HM Prison & Probation Service

Exploring the role of the Internet in radicalisation and offending of convicted extremists

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

Ministry of Justice Analytical Series
2021

Preventing victims by changing lives

Her 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 2021

Any enquiries regarding this publication should be sent to us at researchsupport@justice.gov.uk

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

ISBN 978-1-84099-976-1

The authors

Dr Jonathan Kenyon is a BPS Chartered and HCPC Registered Psychologist. He currently works as a National Specialist Lead for Extremist Offending within HMPPS Intervention Services. He recently completed the Doctorate qualification in Forensic Psychology at Nottingham Trent University. His thesis was entitled The Role of the Internet in the Radicalisation Process and Offending of Individuals Convicted of Extremist Offences.

Dr Jens Binder is a Senior Lecturer in 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 HCI 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 **1**

2. Context **3**

2.1 Research aims and questions 4

3. Approach **6**

3.1 Sample 6

3.2 Procedure 8

3.3 Analysis 8

3.4 Limitations 9

4. Results **10**

4.1 Prominence of the Internet in radicalisation over time 10

4.2 Differences in online activity depending on radicalisation pathway 12

4.3 Profile and vulnerability factors depending on radicalisation pathway 14

4.4 Differences in engagement, intent and capability to act depending on radicalisation pathway 16

5. Implications/Conclusions **20**

5.1 Conclusions drawn from study findings 20

5.2 Recommendations for informing counter-terrorism policy and practice 22

References **24**

Appendix A **28**

Note on terminology 28

Appendix B **29**

Variables of interest 29

List of tables

Table 3.1. Basic demographics for the 235 cases included in the analysis 7

Table 4.1. Online activity variables as predictors for pathway group classification 13

Table 4.2. Percentages of profile and vulnerability factors across pathway groups 14

List of figures

Figure 4.1. Percentages and frequencies of cases showing the primary method of radicalisation for ‘Radicalised Extremists’ over time 11

Figure 4.2. Percentages for overall engagement and intent ratings from the ERG22+ across primary method of radicalisation at time of offending 17

Figure 4.3. Percentages for overall capability ratings from the ERG22+ across primary method of radicalisation at time of offending 18

1. Executive Summary

The aim of the study was to establish the role of the Internet in radicalisation[1] processes and offending of those convicted of extremist offences[2] in England and Wales by comparing radicalisation pathways across three groups: those who primarily radicalised online; those who primarily radicalised offline; and those radicalised through both online and offline influences. Four key areas were investigated: first, whether the Internet plays a prominent role in radicalisation; second, whether those taking different radicalisation pathways differ in their internet use; third, whether differences exist in demographic profiles and type of offences committed by those taking different radicalisation pathways; and fourth, whether the pathway taken impacts on professionals' perceptions of risk of committing future violent extremist offences.

Detailed post-conviction assessments were reviewed, which included 267 Extremism Risk Guidance (ERG22+) and two Structured Risk Guidance (SRG[3]) reports. Both the ERG22+ and SRG assessments are risk and need formulation tools intended for use with individuals who have been convicted of any extremist or extremist-related offence. The sample of reports included within the study comprised all that were available on the convicted extremist population in England and Wales from October 2010 to December 2017. 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. Statistical analyses were used to compare all three radicalisation pathway groups.

A key strength of the study was the data-driven approach utilising a unique dataset, with this being the first time that SRG and ERG22+ assessments have been available to those studying the role of the Internet by convicted extremists. This needs to be weighed against several limitations: only the convicted extremist population was represented; there was potential for missing data due to the purpose of these reports, as well as a general disparity in length and detail of reports accessed; and the number of offenders who primarily

---

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

2 Extremist offending is 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).

3 Following independent evaluation (see Webster, Kerr & Tompkins, 2010), the SRG was revised and was formally renamed the ERG22+ in 2011.

radicalised online was comparatively small – all of which should be borne in mind when interpreting findings.

Key findings

During the time period under investigation, up until 2017, the Internet appeared to play an increasingly prominent role in radicalisation processes for those convicted of extremist offences in England and Wales, reflecting general trends of widespread internet use in today's society. The types of websites, platforms and applications used by convicted extremists had changed over time, with a move from using specific extremist websites to open social media platforms.

The internet-related behaviours that were found to contribute most to a differentiation of pathway groups were general online activities relating to extremist activity, namely learning from others online and the use of open social media platforms. More specialised activities, such as the use of encrypted applications, were less predictive, possibly due to their low frequency of occurrence.

In terms of general profile and vulnerability factors, several differences between pathway groups were identified. Those who primarily radicalised online were less likely to be socially connected in the context of the offence and they were more likely to display signs of mental illness or personality disorder, compared against the other two pathway groups. Conversely, those who primarily radicalised offline were more likely to take on the role of attacker and they were less likely to follow an Islamist ideology, compared against the other two pathway groups.

Most importantly, differences were found in assessed levels of 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. Based on the findings of this study, five recommendations for counter-terrorism policy and practice are proposed.

2. Context

The rapid expansion of the Internet within society has led to marked changes in the way individuals communicate, think and live their lives. This has also resulted in new risks relating to the spread of violent extremism and extremist ideologies within communities (Bastug, Douai & Akca, 2018; see Appendix A for terminology used). The extent of internet use promoting radicalisation and terrorism has been described as "…one of the greatest threats that countries including the UK face" (UK House of Commons Home Affairs Committee, 2017, p. 2). Such concerns have been heightened in light of the recent Covid-19 pandemic since early 2020, which has resulted in people spending more time at home and online (UN-CTED, 2020). Whilst these circumstances might have reduced in-person exposure to potentially radicalising peer groups, this increased Internet use may have heightened exposure to radicalising influences online and provided more opportunity to engage in online spaces supportive of terrorism.

Scrivens and Conway (2019) suggest that whilst policymakers and the media have only recently become aware of the extent of Internet use by extremist offenders, many extremist groups and movements have long recognised the power of this medium. New online platforms and tools are used to disseminate extremist material and ideas with the intention these will resonate with supporters and attract new members. Law enforcement and security agencies have focused attention on learning how online discussions, behaviours and actions of those holding extremist views can spill over into the offline sphere, whilst many social media companies are concerned that their platforms are facilitating extremist communications that may promote violent offline activity (Scrivens, Gill & Conway, 2020). Policymakers have expressed concern that increasing levels of internet access, along with wide production and dissemination of extremist content online, may have violent radicalising effects, particularly as this is the aim of those producing such content (Berger & Strathearn, 2013).

Despite these concerns, the role of the Internet in processes of radicalisation has remained difficult to establish. In recent years, academics, practitioners and policymakers have started examining how the Internet influences radicalisation. However, knowledge gaps remain around the specific contribution of the Internet in radicalisation processes, as well as how this facilitates extremist offending. Many are still grappling with the question of to what extent the Internet acts as a replacement for physical interactions and if online networks have the same influence upon an individual as real-world social networks (see Gill et al., 2017). Due to these

knowledge gaps, there is a clear need for further empirical research to test assertions around radicalisation and the Internet's role(s) in it.

This study contributes to filling this gap via its analysis of a unique dataset of 267 Extremism Risk Guidance (ERG22+) reports and two Structured Risk Guidance (SRG) reports compiled on convicted extremists in England and Wales. These reports provide access to assessment ratings by professionals with expertise in extremist offending, including how engaged or identified with an extremist group or cause the individual was at the time of offending, their level of intent to commit violent extremist acts and capability of doing so. Such ratings have not previously been available to researchers studying the role of the Internet in radicalisation and extremist offending and offer fresh insights into this area. Other key strengths include the data-driven approach of this study, particularly as literature relating to online radicalisation is seen as suffering from a general lack of empirical studies (Gill et al., 2015), and scope of the dataset, representing close to the entire convicted extremist population within custody in England and Wales from 2010 to the end of 2017, given all are subject to an ERG22+ within 12 months of sentencing. Also valuable was the variation in cases within the study, including those affiliated with or influenced by a range of causes and ideologies. The sample included males and females of different ages, from a variety of backgrounds, with varying degrees of social connectivity, including lone actors[4] and members of small cells and larger groups. Finally, the inclusion of both non-violent convicted extremists[5] and violent convicted extremists was another key strength as past studies have often focused on those who have committed violent terrorist acts, despite most individuals involved in terrorism committing non-violent acts (Horgan, Shortland, Abbasciano & Walsh, 2016).

2.1 Research aims and questions

If there are different ways that those who commit extremist offences can be radicalised, which for some may include through use of the Internet, this is likely to be shaped or work in concert with other factors, including the characteristics of an individual. Given the lack of data-driven research relating to the Internet's role in radicalisation processes, it is important to explore whether systematic associations exist between primarily online, primarily offline, and hybrid (i.e. those radicalised through both online and offline influences) radicalisation

[4] The HM Government CONTEST strategy report (Revised June 2018) describes lone actors as "associates or members of a terrorist network who are acting autonomously, or those who may be unconnected to any network, but have been influenced by terrorist or extremist propaganda" (HM Government, 2018, p. 17).

[5] Whilst the category 'non-violent' was used within this study to differentiate those convicted of non-violent behaviours, such as dissemination of extremist material, from those convicted of preparing for or committing acts of extremist violence (i.e. 'violent'), it is recognised that these non-violent behaviours may have directly or indirectly contributed to violence committed by others.

pathways and online activity, offender demographics, offence characteristics and ideological context.

There are a number of concerns specific to online radicalisation, including its covert nature, difficulties in detection and potential to facilitate either lone actor or group-based terrorism (see Appendix A for terminology used). At present, it is unclear whether certain online activities and recruitment strategies are more strongly associated with online radicalisation. It has also yet to be established whether males, females, particular age groups, or those inspired by specific ideologies are more likely to radicalise within an online setting. Internet use has previously been found to be particularly prevalent for lone actors (Kenyon, Baker-Beall & Binder, 2021), but it is less clear how this compares with other types of extremist offender given widespread internet use in today's society.

There is a need to establish whether online radicalisation typically results in violent offline activity or whether offences are more likely to be of a virtual nature (e.g. dissemination of extremist materials online). If the Internet does contribute to radicalising individuals to support terrorism and extremist ideologies associated with terrorist groups, this knowledge should assist counter terrorism agencies in terms of negating the messages and tactics used. In addition, there is a need to discover whether online radicalisation is associated with higher or lower levels of engagement, intent and capability to commit violent extremist offences when compared with other radicalisation pathways. This knowledge will assist professionals working with individuals who have committed extremist violence and support rehabilitative efforts.

To test for these associations, this study investigated whether:

1. The Internet plays a prominent role in radicalisation for those convicted of extremist offences
2. The radicalisation pathway is related to the way in which those convicted of extremist offences use the Internet
3. There are differences in offender demographics and offence-type variables when radicalisation pathways are compared
4. The radicalisation pathway has an impact on an offender's levels of engagement to an extremist group, cause or ideology, along with their levels of intent and capability to perpetrate violent extremist acts.

3. Approach

3.1 Sample

The data source consisted of 267 Extremism Risk Guidance (ERG22+)[6] reports and two Structured Risk Guidance (SRG) reports (the predecessor to the ERG22+). Since September 2011, the ERG22+ has been used throughout prisons and probation services in England and Wales to assess individuals convicted of extremist offences. Recent studies have found the ERG22+ to be a promising risk and need formulation tool for use with extremist offenders having examined the construct validity and internal consistency of the measure (Powis, Randhawa & Bishopp, 2019), with inter-rater reliability ranging from perfect to moderate (Powis, Randhawa-Horne, Elliott & Woodhams, 2019). Within this study, the report subjects were individuals convicted of extremist or extremist-related offences in England and Wales. Only initial ERG22+ reports were included within the study, as these are typically completed within 12 months of sentencing and feature assessment of all cases based on the time of offending. These reports included all available to the Ministry of Justice (MoJ) completed from October 2010 to the end of December 2017. Report authors were either Registered Psychologists or qualified Probation Officers, who had undertaken the standardised two-day national training to learn how to conduct the assessment. These authors had access to a number of restricted information sources, including direct interviews with the offender in many cases when compiling the reports. The average length of reports was 20 pages, the longest comprising 146 pages and the shortest four pages.

As the focus of this study was on the role of the Internet in radicalisation processes and offending of convicted extremists, the analysis centred on those considered to be 'Radicalised Extremists'[7] prior to coming into custody. The SRG and ERG22+ are formulation-guided assessments where the author provides a narrative account of an individual's pathway to extremist offending. Identifying when the development of extremist beliefs occurred could therefore be determined by first-hand accounts within the report or by the author's perception based on their access to official and restricted documentation (see Appendix B for coding criteria and variable definitions). Where sufficient evidence existed within the report to determine the radicalisation pathway based on internet use, individuals

[6] The Extremism Risk Guidance (ERG22+) is a Structured Professional Judgement (SPJ) tool; a formulation guided assessment to help inform overall decisions about risk and identify areas of treatment need for people who have committed extremist offences (see Lloyd & Dean, 2015 for further information on the ERG22+).

[7] '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).

were categorised into one of three groups, consistent with those utilised in previous research (Reinares, Garcia-Calvo & Vicente, 2017):

- Primarily radicalised online ('Internet' group)
- Radicalised through a combination of online and offline influences ('Hybrid' group)
- Primarily radicalised offline ('Face to face' group)

Of the 248 'Radicalised Extremists' within the dataset, the radicalisation pathway could be identified in 235 cases (95%), and subsequent analysis focused on these cases specifically. 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 provided by the author to explain the individual's pathway to offending (see Appendix B for examples of how individuals were categorised into pathway groups). The basic demographics for the 235 cases are detailed in Table 3.1.

Table 3.1. Basic demographics for the 235 cases included in the analysis

Demographic		Percentage (%)
Gender	Male	90
	Female	10
Age[a] (at time of sentencing)	Mean age = 29, Range = 17–63	-
	Up to and including 25	42
	Over 25	58
Place of birth[b]	UK	73
	Non-UK	27
Ideology/cause	Animal Rights	7
	Extreme Right Wing	11
	Islamist Extremist	76
	Other Political	6

[a] Based on 233 cases as age at time of sentencing could not be identified in two cases

[b] Based on 224 cases as place of birth could not be identified in 11 cases

3.2 Procedure

Each report was manually reviewed by the lead researcher to develop a comprehensive coded data set.[8] This involved examining every report and extracting variables of interest by coding information relevant to internet activities and behaviours commonly associated with online radicalisation (see Gill & Corner, 2015; Gill, Horgan & Deckert, 2014; Gill et al., 2017; Whittaker, 2021), demographic and offence-type variables, along with overall engagement, intent and capability ratings (for a full description of variables and how they were coded, see Appendix B). Based on this first examination, a coding frame was drafted that included definitions for each variable, with instructions and examples of how to apply the coding frame consistently.

The drafted coding frame was further refined and verified in a process similar to previous research (e.g. Moreno, Egan & Brockman, 2011). The lead researcher applied the coding to all reports. To ensure consistency and ease of use of the coding frame, two other coders[9] independently coded all variables of interest for a selection of test cases. All three coders then collaboratively reviewed coding of test cases, and where differences were apparent, resolved these through discussion and reaching a consensus. Based on the discussion, the coding frame was then modified to strengthen variable definitions and examples, and the lead researcher used the modified instrument to finalise codings.

3.3 Analysis

A quantitative research design was used involving analysis of coded information within the dataset. The three radicalisation pathway groups were first compared in relation to their prominence over time, then subsequent analyses were clustered to compare these groups in terms of online activities, demographics and offence-type variables, and overall engagement, intent and capability ratings.

Relative frequencies and percentages of all variables of interest were compared for each radicalisation pathway group. Pearson's chi-squared tests were conducted where possible to test for statistically significant relationships between pathway groups and variables of interest. Fisher's exact test was used as an alternative to chi-squared tests where the statistical assumptions for the latter were not met. Binary logistic regression analysis was

---

8 The study received ethical approval from the College Research Ethics Committee at Nottingham Trent University and approval from the National Research Committee (NRC) as the data related to convicted offenders incarcerated in England and Wales.

9 These additional coders were supervisors and university lecturers, with ongoing involvement in the research project and familiarity with quantitative coding procedures.

used to test whether any coded internet behaviour variables could predict pathway group classification, including establishing which were the strongest predictors. The Kruskal-Wallis test was used to determine whether any statistically significant differences existed between pathway groups in relation to overall ratings of engagement, intent and capability at time of offending from the ERG22+ assessments.

3.4 Limitations

There are seven limitations of the study that are important to highlight. First, direct interviewing of convicted extremists or professionals managing cases would likely have resulted in further insights into online activities, especially as internet use is a private activity for most people. The majority of past research in this area has relied on case information from open-source media to draw conclusions and whilst a handful of studies have included interviews with convicted extremists (e.g. Koehler, 2014; Von Behr et al., 2013), additional interview data are likely to increase knowledge and develop the evidence base further. Second, some individuals who committed extremist offences in England and Wales were not included within the sample, such as those who died during the commission of offences, those acquitted at trial and those who were never identified and/or apprehended by the police. Third, there were difficulties distinguishing between missing data and variables that could reliably be coded as not present. This was particularly evident when coding for a range of online behaviours and overcome by coding dichotomously using options of 'Yes' and 'No evidence'. Given the purpose of the SRG and ERG22+ reports was not to provide detailed accounts of all internet behaviours engaged in by individuals, it is possible some online activities may not have been reported and therefore aspects of internet use were missed. Fourth, the reports from which data were obtained varied in length and detail, providing another reason why some may not have covered all online behaviours, even where relevant. Fifth, some information relating to radicalisation pathways and internet use may have been lost, particularly as 23 per cent of convicted extremists decided against contributing to the completion of reports by partaking in interviews. There is also the possibility that those who were interviewed were not always honest with their disclosures. Sixth, the smaller number of non-Islamist extremist offenders should be recognised as a limitation as they made up only 24 per cent of the sample. For this reason, some additional caution is required in generalising the findings of this study to these other ideological groups or causes. Seventh, whilst assessors are encouraged to rate overall levels of intent and capability with consideration to the offender committing an extremist offence likely to cause serious and significant harm, it is possible some assessors may have rated these domains on the basis of the offender committing offences similar to their index offences, which may have been classified as 'non-violent' within this study.

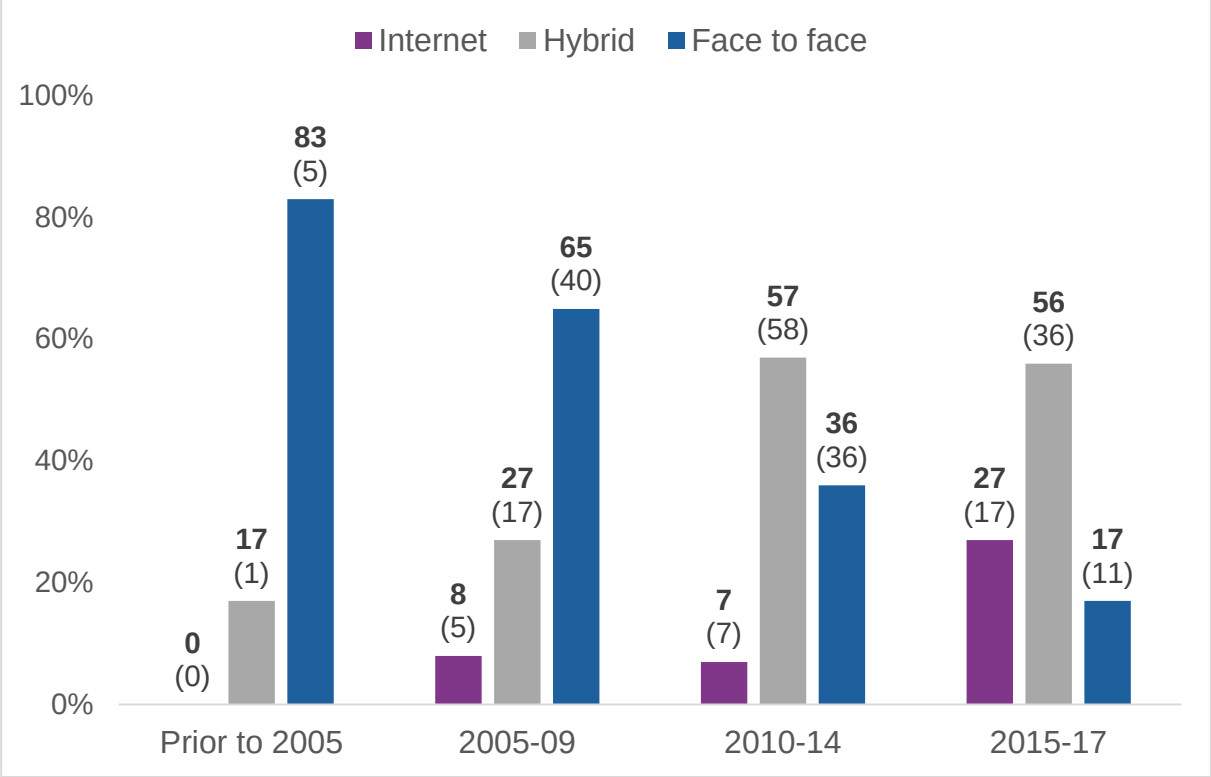
4. Results

4.1 Prominence of the Internet in radicalisation over time

The role of the Internet was found to be increasingly prominent in the radicalisation of convicted extremists in England and Wales. In the period from 2005 to 2017, there was an increase in the number of extremist offenders who were subject to some degree of online radicalisation, including those who primarily radicalised online and those who radicalised through a combination of online and offline influences (83% in 2015–17, 64% in 2010–14, 35% in 2005–09), whilst over the same period, a reduction was observed in the number who were primarily radicalised though offline influences, including face-to-face contact with others (17% in 2015–17, 36% in 2010–14, 65% in 2005–09, see Figure 4.1). This reflects the increase in online activity by society generally, where self-reported internet usage among adults has increased from 12.1 hours per week in 2007 to 24 hours per week in 2017. Furthermore, 22 per cent of all adult internet users reported having a social media account in 2007, in contrast to 77 per cent in 2017 (Ofcom, 2018). Therefore, in the same way the Internet has brought extensive changes to people's lives by revolutionising communication with each other, it also appears to be playing an increasingly prominent role in the way in which radicalisation is occurring.

Both gender and age were categories that showed marked changes over time. The Internet was found to have played an increasingly prominent role in the radicalisation of both males and females, along with younger and older individuals, since 2005. This increase was most marked for females (75-percentage point increase of cases from 2005 to 2017 where internet use was reported to have contributed to radicalisation) and members of the younger generation (54-percentage point increase of cases from 2005 to 2017 where internet use was reported to have contributed to radicalisation).

Figure 4.1. Percentages and frequencies of cases showing the primary method of radicalisation for 'Radicalised Extremists' over time



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

Despite evidence suggesting an increasingly prominent role of the Internet in radicalisation processes, it cannot be concluded that the online domain is simply replacing the offline domain as offline influences featured at least to some extent for most convicted extremists within the dataset. The pathway group with the most individuals were those radicalised through both online and offline influences (48%). This finding supports the assertion by Gill, Corner, Thornton and Conway (2015) that a distinction between online and offline radicalisation is a "false dichotomy" and "plotters regularly engage in activities in both domains" (p. 35). This also supports the findings by Whittaker (2021) that whilst those in his sample of 231 U.S. based Islamic State terrorists had overwhelmingly used the Internet, strong relationships existed between online and offline learning and planning behaviours, leading to the conclusion that terrorists tend to operate across both domains.

The types of websites, platforms and applications used by convicted extremists were found to have changed over time. For those who primarily radicalised online and those who radicalised through both online and offline influences, there was a reduction in the number of individuals using specific extremist websites from 2005 onwards (60 and 83-percentage point

decrease respectively from 2005 to 2017). Across the same period, there was an increase in the number of individuals using open social media platforms (36 and 57-percentage point increase respectively). There was also evidence of increased use of encrypted applications online, particularly around 2015–17, but this increase was most marked for those radicalised through both online and offline influences (25-percentage point increase from 2010 to 2017). According to Scrivens and Conway (2019), this increased use of encrypted applications coincided with the time when disruption of pro-Daesh accounts by major social media companies was taking place (including Facebook, Twitter and YouTube), which forced many extremists off these platforms and towards use of encrypted applications such as Telegram, which became their platform of choice around 2016–17.

The increased prominence of use of open social media platforms by convicted extremists found within this study provides support for the assertion by Bastug et al. (2018) that social media platforms are "a very important radicalising agent" (p. 16). These findings are also consistent with those of Jensen, James, LaFree, Safer-Lichtenstein and Yates (2018) who found the use of social media by U.S. terrorists had increased from around 25 per cent in 2005–10 to 75 per cent by 2011–16. This increased use of open social media platforms demonstrates that those radicalised and subsequently convicted of extremist offences are regularly using online applications that are both familiar to and regularly accessed by the general public. For this reason, it is very important that social media and technology companies take some responsibility in efforts to prevent online radicalisation by working together, blocking dissemination of extremist content on their platforms and protecting users from harmful content.[10]

4.2 Differences in online activity depending on radicalisation pathway

Statistically significant associations were found when comparing radicalisation pathway groups across online activities (learning from online sources, interaction with co-ideologues online, dissemination of extremist propaganda online) and use of sites and applications (extremist websites/home pages, open social media platforms, standard chat applications, encrypted chat applications).

[10] A number of key providers do have policies in place, such as Facebook's policy against Dangerous Individuals and Organizations (https://www.facebook.com/communitystandards/recentupdates/dangerous_individuals_organizations) and Twitter's Violent Organizations policy (https://help.twitter.com/en/rules-and-policies/violent-groups).

When comparing extremist offenders who had primarily radicalised offline with those where the Internet was relevant to the radicalisation pathway (i.e. those who primarily radicalised online and those radicalised by a combination of online and offline influences), the only two statistically significant predictors were found to be whether individuals had learnt from online sources and whether they had used open social media platforms (see Table 4.1).

Table 4.1. Online activity variables as predictors for pathway group classification

Predictor	B	SE(B)	Odds Ratio
Learnt from online sources	6.36***	1.06	575.19 [72.42, 4568.54]
Interact with co-ideologues online	1.61	1.27	4.98 [0.42, 59.40]
Generate own extremist propaganda online	-0.78	1.07	0.46 [0.06, 3.72]
Provision of material support	1.33	1.27	3.80 [0.32, 45.82]
Use of extremist websites/home pages	0.67	0.73	1.94 [0.46, 8.19]
Use of open social media platforms	2.75*	1.10	15.61 [1.81, 134.82]
Use of standard chat applications	0.68	1.18	1.98 [0.20, 19.77]
Use of encrypted applications	0.53	0.10	1.70 [0.07, 42.87]

NB: Logistic regression coefficients predicting radicalisation online (coded as 1) and radicalisation offline (coded as 0). ***significant at $p < .001$, *significant at $p < .05$. Numbers in parentheses refer to 95% confidence intervals.

As seen in Table 4.1, for those extremist offenders who learnt from online sources, the odds of either having primarily radicalised online or through a combination of online and offline influences were 575 times greater than having primarily radicalised offline. This was not surprising given that only 16 per cent of those who primarily radicalised offline reported this online activity, compared to 98 per cent across the other two pathway groups. For those extremist offenders who used open social media platforms, the odds of either having primarily radicalised online or through a combination of online and offline influences were close to 16 times greater than having primarily radicalised offline.

Follow-up analyses comparing extremist offenders who primarily radicalised online with those who primarily radicalised offline also found the only two statistically significant predictors were whether individuals had learnt from online sources ($B = 5.08$, $SE = 1.36$, $OR = 160.97$, 95% CI [11.19, 2315.34], $p < .001$) and whether they had used open social media platforms ($B = 3.56$, $SE = 1.25$, $OR = 35.21$, 95% CI [3.03, 408.69], $p < .01$). No significant predictors were found when comparing those who primarily radicalised offline with those radicalised through both online and offline influences.

When further comparing those who primarily radicalised online with those radicalised through both online and offline influences, similarities were found in their online activities. However, these pathway groups could still be differentiated as a higher percentage of those who primarily radicalised online used the Internet to interact with like-minded others (76% compared to 49%), disseminate their own extremist propaganda (62% compared to 32%) and access open social media platforms (66% compared to 40%). This may reflect that those who primarily radicalised online tended to be more socially isolated offline in the context of their offending and therefore relied more heavily on an online community, particularly via open social media platforms. Those who radicalised through both online and offline influences tended to have rates between the other pathway groups for online activities.

As could be expected, those who primarily radicalised offline had the lowest rates for online activities, using the Internet less often for extremist purposes. However, a sizable minority (42%) of individuals in this pathway group had still used the Internet to some extent for extremist purposes, highlighting the growing influence of the online medium in radicalisation processes and extremist offending generally.

4.3 Profile and vulnerability factors depending on radicalisation pathway

Extremist offenders within each radicalisation pathway group were found to be markedly different in terms of their demographic profile, offending history and socialisation (see Table 4.2). This finding provides support for the notion that no single profile exists for those who commit extremist offences (Borum, 2004; Horgan, 2003; Silke, 2014).

Table 4.2. Percentages of profile and vulnerability factors across pathway groups

Profile and vulnerability factors (n = 235 unless specified)		Internet (n = 29) Percentage (%)	Hybrid (n = 113) Percentage (%)	Face to face (n = 93) Percentage (%)
Age at sentencing**	Up to + including 25	52	51†	28†
	Over 25	48	49†	72†
Gender	Male	79	94	88
	Female	21	6	12
Place of birth (n = 224)	UK	78	72	72
	Non-UK	22	28	28
Prior offending history (n = 233)**	Yes	28	29†	51†
	No	72	71†	49†

Profile and vulnerability factors (n = 235 unless specified)		Internet (n = 29) Percentage (%)	Hybrid (n = 113) Percentage (%)	Face to face (n = 93) Percentage (%)
Presence of mental illness/personality disorder[11] (n = 229)*	Strongly present	25†‡	7‡	5†
	Partly present	4	10	5
	Not present	71	83	89
Violent/non-violent offence**	Violent	21	33†	49†
	Non-violent	79	67†	51†
Role in offence**	Attacker	21‡	33†	49†‡
	All other roles	79‡	67†	51†‡
Degree of social connection (n = 233)***	Lone	63†‡	6‡	3†
	Small cell (2–3)	19	12	8
	Group	19†‡	82‡	89†
Ideology***	Islamist extremist	86‡	86†	61†‡
	All other ideologies	14‡	14†	39†‡

NB: Chi-squared tests were used for overall associations, except for presence of mental illness and degree of social connection where Fisher's exact test was used due to low expected cell count. **significant association with radicalisation pathway at $p < .01$. ***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.

As indicated in Table 4.2, statistically significant associations were found between some profile and vulnerability factors and primary method of radicalisation. The percentages show a general similarity between the two pathway groups that involve some online aspect: those who primarily radicalised online and those who radicalised through a combination of online and offline means. Both these groups contrast to the group that primarily radicalised offline. Whilst a recognised caveat is the varying sample sizes across the three pathway groups (with the smallest group consisting of 29 individuals considered to have primarily radicalised online), post hoc tests allow for some detailed characterisation as follows.

Those found to have radicalised by both online and offline influences were more likely to be younger, to be without a history of prior offending, and to be convicted of non-violent extremist offences (e.g. disseminating extremist materials online) when compared to those who primarily radicalised offline. Further, those who primarily radicalised offline were more likely to have taken the role of an attacker, including those who directly committed an extremist attack on another person or property and those convicted on the basis they would have done had they not been arrested/disrupted, compared to the other pathway groups.

[11] The corresponding ERG22+ factor includes serious cognitive and intellectual impairments; psychotic disorders; major mood disorders and personality disorders. These impairments or disorders should be diagnosed according to an official nosological system or standardised assessment (HM Prison and Probation Service, 2019).

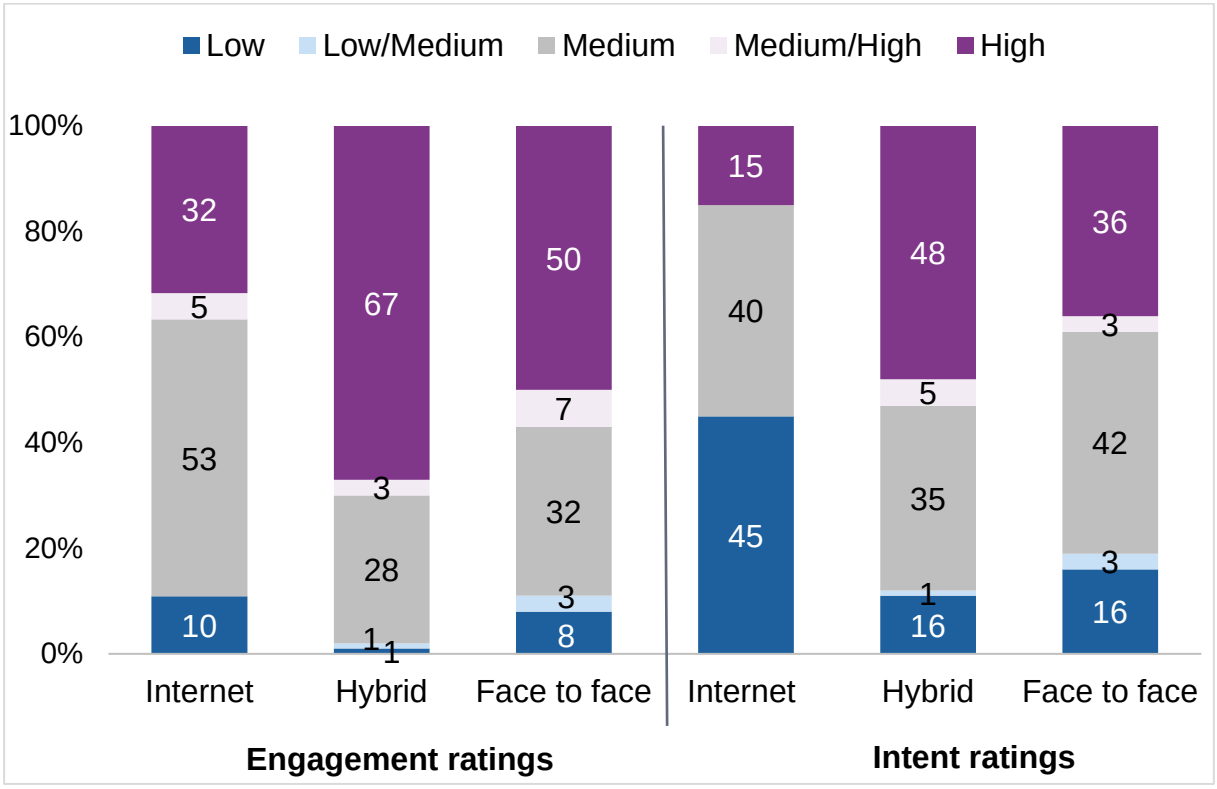
Those who primarily radicalised offline were also less likely to follow an Islamist extremist ideology than those who primarily radicalised online and those who radicalised through a combination of online and offline influences.

The degree of social connection and the presence of mental illness or personality disorder were found to be the two characteristics that set apart those who primarily radicalised online from the two other pathway groups. Those who primarily radicalised online were more likely to be classed as lone (63%) and less likely to have wider connections within a group (19%) as compared to the other two pathway groups where group connections were found to play a role in more than 80% of all cases. Furthermore, those who primarily radicalised online were more likely to show strong presence of mental illness or personality disorder in their reports (25%) when compared to the other two pathway groups with signs of strong presence in less than 10% of all cases. Finally, no significant differences between the pathway groups were found for gender and country of birth.

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

The three radicalisation pathway groups differed in terms of ratings of overall engagement with an extremist group, cause or ideology, along with overall intent and capability ratings to commit violent extremist offences from the ERG22+ at the time of offending. Percentages for overall engagement and intent ratings across each pathway group are displayed in Figure 4.2.

Figure 4.2. Percentages for overall engagement and intent ratings from the ERG22+ across primary method of radicalisation at time of offending



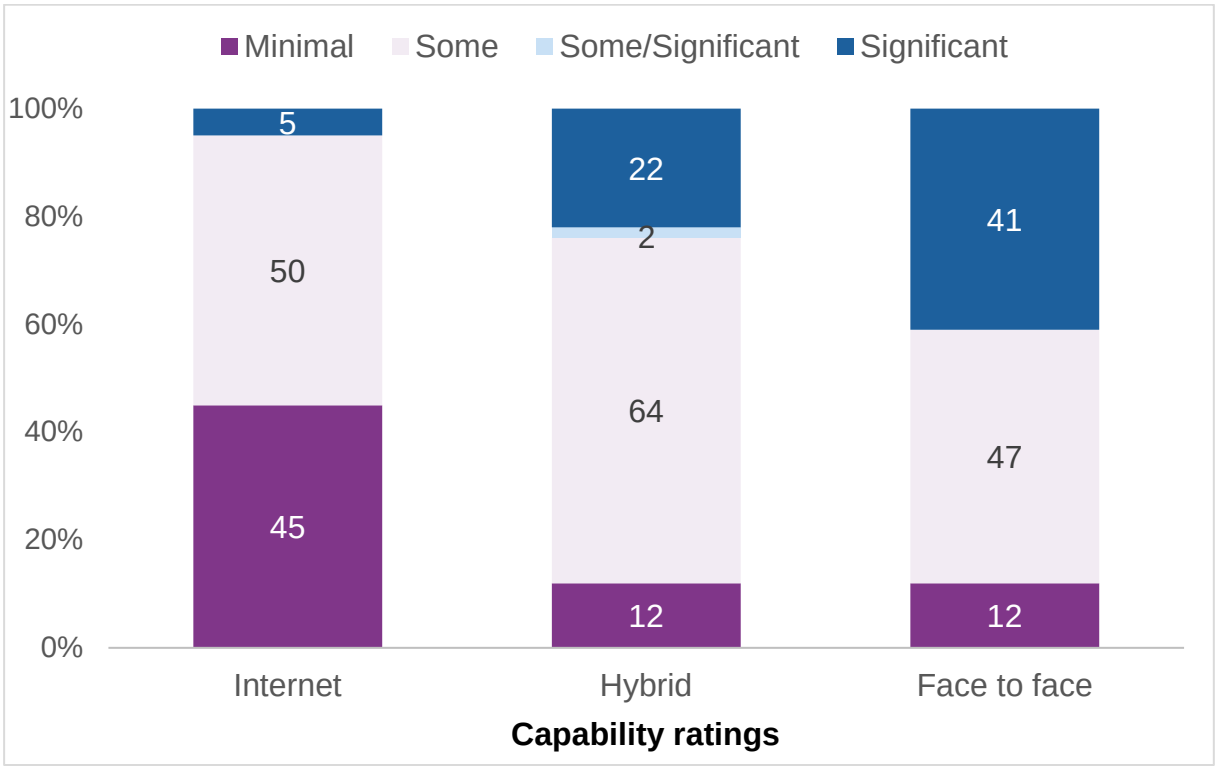
NB: Statistically significant relationships were found between overall engagement ratings and primary method of radicalisation, and overall intent ratings and primary method of radicalisation, both at $p < .01$, using the Kruskal-Wallis test.

As indicated in Figure 4.2, those who primarily radicalised online were found to have the lowest overall engagement levels. As the engagement domain refers to factors that may account for an individual's involvement and growing identification with an extremist group, cause or ideology, this indicates that those subject to online radicalisation appear less involved or identified than those who have taken other radicalisation pathways. This may reflect that some individuals who primarily radicalised online were apprehended at an earlier stage during radicalisation, after breaking the law by perhaps accessing or sharing extremist content online, but before making contact with others offline or taking violent action in an offline setting. In contrast, those radicalised by a combination of online and offline influences were found to have the highest overall engagement levels. This suggests they were perhaps further along the processes of radicalisation, but also highlights the important role of offline contact with other extremists in strengthening involvement and deepening a sense of identity with an extremist group, cause or ideology.

Those considered to have primarily radicalised online were found to have the lowest overall levels of intent. 'Intent' refers here to those 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. It appears that contact with other extremists in an offline setting plays a crucial role in moving an individual from holding extremist views and taking an interest in a specific group, cause or ideology, to becoming more willing or prepared to offend on their behalf. This was reflected by the finding that those radicalised by both online and offline influences had the highest overall levels of intent. It is also possible the combination effect of being exposed to extremist views in both an online and offline setting is more powerful than exposure to offline influences alone, given that those who primarily radicalised offline were found to have lower overall levels of intent in comparison. A possible interpretation is that more intense online socialising occurred for those radicalised through both online and offline influences, as the more substantial online exchanges led to coordinating concerted offline action, even if only to arrange offline meetings with each other. It would follow that those receiving the highest level of exposure to extremist ideas would be engaging with such content within both the online and offline domains. This high level of exposure is likely to increase the extent to which such ideas are reinforced and increase the likelihood of this leading to an individual over-identifying with an extremist group or cause. This may explain why extremist offenders within this radicalisation pathway group had the highest engagement and intent ratings.

Figure 4.3. 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 $p < .01$ using the Kruskal-Wallis test.

As with overall ratings of engagement and intent, those who primarily radicalised online were found to have the lowest levels of capability, as indicated in Figure 4.3. The capability domain refers to those factors that enable an individual to cause harm, offend or perpetrate violence on behalf of a group, cause and/or ideology. Those who primarily radicalised offline were found to have the highest overall levels of capability, suggesting the significance of offline contacts in providing individuals with the necessary knowledge, skills and networks to take violent action in support of an extremist group or cause.

Christmann (2012) argued that face-to-face contact remains important to recruitment and the group dynamics that can drive radicalisation, especially that which leads to violence. This may explain higher ratings across the domains of engagement, intent and capability for those who primarily radicalised offline and through a combination of online and offline influences, compared with those who primarily radicalised online. Corner and Gill (2015) found that individuals who engaged in internet activities, such as interacting virtually with co-ideologues, were less likely to carry out violent attacks, and those who engaged in online learning were less likely to kill or injure others in the commission of their offending. Reynolds and Hafez (2019) also found that offline social networks played a stronger role in mobilisation than online radicalisation in their study of German foreign fighters. One possible explanation is that groups tend to not only support the process of moral disengagement but also provide the necessary operational capabilities to carry out terrorist attacks. Therefore, in the absence of a group setting, violent extremist acts can be more difficult to commit for practical and psychological reasons (Gill, 2012).

5. Implications/Conclusions

5.1 Conclusions drawn from study findings

The findings from this study have provided insights into the role of the Internet in radicalisation processes and extremist offending, along with insights into wider trajectories towards extremist offending more generally. The Internet appears to be playing an increasingly prominent role in radicalisation processes of those convicted of extremist offences in England and Wales. From 2005 to 2017, the number of convicted extremists in the sample who were subject to online radicalisation had increased, whilst a reduction was observed in the number of those primarily subject to radicalising influences in offline settings over the same time period. This is seen to reflect general trends in society relating to the widespread use of the Internet. The findings from this study supported the notion that younger individuals and females in particular now have opportunities to engage with extremist groups and causes online in a way that was more difficult previously. This also mirrors general societal trends, with those in the 16–24 age group self-reporting the highest volume of weekly internet use and females reporting being more likely to have a social media profile/account than males (Ofcom, 2018).

Whilst this study only featured cases convicted up to 2017, it is expected that the Internet will have continued to increase in prominence since this time, particularly in light of the Covid-19 pandemic where people are spending more time online than ever before, coupled with the reduced opportunities for face-to-face contact with others. However, there is a lack of evidence to suggest the online domain is replacing the offline domain, as offline influences featured at least to some extent for most individuals within the dataset. As most individuals who commit extremist offences had a tendency to operate across both domains, this provides support for Gill et al.'s (2015) assertion that a distinction between online and offline radicalisation is a "false dichotomy" (p. 35). It is also clear that the way in which extremist offenders use the Internet has changed over time, which is again consistent with general trends across wider society. In particular, there appears to be less reliance on specific extremist websites and more on open social media platforms across the period 2005 to 2017. Such changes demonstrate the constantly adapting threat of online radicalisation and associated difficulties faced by those trying to counter this threat.

Differences are apparent in both the way and extent to which those following different radicalisation pathways engage with the Internet as a tool for extremist purposes. The two online activity predictors able to differentiate between individuals where the Internet was relevant to their radicalisation pathway from those who primarily radicalised offline included

whether they had learnt from online sources and whether they used open social media platforms within their extremist activities. Similarities were found in online activities between those who primarily radicalised online and those who were radicalised by both online and offline influences, yet these pathway groups could still be differentiated as those who primarily radicalised online had a greater tendency to interact with like-minded others, disseminate their own extremist propaganda and access open social media platforms. This may be due to them being more socially isolated offline and relying more heavily on an online community, particularly through open social media platforms.

The typical profile of individuals following different radicalisation pathways was found to differ, supporting the notion that there is no single profile for an extremist offender. Whilst a general similarity was found between the two pathway groups involving some online aspect, the degree of social connection and the presence of mental illness or personality disorder were two characteristics that clearly set apart those who primarily radicalised online from the other two pathway groups. In contrast, extremist offenders who primarily radicalised offline were the most likely to have assumed the role of an attacker compared to the other pathway groups and were also found to be less likely to adhere to an Islamist extremist ideology.

Perhaps most interesting of all is that the radicalisation pathway appears to impact on the extent to which individuals engage with an extremist group or cause, their level of intent to commit violence on behalf of the cause and their capability of doing so. Whilst the role of the Internet is clearly growing in prominence, face-to-face human contact appears to still play an important role in driving deeper levels of radicalisation, including that leading to a willingness to commit violent action. The differences across levels of engagement, intent and capability when comparing pathway groups does suggest there is value in demarcating those who have primarily radicalised online from those exposed to offline influences. This finding in particular provides insight into how monitoring and risk management strategies should be tailored to the varying radicalisation pathways of different individuals.

Finally, and importantly, the findings of this data-driven study, using a unique dataset of specialist assessment reports by professionals working directly with convicted extremists, largely accord with what is known from an existing literature base that has generally relied upon open-source data or small numbers of case studies to draw conclusions. In terms of future directions for research, adding more cases to this existing dataset from reports completed in 2018 onwards is likely to offer new insights given the rapid evolution of Internet technology development and take-up. In addition, whilst a handful of previous studies have featured interviews with convicted extremists focusing on internet use, further interviews with

current or former extremists is likely to take us one step closer to a more holistic triangulation of data. This will help researchers and policy-makers obtain a more complete understanding of the role of the Internet in radicalisation processes and extremist offending.

5.2 Recommendations for informing counter-terrorism policy and practice

Based on the findings from this study, five recommendations are proposed to inform future counter-terrorism policy and practice:

1. Whilst the Internet appears to be playing an increasingly prominent role in radicalisation processes, offline influences featured at least to some extent for most cases, suggesting extremist offenders generally operate across both domains. To reflect this, security services and counter-terrorism initiatives should continue to target the Internet as a setting where extremist socialisation can occur, but not at the expense of paying attention to environmental interactions offline.
2. New online counter-terrorism measures should aim to target younger users and appeal not just to males, but also to females, given the particularly marked increase in prominence of the Internet in radicalisation for these groups.
3. Given that those who primarily radicalised online tended to be socially isolated offline with higher rates of mental illness and personality disorder, once vulnerable individuals have been identified online, it is important their wider needs are considered as opposed to focusing solely on interventions to address an increasingly extremist mind-set. In particular, those who appear vulnerable to online radicalisation may benefit from initiatives designed to increase their support network and access to social opportunities to reduce feelings of social isolation. These individuals may also require referral to and support from specialist mental health and/or personality disorder services.
4. Further work should determine how radicalisation pathways can inform treatment of extremist offenders during rehabilitation efforts within custodial and community settings. The differences found in engagement, intent and capability ratings between radicalisation pathway groups provide a more nuanced understanding to potentially inform decisions on appropriate response measures. For example, those who have primarily radicalised online and considered less engaged may benefit from interventions that help them get back to a more meaningful life through focusing on positive approach goals. In contrast, those who are considered highly engaged through online and offline influences may require more intensive rehabilitation efforts, including that which specifically addresses extremist beliefs/ideology.

5. ERG22+ assessors should have up-to-date knowledge around the role of the Internet in radicalisation processes and extremist offending given the increasingly prominent role of the Internet in radicalisation processes. This includes awareness of literature around extremists' online behaviours and familiarity with changes in the way the online space is being used (e.g. the types of platforms/applications favoured, how these platforms/applications work and how they are being used). This should help assessors develop a fuller understanding of how individuals come to be engaged with an extremist group or cause, along with greater knowledge around their capabilities for committing extremist offences in the future.

References

Bastug, M. F., Douai, A. and Akca, D. (2018) Exploring the “demand side” of online radicalization: Evidence from the Canadian context. *Studies in Conflict and Terrorism,* 1–22.

Berger, J. M. and Strathearn, B. (2013) *Who matters online: Measuring influence, evaluating content and countering violent extremism in online social networks*. Kings College London: ICSR. Retrieved from http://icsr.info/wp-content/uploads/2013/03/ICSR_Berger-and-Strathearn.pdf

Borum, R. (2004) *The psychology of terrorism*. University of South Florida.

Christmann, K. (2012) *Preventing religious radicalisation and violent extremism: A systematic review of the research evidence.* Retrieved from https://www.safecampuscommunities.ac.uk/uploads/files/2016/08/yjb_preventing_violent_extremism_systematic_review_requires_uploading.pdf

Corner, E. and Gill, P. (2015) A false dichotomy? Mental illness and lone-actor terrorism. *Law and Human Behavior, 39*(1), 23–34.

Gill, P. (2012) Terrorist violence and the contextual, facilitative and causal qualities of group-based behaviors: A case study of suicide bombing plots in the United Kingdom. *Aggression and Violent Behavior, 17*(6), 565–74.

Gill, P. and Corner, E. (2015) Lone-actor terrorist use of the Internet and behavioural correlates. In *Terrorism online: Politics, law, technology and unconventional violence*, L. Jarvis, S. Macdonald and T. Chen (eds.). London: Routledge.

Gill, P., Corner, E., Thornton, A. and 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.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M. and Horgan J. (2017) Terrorist use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes. *Criminology and Public Policy, 16*(1), 99–117.

Gill, P., Horgan, J. and Deckert, P. (2014) Bombing alone: tracing the motivations and antecedent behaviors of lone-actor terrorists. *Journal of Forensic Science, 59*(2), 425–435.

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). Intervention Services (Internal document).

HM Government (2018) *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (Revised June 2018). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714402/060618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.PDF

Horgan, J. (2003) The social and psychological characteristics of terrorism and terrorists. In T. Bjorgo, (Ed.) *A forerunner to fighting terrorism for humanity: A conference on the roots of evil*. New York. Norwegian Institute of International Affairs and Norwegian Ministry of Foreign Affairs.

Horgan, J., Shortland, N., Abbasciano, S. and Walsh, S. (2016) Actions speak louder than words: A behavioural analysis of 183 individuals convicted for terrorist offenses in the United States from 1995 to 2012. *Journal of Forensic Sciences 61*(5), 1228–1237.

Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A., and Yates, E. (2018) The use of social media by United States extremists. *National Consortium for the Study of Terrorism and Responses to Terrorism*. Retrieved from https://www.start.umd.edu/publication/use-social-media-united-states-extremists

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

Koehler, D. (2014) The radical online: Individual radicalization processes and the role of the Internet. *Journal for Deradicalization 1*, 116–134.

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

Moreno, M. A., Egan, K. G. and Brockman, L. (2011) Development of a researcher codebook for use in evaluating social networking site profiles. *Journal of Adolescent Health, 49*(1), 29–35.

Ofcom (2018) *Adults' media use and attitudes report 2018*. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf

Powis, B., Randhawa, K. and Bishopp, D. (2019) An examination of the structural properties of the Extremism Risk Guidelines (ERG22+); a structured formulation tool for extremist offenders. *Terrorism and Political Violence.* Retrieved from https://doi.org/10.1080/09546553.2019.1598392

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

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

Reynolds, S. C., and Hafez, M. M. (2017) Social network analysis of German foreign fighters in Syria and Iraq. *Terrorism and Political Violence, 31*(4), 661–686.

Scrivens, R. and Conway, M. (2019) *The roles of 'old' and 'new' media tools and technologies in the facilitation of violent extremism and terrorism*. Retrieved from https://www.researchgate.net/publication/336588722_The_Roles_of_'Old'_and_'New'_Media_Tools_and_Technologies_in_the_Facilitation_of_Violent_Extremism_and_Terrorism

Scrivens, R., Gill, P. and Conway, M. (2020) The role of the Internet in facilitating violent extremism and terrorism: Suggestions for progressing research. In T. J. Holt and A. Bossler (Eds.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–20). London, UK: Palgrave.

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.

UK House of Commons Home Affairs Committee (2017) *Radicalisation: the Counter-Narrative and Identifying the Tipping Point*, Eighth Report of Session 2016–17 (HC 135). Retrieved from https://www.parliament.uk/documents/commons-committees/home-affairs/Correspondence-17-19/Radicalisation-the-counter-narrative-and-identifying-the-tipping-point-government-response-Eighth-Report-26-17-Cm-9555.pdf

United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2020) *The impact of Covid-19 pandemic on terrorism, counterterrorism and countering violent extremism.* Retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper–-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf

Von Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013) *Radicalisation in the digital era, the use of the internet in 15 cases of terrorism and extremism*. Brussels: RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Webster, S., Kerr, J. and Tompkins, C. (2010) *A process evaluation of the structured risk guidance for extremist offenders: Final report*. London, UK: National Centre for Social Research. Ministry of Justice Publications: Research and Analysis.

Whittaker, J. (2021) The online behaviors of Islamic state terrorists in the United States. *Criminology and Public Policy* (published online). Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12537?af=R

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).

Lone actor terrorism – the HM Government CONTEST strategy report (Revised June 2018) describes lone actors as “associates or members of a terrorist network who are acting autonomously, or those who may be unconnected to any network, but have been influenced by terrorist or extremist propaganda” (HM Government, 2018, p. 17).

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 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, while 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 of 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 cases 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 cases 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.

Provision of material support online – This variable related to whether an individual had been involved in the provision of material support online. Examples included if an individual had donated funds or sent equipment to support another co-ideologue.

Access to specific extremist websites – 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 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 E-mail/standard chat applications – This variable related to whether an individual had used e-mail/standard chat applications online. E-mail/standard chat applications 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 encrypted applications – This variable related to whether an individual had used encrypted applications online (e.g. Telegram, Viber and WhatsApp).

To obtain demographic and offence type information for all cases within the dataset, 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'.

Gender – Coded as 'Male' or 'Female'.

Place of birth – Coded as 'UK' or 'Non-UK'.

Convicted offending history – Coded as 'Yes' or 'No'.

Presence of mental illness/personality disorder – This variable related to whether an individual had mental health difficulties and/or personality disorder as scored from the corresponding factor within the ERG22+ assessment.

Violent or non-violent – 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.

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'.

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'.

In terms of variables specific to the ERG22+ assessment, the overall rating for engagement, intent and capability was recorded for individuals from either the ERG22+ scoring grid attached to each report or where referenced within the body of the report. These variables were coded based on the corresponding overall 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, Medium or High) to reflect the individual's level of engagement to the extremist group/cause 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, Medium 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, Some 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.