination		
8. Political, moral motivation		
9. Opportunistic involvement		
10. Family and/or friends support extremism		
11. Transitional periods		
12. Group influence and control		
13. Mental health issues		