Understanding the role of the Internet in the process of radicalisation: An analysis of convicted extremists in England and Wales

Jonathan Kenyon[a1], Jens Binder[b] & Christopher Baker-Beall[c]

[a]HMPPS Interventions Services, London, UK; [b]Department of Psychology, Nottingham Trent University, UK; [c]Disaster Management Centre, Bournemouth University, UK

PRE-PUBLICATION VERSION, DO NOT CITE

MANUSCRIPT ACCEPTED FOR PUBLICATION BY STUDIES IN CONFLICT & TERRORISM

Word count – 12,384

Contact: Jonathan Kenyon | jonathan.kenyon@justice.gov.uk | National Specialist Lead for Extremist Offending (HMPPS Interventions Services) 8th Floor, 102 Petty France, London, SW1H 9AJ

Abstract

This study explores the Internet's role in radicalisation pathways and offending of 235 convicted extremists in England and Wales. A comprehensive database was developed by coding content of specialist assessment reports by professionals with direct contact with individuals concerned. A series of quantitative analyses were then conducted. Findings suggest the Internet is playing an increasingly prominent role in radicalisation, with variations in online activities depending on pathway taken. Internet use has also changed over time, with increasing social media use. This study informs the debate on the Internet's role within radicalisation pathways, guiding counter-terrorism approaches and policy in this area.

Introduction

The terrorist attacks of 11 September 2001 coincided with the rapid global expansion of the Internet and digital technologies into all aspects of society and our everyday lives. The Internet has not only made it easier to find people and create networks amongst like-minded individuals across national borders, but also lowered the threshold for individuals to engage in 'risky' behaviour due to its ability to conceal users' identities and avoid prosecution.[1] As society has embraced the Internet, the potential opportunity for those wanting to use the online space for terrorist purposes has also grown, resulting in the spread of violent extremism and extremist ideologies within communities.[2]

A number of high-profile cases where individuals have seemingly radicalised online, before committing acts of terrorism, have come to the public's attention through widespread media reporting. This includes 21-year-old British student Roshonara Choudhry sentenced to life imprisonment in 2010 for stabbing her local MP for his support of the Iraq War after watching online sermons in her bedroom by US-born extremist Anwar Al-Awlaki on YouTube.[3] Another example is that of a teenage neo-Nazi group leader (not named for legal reasons) who, in 2021, became one of Britain's youngest convicted terrorists at 16-years old.[4] He started gathering terrorist material at age 13, used online chatrooms to share far-right extremist ideology by 14, before becoming leader of a British cell of Feuerkrieg Division, a neo-Nazi group idolizing and promoting mass violence. Such cases have led to the UK Home Affairs Committee reporting that Internet use to promote radicalisation and terrorism is "…one of the greatest threats that countries including the UK face."[5] The COVID-19 pandemic has resulted in increased concerns around the threat of online radicalisation, with people spending more time at home and online than ever before.[6] Although the pandemic may have reduced in-person exposure to potentially radicalising peer groups, increased Internet use may have heightened exposure to radicalising influences online and provided more opportunity for engagement with online spaces supportive of terrorism.[7] Since the start of the pandemic, there has been increased visibility of conspiracy theories online, and it has been suggested that extremist groups have used such conspiracies to further their own ideological aims.[8]

Concerns specific to online radicalisation relate to its covert nature, difficulties in detection and potential to facilitate lone-actor and group-based terrorism.[9] To inform and tailor counter-terrorism response measures, there is a need to establish whether increasingly widespread use of the Internet in society is reflected in the way those who commit extremist offences are radicalised. This study therefore investigates whether differences exist in Internet use for extremist purposes by those taking different pathways to extremist offending. This includes investigating whether certain online activities and recruitment strategies are more strongly associated with online radicalisation and if these have changed over time. Finally, this study investigates differences in Internet use within radicalisation pathways over time depending on

age, sex, ideology, whether convicted extremists are considered violent or non-violent and the role held in support of a group or cause.

Aims of Study

The primary aim of this study is to explore the role of the Internet in the radicalisation process and offending of convicted extremists.[10] To this end, a database of 269 convicted extremists in England and Wales is used, informed by Structured Risk Guidance (SRG) and Extremism Risk Guidance (ERG22+) assessment reports. This constitutes a unique data source not previously used for this purpose and not normally accessible to researchers.

The present study compares radicalisation pathways based on relevance of internet use to investigate four key areas. First, the extent to which the Internet plays a prominent role in radicalisation for those convicted of extremist offences. Within this study, 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 commission of offences and/or the use of violence in pursuit of its objectives."[11] Second, whether the radicalisation pathway is related to the way those convicted of extremist offences use the Internet. Third, if there have been changes in types of websites/platforms/applications used by convicted extremists over time. Fourth, if Internet use in radicalisation pathways has varied over time when comparing cases based on age, sex, ideology, whether a violent or non-violent offence was committed, and role assumed within the context of offending.

Literature Review

Scrivens and Conway suggest that while 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.[12] Meleagrou-Hitchens and Kaderbhai report that Internet use by extremists has evolved rapidly, with new online platforms and tools being used to disseminate extremist ideas with the intention these will resonate with supporters and attract new members.[13] Law enforcement and security agencies have focused attention on learning how online discussions and activities of those holding extremist views can spill over into the offline sphere, while social media companies have expressed concern their platforms are being used to facilitate extremist communications that promote violent activity offline.[14] Policymakers are concerned that increasing production and dissemination of extremist content online may have radicalising effects, particularly as this is the intention of those producing such material.[15]

The Internet and Radicalisation

The Internet's role in radicalisation processes has remained a difficult area to establish. In this study, radicalisation is defined as, "the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups."[16] Firm conclusions based on empirical evidence remain scarce (Meleagrou-Hitchens & Kaderbhai[17]) given that there is a general lack of empirical studies in this area. Those that have been conducted have largely relied upon open-source media to inform conclusions. One notable exception is the study by Von Behr et al. who accessed interviews with 15 radicalised individuals, including nine convicted under terrorism legislation in the UK.[18] Based on their findings, Von Behr et al. argued the Internet afforded more prospects for radicalisation as it was a "key source of information, communication and of propaganda for their extremist beliefs" for all cases in their sample.[19] The Internet was also seen as providing "greater opportunity than offline interactions to confirm existing beliefs."[20]

In another study relying on primary data, Koehler analysed interviews with eight former German right-wing extremists.[21] Support was found for the prominent role of the Internet by providing a more effective means of communication, anonymity, and improved networking opportunities. However, some formers indicated they only truly felt part of a movement after attending rallies and meeting others offline. Another study by Gaudette et al. involved in-depth interviews with 10 Canadian former right-wing extremists.[22] An interaction between online and offline domains was highlighted. For some formers, the Internet played a secondary role, reaffirming or advancing pre-existing beliefs acquired through in-person relationships; for others, the initial interest was sparked through exposure to extremist content online. The Internet was described as best for immersing individuals in extremist content and networks, with some formers describing the online domain as 'a gateway' to engage in violent extremist activities offline, connecting those in the online and offline worlds.

An influential study by Gill et al. explored Internet use by 227 UK extremist offenders using open-source data.[23] Their findings largely supported the notion that the Internet was a facilitative tool that enabled radicalisation, rather than radicalisation being reliant on it. More recently, Bastug et al. focused on the role of social media by accessing media and court reports for 51 Canadian Islamist extremists.[24] For 32 cases where radicalisation data were available, online social media was found to have played a role in 21 cases. Furthermore, at least 26 cases had used social media for terrorism-related activities after becoming radicalised. The most common online activities included spreading extremist ideologies or encouraging terrorism through posting and exchanging extremist messages or sharing extremist videos. Holbrook and Taylor reviewed pre-arrest media usage of five cases in the UK of those convicted of attempts to orchestrated terrorist attacks.[25] Within this study, all cases examined interacted with beliefs and ideas first through online social media, before proceeding to more operational activities where they planned to put ideas into action. Most recently, Whittaker investigated the online behaviours of 231 U.S. based terrorists affiliated with Daesh using a combination of court documents, academic and grey literature of case studies and journalistic data.[26] It was found that the Internet served as a tool for learning about their intended activity and networking with co-ideologues.

To summarise, key insights to date include the Internet being seen as providing more opportunities for radicalisation, particularly for learning, communication, and networking with other extremists. The Internet was considered useful in sparking initial interest in some cases and cementing beliefs through immersion in ideological content in others. Once beliefs are established, the Internet has been found to play an important role in connecting online and offline worlds and facilitating operational activities. However, knowledge gaps remain in relation to the specific contribution of the Internet in radicalisation processes, as well as its contribution to extremist offending.

Open Questions: Online Activities, Offender Demographics and Offence Characteristics

After reviewing research perspectives on online radicalisation, Meleagrou-Hitchens and Kaderbhai[27] suggested academics are still grappling with the extent to which the Internet acts as a replacement for physical interactions and if online networks have the same influence on individuals as real-world social networks (see Gill et al.[28]). There is also a lack of clarity as to whether those taking various radicalisation pathways utilise the Internet in different ways, for example, comparing online activities of those radicalised online with those radicalised offline.

There remains a need to establish more clearly the relevance of various online platforms and applications to radicalisation processes, and whether these have changed over time. Watkin and Whittaker referred to an evolution in the way extremist groups have used the Internet over

time: while members first accessed extremist homepages/websites, many transitioned to mainstream social media and micro-blogging sites, including Facebook and Twitter, when initial sites were infiltrated by security services.[29] Then, in response to adapting governments and service providers, members migrated towards encrypted platforms, such as Telegram, offering similar features to open platforms but with more security and privacy. As this study utilises a large database of extremist offences over many years, the relevance of various types of Internet services can be explored over time.

Further knowledge gaps include potential differences in the way the Internet is used for distinct sub-sets of extremist offenders based on age, sex, ideology, whether cases are considered violent or non-violent and role taken within an extremist group or cause. One study suggesting potential age differences is that by Nesser who investigated generational differences in European jihadists.[30] He found the Internet was a more important resource for the younger generation, described as more impatient and reckless than their predecessors. It has been suggested that social media use in particular may differ by age, as this has been described as a space dominated by 'digital natives' between 14 and 24 years of age.[31] Furthermore, there is potential for sex differences in Internet use by convicted extremists, given females have been found more likely to use social media to communicate with pre-existing friends, while males are more likely to use social media for information seeking, making new contacts and entertainment.[32] Ideological differences have previously been reported by Gill et al., who found extreme right wing offenders in the UK were more likely to learn online and communicate online with co-ideologues than Jihadist-inspired individuals.[33] In another study, Jensen et al. investigated internet use by U.S. extremists using PIRUS data from 2005-2016.[34] They found Islamist extremists displayed highest rates of social media usage overall, while far-right extremists engaged in other online behaviours at a higher rate, including participating in extremist dialogue and creating extremist content.

When focusing on offence type and role within an extremist group or cause, differences have been found when comparing posting behaviours of violent and non-violent right wing extremists.[35] Jensen et al.,[36] also reported differences in social media use comparing violent extremists, with non-violent extremists and travellers. Of 226 U.S. extremists involved in violent acts (or had clear intent to engage in violence), the majority (52%) were found to have radicalised or mobilised through social media use. In contrast, the majority (60%) of non-violent extremists were found not to be active on social media. Of those who travelled (or intended to travel) to conflict zones overseas, 79% were active on social media. One key strength of the present study is the variation in cases within the dataset, which allows for a systematic comparison of sub-groups based on demographics and offence characteristics.

Risk Assessment of Extremist Offenders in England and Wales

The database used to inform this study includes 267 ERG22+ reports and two SRG[37] reports (the predecessor to the ERG22+). This represents close to the entire convicted extremist population in England and Wales from 2010 to 2017.[38] It is important to understand the purpose of ERG22+ reports and how these assessments are completed as this informs the coding process. Since September 2011, the ERG22+ has been used throughout prison and probation services in England and Wales to assess all individuals convicted and sentenced under Terrorism Act (TACT) legislation[39] and those who committed other offences where the motivation was considered extremist. The ERG22+ adopts a structured professional judgement approach and analyses the personal and contextual factors, along with the circumstances that contributed to an individual's offending and engagement with an extremist group or cause. It is recommended for use with those with any ideological reference, of either sex, and on lone

actors and group actors alike.[40] It is based on case formulation and utilised for risk management. 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,[41] with inter-rater reliability ranging from perfect to moderate.[42]

Despite the widespread use of the ERG22+ in England and Wales, the structure has received some attention and criticism. For example, Knudsen argued that while the ERG22+ factors are not intended to capture the full political and societal context of an individual's radicalisation, the current reliance on these indicators by counter-terrorism in England and Wales make their limited explicit incorporation of political and societal context problematic.[43] Knudsen was also critical of the ERG22+ for only providing a 'radicalisation snapshot' of a person's psychology at the time an assessment is carried out.[44] Herzog-Evans was critical of the ERG22+ for its lack of inclusion of cognitive psychological factors such as need for closure.[45] However, such criticisms may reflect a degree of unfamiliarity with the ERG22+ and how this tool is applied in practice. Although the 22 factors are unlikely to capture the full political and societal context, assessors are encouraged to consider wider contextual circumstances when formulating how individuals become drawn into terrorism, bringing a level of political, cultural and situational awareness to the process. For the initial ERG22+, assessors provide two sets of ratings: one to reflect the presence of factors at the time the extremist offence was committed and a second set of ratings to reflect the individual at time of assessment. The structure of the tool also allows for inclusion of additional factors outside the 22 if considered relevant.

Silke identified four groups of terrorist-risk concern within prison settings, all of whom could potentially be assessed using the ERG22+.[46] The first group are 'Radicalised extremists' who entered prison already holding extremist views and have engaged in extremist actions outside of prison, ranging from planning or carrying out extreme acts of violence, to encouraging or supporting others to commit crime, including recruiters, fundraisers, and online propagandists. 'Radicalised extremists' would be assessed using the ERG22+ and are of particular interest in this study given the aim of exploring the role of the Internet in radicalisation processes and offending. The second group are those convicted of involvement in extremism or terrorism, but where there is a lack of evidence they were radicalised at the time. These 'Affiliates' may have been coerced into playing a role or unaware of the seriousness of what they were involved in. Individuals within this group, like the remaining two, fall outside the scope of this study given they are not considered radicalised. The third group are those who have shown no interest in an ideological or political cause prior to prison, but are then radicalised in custody, often as a result of contact with convicted extremists ('Prison recruits'). Internet-enabled devices, however, should not be accessible in custody and therefore not contribute to radicalisation. Finally, there are 'Vulnerables', who are not considered radicalised, but seen as vulnerable in the right circumstances.

Methodology

Sample

The data source consisted of 267 ERG22+ reports and two SRG reports. Within this study, the report subjects were individuals convicted of either extremist[47] or extremist-related[48] offences in England and Wales.[49] For cases within the sample, sentencing dates ranged from 1982 to 2017, with 97% of cases sentenced from 2005 onwards. Only initial ERG22+ reports were included as, unlike ERG22+ review reports, these feature a 'baseline' assessment of cases at the time of committing their extremist offence. The reports included all that were available to the Ministry of Justice (MoJ) completed from October 2010 to December 2017 as the

researchers were granted access up to this point.[50] Report authors were Registered Psychologists or qualified Probation Officers who had undertaken the same two-day national training to learn how to conduct the assessment. These authors had access to a range of restricted information sources when compiling the reports, including direct interviews with the subject of the report in most cases to provide a first-hand account. The average length of reports was 20 pages, the longest comprising of 146 pages and the shortest 4 pages.

As the focus was on the role of the Internet in the radicalisation process and offending of convicted extremists, the analysis focused exclusively on those considered 'Radicalised Extremists,' defined as those who have entered prison already holding extremist views and who have engaged in extremist actions in the outside world.[51]

Both the SRG and ERG22+ are formulation-guided assessments where the author provides a narrative account of an individual's pathway to extremist offending. For this reason, it was possible in most cases to establish when the development of extremist beliefs occurred and relevance of the Internet to the individual's pathway prior to committing the extremist offence(s) for which they were convicted. For example, in some cases, there was a lack of evidence suggesting the individual had engaged in offline interactions or meetings with other extremists but had participated in online activity or exchanges with other extremists. In such cases, the development of their extremist beliefs was considered to have occurred primarily online. If an individual reported initially being exposed to extremist materials and discussions online but later sharing their views and having these reinforced by co-ideologues in offline settings, this would indicate both online and offline influences contributed to the development of an extremist mind-set. Such information was obtained from the formulations themselves and content within the reports. When it was not possible to identify the point when the development of extremist beliefs occurred, these cases were excluded from analysis. Where sufficient evidence existed to determine radicalisation pathway based on relevance of the Internet, cases were categorised into one of three groups consistent with those utilised in previous research:[52] Primarily radicalised online ('Internet' group); Primarily radicalised offline ('Face to face' group); and Radicalised through both online and offline influences ('Hybrid' group).

Of the 269 convicted extremists within the dataset, 248 were coded as 'Radicalised Extremists'. The radicalisation pathway could be reliably determined based on information contained within reports in 235 cases (95%), so analysis focused on these cases specifically. The basic demographics for the 235 cases are detailed in Table 1.

Table 1. Basic Demographics for the 235 cases included within the Analysis

Demographic		Percentage (%)
Sex	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

Note: *See section on Procedure and Coding for how variables were derived.*

[a]Based on 233 cases as age at time of sentencing could not be identified in 2 cases
[b]Based on 224 cases as place of birth could not be identified in 11 cases

Of the 235 cases, 211 (90%) were male and 24 (10%) were female. In terms of age, 99 cases (42%) were 25 years old and under, while 136 cases (58%) fell in the 'Over 25' age category. A total of 163 cases were born in the UK (73%), whereas 61 (27%) were born outside of the UK. In terms of ideology breakdown, 179 were Islamist extremists (76%), 25 were Extreme Right Wing (11%), 16 were Animal Rights (7%) and the remaining 15 cases reflected individuals described as either anti-establishment or supporting an extreme far-left ideology, or those affiliated with nationalist or separatist movements. This group were classified as Other Political (6%).

Research Ethics

The study received ethical approval from the College Research Ethics Committee at Nottingham Trent University and the National Research Committee (NRC) as the data related to individuals convicted of extremist offences and either incarcerated or under probation supervision in England and Wales. Specific consideration was given to ways of managing risk of distress and vicarious trauma amongst researchers as the methodology involved accessing and reviewing reports featuring content of a distressing and concerning nature.

Procedure and Coding

Each report was manually reviewed by the lead researcher to develop a comprehensive coded dataset. This involved examining each report and extracting variables of interest (outlined below) by coding information relevant to radicalisation pathway, demographic variables, including ideological affiliation, and internet behaviours commonly associated with online radicalisation.[53] A codebook was developed that included variable definitions, with instructions and examples of how to apply the coding frame consistently. This process of developing and verifying the coding system was consistent with previous research.[54] The lead researcher was initially tasked with coding all variables of interest from the dataset. To ensure consistency and ease of use of the coding frame, two other coders then independently coded all variables of interest for a selection of cases. These additional coders were academic experts with ongoing involvement in the research project and familiarity with quantitative coding procedures. As part of an iterative process, all three coders then collaboratively reviewed the coding of test cases and where differences were apparent, resolved these though discussion and reaching a consensus.

Having identified 'Radicalised Extremists' based on Silke's four types of prison extremists[55] and assigning cases to one of three radicalisation pathway groups, a number of demographic variables were coded for all cases. These included: a) sex (coded as 'Male' or 'Female'); b) age at time of sentencing (coded as 'Up to and including 25' or 'Over 25'); c) place of birth (coded as 'UK' or 'Non-UK'); and d) ideology (coded as 'Animal Rights', 'Extreme Right Wing', 'Islamist Extremist' or 'Other Political'). Two offence characteristic variables were also coded, including e) violent/non-violent offence (coded as 'Violent' or 'Non-violent') and

f) role in group/cause (coded as 'Attacker', 'Facilitator', 'Financer' and 'Traveller' – where appropriate in some cases, more than one role was assigned).

Five online activity variables, describing the content and nature of behaviours (see Gill, Horgan & Deckert[56]; Gill & Corner[57]), were coded dichotomously[58] for all cases (e.g., 'Yes' or 'No evidence'), unless stated otherwise: a) Learnt from online sources; b) Interact with co-ideologues online; c) Generate their own extremist propaganda online; d) Provision of material support online; and e) Active or passive internet user (coded as 'Active' for those who create or contribute to extremist content online, 'Passive' for those who only consume online extremist content or 'N/A' where internet use was not relevant for the case). Four additional variables (informed by the suggestion of an evolution in the way extremist groups have used the Internet – see Watkin & Whittaker[59]) describing the tools/services/applications used in relation to online extremist activity were also coded dichotomously (e.g., 'Yes' or 'No evidence'): a) Access to specific extremist websites; b) Use of open social media platforms; c) Use of E-mail/standard chat applications; and d) Use of encrypted applications. Four online planned action behaviours (see Gill & Corner[60]) were originally coded for all cases within the dataset, including: a) Attack preparation; b) Target choice; c) Overcoming difficulties/hurdles; and d) Signalling intent. However, as online planned action behaviours were only relevant to a small portion of the dataset (i.e., those who had committed or planned to commit a violent extremist offence), frequency counts were low and subsequently these variables were excluded from analysis.

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 in trajectories towards extremist offending over time. Within each pathway group, user demographics and offence characteristics were likewise inspected over time. In a second step, pathway groups were compared with each other in terms of online activities.

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 group membership 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 used to test whether any coded internet behaviour variables could predict pathway group membership, including establishing which were the strongest predictors.

Study Limitations

A number of limitations of the study can be identified. Direct interviewing of convicted extremists or professionals managing cases would likely have resulted in further insights into online behaviours. Most research has relied on case information from open-source media to draw conclusions and while a handful of studies have included interviews with convicted extremists (e.g., Koehler;[61] Von Behr et al.[62]), additional interview data would be desirable. Some individuals were impossible to include within the sample, such as those who died during the commission of offences, those acquitted at trial and those never identified and/or apprehended by the police. Another limitation includes the difficulties distinguishing between missing data and variables that could reliably be coded as not present. Given the purpose of the SRG and ERG22+ reports was not to provide detailed accounts of all internet behaviours of relevance, it is possible some online behaviours may not have been reported and therefore

aspects of internet use were missed. The reports varied in length and detail, providing another reason why some may not have covered all online behaviours, even where relevant. It is recognised that some information relating to the radicalisation pathway and internet use may have been lost, particularly as 23% of convicted extremists decided against directly contributing to reports through interviews. There is also the possibility that those interviewed were not always honest with their disclosures and that some professionals authoring the reports have added their own interpretations to the information. Also, the findings from this study reflect the convicted extremist offender population in England and Wales where a SRG or ERG22+ assessment was completed up to the end of December 2017, the time period for which access was granted to the researchers.

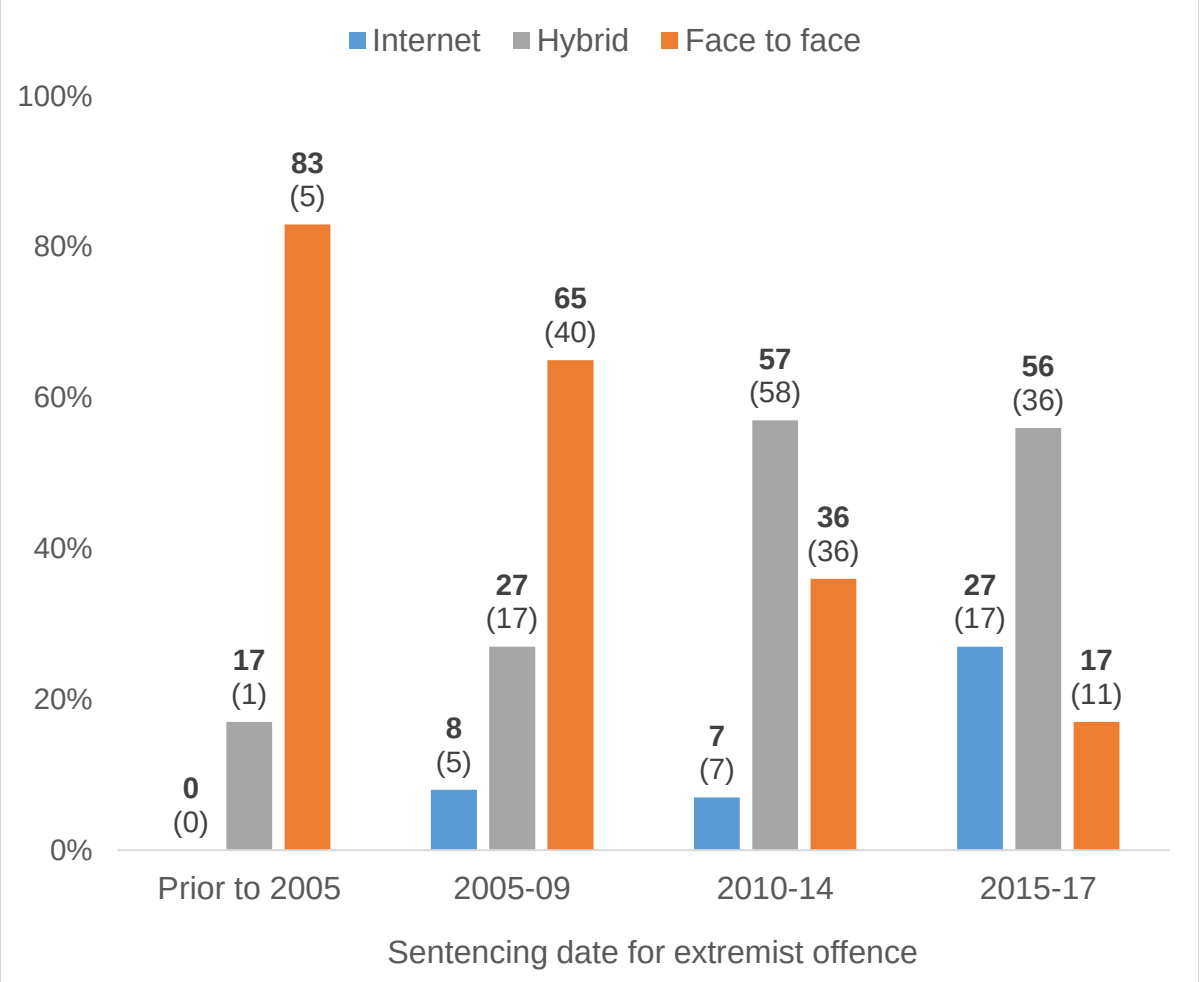
Results

Prominence of the Internet in Radicalisation Pathways over time

The role of the Internet was found to have become increasingly prominent in radicalisation processes of convicted extremists in England and Wales. In the period from 2005 to 2017, there was an increase in number of extremist offenders who were subject to some degree of online radicalisation, including those who primarily radicalised online and those radicalised through both online and offline influences (83% in 2015-17, 64% in 2010-14, 35% in 2005-09). Over the same period, a reduction was observed in the number who were primarily radicalised offline before committing an extremist offence (17% in 2015-17, 36% in 2010-14, 65% in 2005-09, see Figure 1).

Despite evidence suggesting an increasingly prominent role of the Internet in radicalisation processes of convicted extremists, further analysis showed that offline influences featured at least to some extent for most individuals within the dataset (88%). The largest pathway group were those radicalised through a combination of both online and offline influences (48%), followed by those primarily radicalised offline (40%), with those primarily radicalised online making up only 12% of the sample.

Figure 1. Percentages and Frequencies of cases showing the Primary Method of Radicalisation for 'Radicalised Extremists' over Time



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

Differences in Online Activity depending on Radicalisation Pathway

To establish whether certain online behaviours and recruitment strategies are more strongly associated with online radicalisation, five online activity variables were compared across the three radicalisation pathway groups. These included whether individuals had learnt from online sources, interacted with co-ideologues online, disseminated their own extremist propaganda, provided online material support to others and if they were active or passive Internet users (see Table 2).

Table 2. Percentages for Online Activity variables compared across Primary Method of Radicalisation

		Internet (n = 29)	Face to face (n = 93)	Hybrid (n = 113)
Learnt from online sources**	Yes	93.1%	16.1%	99.1%
	No evidence	6.9%	83.9%	0.9%
Interact with co-ideologues online**	Yes	75.9%	18.3%	48.7%
	No evidence	24.1%	81.7%	51.3%

Disseminate own extremist propaganda**	Yes	62.1%	11.8%	31.9%
	No evidence	37.9%	88.2%	68.1%
Provision of material support online	Yes	10.3%	4.3%	14.2%
	No evidence	89.7%	95.7%	85.8%
Active or passive internet user*	Active	79.3%	25.8%	64.0%
	Passive	20.7%	16.1%	46.0%
	N/A	0.0%	58.1%	0.0%

Note: ***significant association with radicalisation pathway at p < .01. *significant association with radicalisation pathway at p < .05*

Statistically significant associations were found across four of the five online behaviours when comparing pathway groups. For 'Learnt from online sources' (χ^2 = 166.67, p < .01), those who primarily radicalised online were found to be 70.20 times more likely to have learnt from online sources than those who primarily radicalised offline, while those who radicalised through both online and offline influences were 582.40 times more likely than those primarily radicalised offline. For 'Interact with co-ideologues online' (χ^2 = 37.36, p < .01), those who primarily radicalised online were found to be 14.05 times more likely to have interacted with co-ideologues online than those who primarily radicalised offline, while those radicalised through both online and offline influences were 4.24 times more likely than those primarily radicalised offline. For 'Disseminate own extremist propaganda' (χ^2 = 29.81, p < .01), those who primarily radicalised online were found to be 12.20 times more likely to have disseminated their own extremist propaganda online than those who primarily radicalised offline, while those radicalised through both online and offline influences were 3.49 times more likely than those who primarily radicalised offline. For 'Active or passive internet user' (χ^2 = 6.22, p < .05), those who primarily radicalised online were found to be 2.40 times more likely to have been an active user than those who primarily radicalised offline (but had used the Internet during their extremist offending). Those who radicalised through both online and offline influences were 1.36 times more likely to have been an active user than those who primarily radicalised offline (but had used the Internet during their extremist offending).

All three radicalisation pathway groups were then compared based on the types of websites and online applications used.

Table 3. Percentages of Types of Websites or Applications used across Primary Method of Radicalisation

		Internet (n = 29)	Face to face (n = 93)	Hybrid (n = 113)
Accessing specific extremist websites/ homepages**	Yes	17%	10%	28%
	No evidence	83%	90%	72%
Use of social media applications/ platforms**	Yes	66%	5%	40%
	No evidence	34%	95%	20%
Use of standard chat applications*	Yes	24%	10%	25%
	No evidence	76%	90%	75%

Use of encrypted applications*	Yes	0%	2%	11%
	No evidence	100%	98%	89%

Note: ***significant association with radicalisation pathway at p < .01. *significant association with radicalisation pathway at p < .05*

Statistically significant associations were found across all four types of websites or applications when comparing pathway groups. For 'Accessing specific extremist websites/homepages' ($\chi^2 = 11.38$, $p < .01$), those who primarily radicalised online were found to be 1.94 times more likely to have accessed specific extremist websites or homepages than those who primarily radicalised offline, while those radicalised through both online and offline influences were 3.69 times more likely than those who primarily radicalised offline. For 'Use of social media applications/platforms' ($\chi^2 = 50.04$, $p < .01$), those who primarily radicalised online were found to be 33.44 times more likely to have used social media platforms or applications than those who primarily radicalised offline, while those who radicalised through both online and offline influences were 11.65 times more likely than those who primarily radicalised offline. For 'Use of standard chat applications' ($\chi^2 = 8.28$, $p < .05$), those who primarily radicalised online were found to be 2.97 times more likely to have used standard chat applications than those who primarily radicalised offline, while those radicalised through both online and offline influences were 3.07 times more likely than those who primarily radicalised offline. For 'Use of encrypted applications', this was only relevant for those who radicalised through both online and offline influences and those who primarily radicalised offline, but only in the minority of cases (11% and 2% respectively). Surprisingly, no cases were reported as having used encrypted applications for those who primarily radicalised online, a point we will revisit in the discussion. A significant relationship was found ($\chi^2 = 8.63$, $p < .05$), with those radicalised through both online and offline influences 10.81 times more likely to have used encrypted online applications than those who primarily radicalised offline.

Changes in types of Websites/Platforms/Applications used over Time

Within this study, the types of websites, platforms and applications used by convicted extremists were found to have changed over time. For individuals who primarily radicalised online and those who radicalised through both online and offline influences, there was a reduction in the number using specific extremist websites from 2005 onwards (60 and 83-percentage point decrease from 2005 to 2017 respectively). Across the same period, there was an increase in the number of individuals using open social media platforms to support extremist activity (36 and 57-percentage point increase respectively). There was also evidence of an increase in use of encrypted applications online, particularly around 2015-17, but this was most marked for those radicalised through a combination of both online and offline influences (25-percentage point increase from 2010 to 2017).

Online Activity Variables as Predictors of Pathway Group Membership

The analysis then established which online activity variables were the strongest predictors to differentiate between radicalisation pathway groups.

Table 4. Online Activity Variables as Predictors for Pathway Group Membership

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]

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

Numerous associations were found between online activity variables and pathway group membership. To get a better understanding of the multivariate associations and identify those online activity variables with the strongest association when considering all variables together, a multiple logistic regression was conducted. All eight online activity variables were entered as predictors and a new criterion variable was created that contrasted some extent of online radicalisation (i.e., those who primarily radicalised online and those radicalised by both online and offline influences) with offline only.

When comparing extremist offenders who primarily radicalised offline with those where the Internet was relevant to radicalisation pathway, the only two statistically significant predictors were found to be whether individuals learnt from online sources and used open social media platforms (see Table 4). For those who learnt from online sources, the odds of either having primarily radicalised online or through both online and offline influences were 575 times greater than having primarily radicalised offline. This is not surprising given only 16% of those who radicalised offline reported this online activity, as compared to 98% across the other two pathway groups. For those who used open social media platforms, the odds of either having primarily radicalised online or through both online and offline influences were close to 16 times greater than having primarily radicalised offline.

Follow-up regression analyses were carried out to compare, firstly, extremist offenders who primarily radicalised online with those who primarily radicalised offline and, secondly, those who primarily radicalised offline with those radicalised through both online and offline influences. In the first regression, 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 in the second regression.

When further comparing those who primarily radicalised online with those radicalised through both online and offline influences, similarities were found in their online behaviours. However, these two pathway groups could still be differentiated as a higher percentage of those who primarily radicalised online had 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%). It was also noted that those who radicalised through both online and offline influences tended to have rates between the other two pathway groups for online behaviours relating to extremist activity. These differences in online activity suggest this sample of convicted extremists can reliably be split into the three distinct groups based on primary method of radicalisation.

It was not possible to include the 'Active or passive internet user' variable within the multiple logistic regression due to three possible response options (e.g., 'active', 'passive' or 'N/A'). Instead, a Pearson's chi-square test was used to compare those who primarily radicalised online with those radicalised through both online and offline influences in relation to this variable. A significant relationship was found ($\chi^2 = 6.13$, $p < .05$), with those who primarily radicalised online 3.27 times more likely to be active internet users (i.e., those who create or contribute to extremist content online, rather than only consuming such content) than those radicalised through both online and offline influences.

In contrast to the other pathway groups, those who primarily radicalised offline had the lowest rates for online behaviours, using the Internet less often for extremist purposes. However, a sizable minority (42%) of this pathway group had still used the Internet to some extent for extremist purposes, highlighting the growing influence of the online domain in radicalisation processes and extremist offending generally.

Prominence of the Internet in Radicalisation Pathways over Time, comparing variables of Age, Sex, Ideology, whether cases were Violent/Non-violent, and Role in group/cause

Having already established that the Internet is playing an increasingly prominent role in radicalisation pathways across convicted extremists generally, cases were then separated by age, sex, ideology, whether cases were violent or non-violent based on extremist offence(s) committed and role in group/cause to investigate whether similar patterns were observed. Percentages for each variable across pathway groups are displayed in Table 5.

Table 5: Percentages for each Radicalisation Pathway comparing Age, Sex, Ideology, Violent/Non-violent offence and Role in group/cause over Time (based on sentencing date)

Variable		2005-09			2010-14			2015-17		
		Internet	FTF	Hybrid	Internet	FTF	Hybrid	Internet	FTF	Hybrid
Age	<=25	14	57	29	11	27	62	23	3	73
	>25	5	68	27	4	43	54	29	29	41
Sex	Male	8	63	29	6	38	56	50	33	17
	Female	0	100	0	11	56	33	42	25	33
Ideology	Animal Rights	0	100	0	0	86	14	0	0	0
	Extreme Right Wing	40	20	40	7	29	64	0	50	50
	Islamist Extremist	4	63	33	8	28	64	29	12	59
	Other Political	50	50	0	0	83	17	0	75	25
Violent/Non-Violent	Violent	11	68	21	4	43	52	13	13	75
	Non-violent	6	62	32	9	29	62	29	18	54
Role*	Attacker	5	29	9	2	17	21	1	1	8
	Facilitator	2	29	17	3	11	19	11	8	23
	Financer	0	2	3	0	3	10	4	3	9
	Traveller	2	3	0	1	1	11	8	4	19

*Role percentages calculated based on the total number of roles coded for each time-period to take account of some cases having assumed more than one role within the group/cause (i.e., facilitator and financer).

When comparing age across pathway groups, for those aged 25 or under, the number who primarily radicalised offline was found to have decreased by 54 percentage points from 2005 to 2017. Over the same time period, taking those who primarily radicalised online with those who radicalised through both online and offline influences equated to 43% of cases in 2005-09, 73% of cases in 2010-14, and 96% of cases in 2015-17. This reflected an increase of 53 percentage points over time for those aged 25 and under where the Internet was relevant in their radicalisation pathway. For those aged over 25, the number who primarily radicalised offline decreased by 39 percentage points from 2005 to 2017. Over the same time period, taking those who primarily radicalised online with those who radicalised both through both online and offline influences equated to 32% of cases in 2005-09, 58% of cases in 2010-14, and 70% of cases in 2015-17. This reflected an increase of 38 percentage points over time for those over 25 where the Internet was relevant in their radicalisation pathway.

When focusing on males, an increase was found in the number who were primarily radicalised online from 2005 to 2017 (42 percentage point increase). Taken together, males who primarily radicalised online and those who radicalised through both online and offline influences equated to 37% of cases in 2005-09, 62% of cases in 2010-14, and 67% of cases in 2015-17. This reflected an increase of 30 percentage points over time for males where the Internet was relevant in their radicalisation pathway. An increase in the number of females primarily radicalised online from 2005 to 2017 was also found (42 percentage point increase). Taken together, females who primarily radicalised online and those who radicalised through both online and offline influences equated to 0% of cases in 2005-09, 44% of cases in 2010-14, and 75% of cases in 2015-17. This reflected an increase of 75 percentage points over time for females where the Internet was relevant in their radicalisation pathway.

When comparing ideology across pathway groups, individuals within the Animal Rights and Other Political groups had primarily radicalised offline across all three time periods, although it should be noted there was comparatively less cases in these groups. For those supporting an Extreme Right Wing ideology, the number who primarily radicalised offline was found to have increased by 30 percentage points from 2005 to 2017. For Islamist Extremists, the number who primarily radicalised offline represented the biggest change, with a decrease of 51 percentage points from 2005 to 2017. At the same time, taking those who primarily radicalised online with those who radicalised both through both online and offline influences equated to 37% of cases in 2005-09, 72% of cases in 2010-14, and 88% of cases in 2015-17. This reflected an increase of 51 percentage points over time for Islamist Extremists where the Internet was relevant in their radicalisation pathway.

When violent and non-violent cases were compared across pathway groups, the number of violent cases who primarily radicalised offline was found to have decreased by 55 percentage points from 2005 to 2017. Over the same time period, taking violent cases who primarily radicalised online with those who radicalised both through both online and offline influences equated to 32% of cases in 2005-09, 56% of cases in 2010-14, and 88% of cases in 2015-17. This reflected an increase of 56 percentage points over time for violent cases where the Internet was relevant in their radicalisation pathway. For non-violent cases, the number who primarily radicalised offline was found to have decreased by 44 percentage points from 2005 to 2017. Over the same time period, taking non-violent cases who primarily radicalised online with those who radicalised both through both online and offline influences equated to 38% of cases in 2005-09, 71% of cases in 2010-14, and 83% of cases in 2015-17. This reflected an increase of 45 percentage points over time for non-violent cases where the Internet was relevant in their radicalisation pathway.

When considering roles within the group/cause, during the time period 2005-09, the most common roles were Attackers and Facilitators, which were most commonly held by those who primarily radicalised offline (29% for both roles of the total number of roles coded during that time period). In 2010-14, the most common roles remained Attackers and Facilitators, but the majority of cases holding these roles were radicalised by a combination of online and offline influences (for Attackers, 21% of total number of roles coded during this time period, for Facilitators, 19% for total number of roles coded). In 2015-17, the most common roles changed to Facilitators and Travellers. The majority holding these roles were radicalised by a combination of online and offline influences (for Facilitators, 23% of total number of roles coded during this time period, for Travellers, 19% of total number of roles coded).

Discussion

General findings from this study have confirmed existing knowledge or supported common assumptions around the role of the Internet in radicalisation and extremist offending. The finding that the Internet is playing an increasingly prominent role in radicalisation processes of those convicted of extremist offences in England and Wales up to 2017 comes as no surprise, neither does the finding that the prominence of the Internet in radicalisation pathways for the younger generation shows a particularly marked increase. However, this study has provided a population-based confirmation of such trends for extremist offenders in England and Wales. Other findings offer evidence to inform debates around the role of the Internet and provide novel insights.

First, this study found a lack of evidence to suggest the online domain is replacing the offline domain, given offline influences featured at least to some extent for most individuals within the sample. Instead, the findings provide support for the notion that most extremist offenders tend to operate across both domains. This supports the findings of Whittaker in his study of 231 U.S. based terrorists affiliated with Daesh, who found that strong relationships existed between online and offline learning and planning behaviours, leading to the conclusion that terrorists tend to operate across both domains.[63] The present findings also resonate with the assertion by Gill et al. that a distinction between online and offline radicalisation is a "false dichotomy" and "plotters regularly engage in activities in both domains."[64] Linked to this idea that terrorists generally operate across both domains is the concept of 'onlife,' where radicalisation processes are considered to unfold in hybrid environments, incorporating online and offline activities.[65] The first recommendation to reflect this finding is that security services and counter-terrorism initiatives should continue targeting the Internet as a setting where extremist socialisation can occur, but not at the expense of paying attention to environmental interactions offline.

Second, differences were found in 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 those where the Internet was relevant to their radicalisation pathway, from those who primarily radicalised offline, referred to learning from online sources and using open social media platforms. Similarities were found in the online behaviours between those who primarily radicalised online and those exposed to both online and offline influences. However, these pathway groups could still be differentiated as those influenced primarily online were more likely to be active internet users, reflected by their greater tendency to interact with like-minded others, disseminate their own extremist propaganda and access open social media platforms. It may be that those who were primarily radicalised online were more socially isolated offline and therefore relying more on social media communities, however further analysis is required to confirm this. Somewhat in contrast to the statement by Gill et al. that a distinction between online and offline radicalisation is a

"false dichotomy",[66] these differences in online activities suggest there may be some value by differentiating radicalisation pathway groups in this manner.

Third, the way extremist offenders have used the Internet was found to have changed over time, with decreasing reliance on specific extremist websites and homepages and increasing use of open social media platforms across the period 2005 to 2017. This provides empirical support for the progression suggested by Watkin and Whittaker from specialised extremist websites to open social media platforms, and eventually to encrypted applications, in response to the reaction of security services.[67] These changes come as no surprise as it would stand to reason that extremists and extremist groups have adapted how they use the Internet to take advantage of what technology can offer, in much the same way as members of the public. This point is reflected within the UK Government's Online Harms White Paper which states that extremist propaganda "...are not only restricted to the largest, best-known services, but are prevalent across the internet" and that, "Terrorist groups and their supporters constantly diversify their reliance on the online services they use to host their material online."[68] A number of recent studies have referred to a social media ecosystem as a way of describing how extremist groups are not using sites homogeneously and have adapted the way they use platforms in response to disruption efforts. Examples include using mainstream sites such as Twitter to redirect followers to file-sharing sites where large quantities of extremist content can be found[69] or to platforms such as Telegram with greater levels of user privacy.[70] Other examples include sharing news sources on mainstream sites that validate the group's stance but fall short of violating the platform's terms of service.[71]

The increased use of open social media platforms indicates that those radicalised and convicted of extremist offences are commonly using online applications that are familiar to and regularly accessed by the public. Similarly, Scrivens and Conway described social media channels as useful for sharing extremist propaganda and networking.[72] Likewise Bastug et al. within their study of fifty-one Canadian Islamist extremists consider social media platforms as "a very important radicalising agent."[73] Jensen et al. found social media use by U.S. terrorists had increased from around 25% in 2005-10 to 75% by 2011-16.[74] On this basis, it is important that social media and technology companies continue taking responsibility to counter online radicalisation by working together, blocking dissemination of extremist content on their platforms and protecting users from harmful content. It is encouraging that many providers already have policies, such as Facebook's policy against Dangerous Individuals and Organizations[75] and Twitter's Violent Organizations policy.[76] As first suggested by Stevens and Neumann, it is recommended that efforts to counter online radicalisation view new technologies and modes of interaction as opportunities, rather than threats.[77] One example may be to capitalise on the collective power of Internet users through user-driven self-regulation, where users are encouraged to challenge and report extremist content online to reduce availability. YouTube, for example, enables community members to flag offensive and/or illegal content, which is then reviewed and removed if found to breach internal policies, licence agreements, or national or international law.[78] Initiatives supportive of cross-platform working are also encouraged, such as the approach taken by the Global Internet Forum to Counter Terrorism (GIFCT). The GIFCT was established in 2017 as a joint enterprise between Facebook, Twitter, Google/YouTube and Microsoft, with membership having since expanded. A hash-sharing database has been developed featuring known terrorist content that members have removed for violating their terms of service, which is shared between members to support content blocking efforts.

Surprisingly, no cases of those who primarily radicalised online were reported to have used encrypted applications. This is despite it being known that extremists, particularly those

supporting Daesh, have moved towards use of online encrypted applications including Telegram.[79] One explanation is that the move towards use of encrypted applications did not occur in large numbers until the disruption of pro-Daesh accounts by major open social media companies forced many extremists off these platforms. For Twitter, a platform particularly favoured by Daesh and its supporters, disruption efforts gathered pace from mid-2014 and continued throughout 2015 and 2016,[80] leading to Telegram becoming the platform of choice.[81] This may account for the lack of evidence of encrypted application use generally across all radicalisation pathway groups, but particularly those who primarily radicalised online, as the dataset only included those convicted and sentenced for extremist offences prior to the end of 2017. It is also possible that assessors were less familiar with encrypted applications compared with open social media platforms and standard chat applications, so may not have recorded these online behaviours even if mentioned during interview.

Fourth, the findings of this study suggest there has been an increase in prominence of the Internet over time for both males and females, although this was most marked for females. The relevance of the Internet for females is not surprising, especially for those considered Islamist extremists and particularly during the years 2015-17, as this was shortly after Daesh declared the creation of a caliphate in 2014. Pearson and Winterbotham reported that females were explicitly targeted for recruitment by Daesh around this time, with women making up a significant demographic of those travelling or attempting to travel to Syria and Iraq.[82] Daesh women were also considered particularly active online, with their radicalisation generally less visible than for men.[83] For women in particular, the Internet has played a key role in lowering the threshold for their engagement and involvement with Islamist extremist groups by helping them overcome traditional barriers to entry such as a lack of information about the group, a lack of extremist social network, and a lack of publicised role for women.[84] This trend of increasing numbers of females was evident within this study as whilst females only accounted for 10% of all 'Radicalised extremists', a steady increase was observed in number of females sentenced for extremist offences over time, with 12% of females sentenced between 2005-2009, 38% between 2010-2014 and 50% sentenced between 2015-17.

Fifth, an increase in prominence of the Internet in radicalisation pathways for Islamist extremists was found over time, which may be explained by the extensive online propaganda and recruitment effort by Daesh over recent years. Rather surprisingly and in contrast to findings by Gill et al.,[85] the numbers of those who primarily radicalised offline supporting an Extreme Right Wing ideology were found to have increased over time. However, recent findings by Scrivens et al.[86] when comparing posting behaviours of violent and non-violent right wing extremists may offer some explanation. A general decline in posting behaviour was found over time for right wing extremists, but particularly those who became actively involved in extremist activities offline due to concerns their online activity may be monitored. For Animal Rights activists and for those in the Other Political group, in-person, offline radicalisation has remained a key aspect for engagement with these groups and causes over time.

Sixth, when considering offence characteristics, an increase in prominence of the Internet over time in radicalisation pathways for both violent and non-violent convicted extremists was found, suggesting the online domain plays a facilitative role regardless of type of offence committed. However, as was found within the U.S. sample by Jensen et al., this was particularly marked for those who have committed violent offences.[87] The most common roles held had changed over time from Attackers and Facilitators in 2005-09, the majority of whom had radicalised offline, to Attackers and Facilitators in 2010-14, with most radicalised via both online and offline influences. In 2015-17, the most common roles held changed to Facilitators

and Travellers (with the increase in Travellers accounted for by the declaration of the creation of a caliphate in 2014 by Daesh), with the majority radicalised through both online and offline influences. This highlights the increasingly prominent role of the Internet over time generally, but also in facilitating the varied roles held within an extremist group/cause.

When considering the above findings and incorporating the particularly marked increase of Internet use by the younger generation, it is recommended that new online counter-terrorism measures target younger users, appeal to males and females, and are sensitive to different ideological perspectives. An example of this is the Average Mohamed campaign, which involved five preventative educational videos aimed at reaching young Somali-Muslims living in the U.S. The target audience was 14–15-year-olds, with one video ('Be Like Aisha') using more female-focused targeting due to its message of Muslim female empowerment.[88] It is already known that young people are heavily influenced by content they see online, with many obtaining information from Google and social media sites including Facebook, Instagram and Twitter.[89] The emergence of new platforms including TikTok which has seen a rapid rise in popularity, particularly amongst children and teenagers, are also seen as highly influential to the younger generation.[90] In addition, social media platforms are seen as vital in enabling women to network with other extremists virtually, which has had a considerable impact given the frequent lack of opportunities for females to be fully integrated into extremist groups in offline settings.[91] Recently, there has been recognition of the potential value of youth participation in countering violent extremism, including their involvement in preventative measures, as well as delivery of deradicalisation programmes.[92] This is particularly relevant to the Internet, where young people are often the target audience and are generally more in tune with emerging technologies and more able to innovate than policy makers and other counter-terrorism stakeholders.

Conclusion and Directions for Future Research

Following this data-driven study, using a unique dataset of specialist assessment reports by professionals working directly with convicted extremists in England and Wales, the findings largely accord with, but also expand on, what is known from an existing literature base that has generally relied upon open-source data or small number 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 in the way wider society is using the Internet. In addition, although a handful of previous studies have featured interviews with convicted extremists focusing on internet use, further interviews with current or former extremists are likely to take us one-step closer to a more holistic triangulation of data. This will help researchers and policymakers obtain a more complete understanding of the role of the Internet in radicalisation processes and extremist offending. Finally, conducting further analysis of this sample by comparing the three radicalisation pathway groups using a wider range of socio-demographic and offence-type variables, along with professional ratings from ERG22+ assessments of overall levels of engagement with an extremist group or cause, and overall levels of intent and capability to commit violent extremist offences is likely to reveal additional insights into the convicted extremist population for England and Wales.

Notes

[1] Tim Stevens, and Peter Neumann, "*Countering online radicalisation: A strategy for action"* (London, UK: International Centre for the Study of Radicalisation, 2009). https://cst.org.uk/docs/countering_online_radicalisation1.pdf
[2] Mehmet. F. Bastug, Aziz Douai, and Davut Akca, "Exploring the 'demand side' of online radicalization: Evidence from the Canadian context," *Studies in Conflict and Terrorism* (2018): 1-22.
[3] Europol, *"EU Terrorism Situation and Trend Report"* (Brussels, 2011).
[4] *"Youngest British terrorist sentenced for neo-Nazi manuals stash," CPS*, last modified February 08, 2021, https://www.cps.gov.uk/cps/news/youngest-british-terrorist-sentenced-neo-nazi-manuals-stash (accessed September 22, 2021)
[5] UK House of Commons Home Affairs Committee, *"Radicalisation: the Counter-Narrative and Identifying the Tipping Point,"* Eighth Report of Session 2016–17 (HC 135, 2017), 2. 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
[6] United Nations Security Council Counter-Terrorism Committee Executive Directorate, *"The impact of Covid-19 pandemic on terrorism, counterterrorism and countering violent extremism"* (2020). 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
[7] It is important to note this study concluded prior to the onset of the COVID-19 pandemic.
[8] United Nations Security Council Counter-Terrorism Committee Executive Directorate, "The impact of Covid-19"
[9] Jonathan Kenyon, Christopher Baker-Beall, and Jens Binder, "Lone-actor terrorism – A systematic literature review," *Studies in Conflict and Terrorism* (advanced online publication, 2021). https://www.tandfonline.com/doi/abs/10.1080/1057610X.2021.1892635
[10] A sub-set of findings was published as part of a UK Government report in September 2021 on gov.uk. The present work goes beyond this report in its contextual information, commentary and analysis provided.
[11] National Offender Management Service, *"Extremism Risk Guidance. ERG22+ structured Professional Guidelines for Assessing Risk of Extremist offending"* (London, UK: Ministry of Justice, 2011).
[12] Ryan Scrivens, Paul Gill, and Maura Conway, "The role of the Internet in facilitating violent extremism and terrorism: Suggestions for progressing research," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, eds. Thomas J. Holt and Adam M. Bossler (London, UK: Palgrave, 2020), 1-20.
[13] Alexander Meleagrou-Hitchens, and Nick Kaderbhai, *"Research Perspectives on Online Radicalisation: A Literature Review, 2006–2016"* (ICSR/VOX-Pol Paper, 2017) http://icsr.info/ 2017/05/icsr-vox-pol-paper-research-perspectives-onlineradicalisation-literature-review-2006-2016/
[14] Ibid.
[15] J. M. Berger, and Bill Strathearn, "*Who matters online: Measuring influence, evaluating content and countering violent extremism in online social networks"* (Kings College London: ICSR, 2013). http://icsr.info/wp-content/uploads/2013/03/ICSR_Berger-and-Strathearn.pdf
[16] HM Government, *"Revised Prevent Duty guidance: for England and Wales"* (April 01, 2021). https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales#f-glossary-of-terms).
[17] Meleagrou-Hitchens and Kaderbhai, "Research Perspectives on Online Radicalisation"
[18] Ines von Behr, Anais Reding, Charlie Edwards, and Luke Gribbon, "*Radicalisation in the digital era, the use of the internet in 15 cases of terrorism and extremism*." (Brussels: RAND, 2013). https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
[19] Ibid., 12.
[20] Ibid.
[21] Daniel Koehler, "The radical online: Individual radicalization processes and the role of the Internet," *Journal for Deradicalization,* 1, (2014): 116–134.
[22] Tiana Gaudette, Ryan Scrivens, and Vivek Venkatesh, "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists" in *Terrorism and Political Violence,* (2020). https://www.tandfonline.com/doi/abs/10.1080/09546553.20
[23] P. Gill, E. Corner, A. Thornton, and M. Conway, "*What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists"* (EU FP7 VOX-Pol report, 2015). http://voxpol.eu/what-are-the-roles-of-the-internet-interrorism.
[24] Bastug et al., "Exploring the 'demand side' of online radicalization"
[25] Donald Holbrook, and Max Taylor, "Terrorism as process narratives: A study of pre-arrest media usage and the emergence of pathways to engagement," *Terrorism and Political Violence 31*, no. 6 (2019): 1307-1326.
[26] Joe Whittaker, "The online behaviors of Islamic state terrorists in the United States," *Criminology and Public Policy* (2021) https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12537?af=R; Chamin Herath, and Joe

Whittaker, "Online Radicalisation: Moving beyond a simply dichotomy," *Terrorism and Political Violence* (2021).
[27] Meleagrou-Hitchens and Kaderbhai, "Research Perspectives on Online Radicalisation"
[28] Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan, "Terrorist use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology and Public Policy*, 16, no. 1 (2017): 99-117.
[29] Amy-Louise Watkin, and Joe Whittaker, "Evolution of terrorists' use of the Internet," *Counter-Terror Business* (last modified October 20, 2017). https://counterterrorbusiness.com/features/evolution-terrorists%E2%80%99-use-internet.
[30] Petter Nesser, "How did Europe's global jihadis obtain training for their militant causes?" *Terrorism and Political Violence 20*, no.2 (2008): 234-256.
[31] Katherine Brown, and Elizabeth Pearson, "Social media, the online environment and terrorism," in *Routledge handbook of terrorism and counterterrorism,* ed. Andrew Silke, (London: Routledge, 2018).
[32] Dawn Branley, *"Risky behaviour: Psychological mechanisms underpinning social media users' engagement*" (Doctoral diss., Durham University, 2015). http://etheses.dur.ac.uk/11309/
[33] Gill, et al., "What are the roles of the internet in terrorism?"
[34] Michael Jensen, Patrick James, Gary LaFree, Aaron Safer-Lichtenstein, and Elizabeth Yates, "The use of social media by United States extremists," *National Consortium for the Study of Terrorism and Responses to Terrorism*, (2018). https://www.start.umd.edu/publication/use-social-media-united-states-extremists
[35] Ryan Scrivens, Thomas W. Wojciechowski, Joshua D. Freilich, Steven M. Chermak, and Richard Frank, "Comparing the online posting behaviors of violent and non-violent right-wing extremists," *Terrorism and Political Violence* (2021). https://www.tandfonline.com/doi/abs/10.1080/09546553.2021.1891893
[36] Jensen et al., "The use of social media by United States extremists"
[37] The SRG was a set of formal guidelines developed in 2009 for assessment of extremist offenders. Following independent evaluation (see Stephen Webster, Jane Kerr, and Charlotte Tompkins, *"A process evaluation of the structured risk guidance for extremist offenders: Final report"* (London, UK: Ministry of Justice Analytical Series, 2017)), the SRG was revised and renamed the ERG22+ in 2011.
[38] Described as 'close to' as the dataset included all SRG and ERG22+ reports available to the MoJ Research and Evaluation Team at the time of data collection, but it is possible some reports may not have been included.
[39] National Offender Management Service, *"ERG22+ & Extremism Risk Screen: Summary and overview"* (London: Ministry of Justice, 2017).
[40] Monica Lloyd, and Christopher Dean, "The development of structured guidelines for assessing risk in extremist offenders," *Journal of Threat Assessment and Management*, 2, (2015): 40–52.
[41] Beverly Powis, Kiran Randhawa, and Darren Bishopp, "An examination of the structural properties of the Extremism Risk Guidelines (ERG22+); a structured formulation tool for extremist offenders," *Terrorism and Political Violence* (2019) https://doi.org/10.1080/09546553.2019.1598392
[42] Beverly Powis, Kiran Randhawa-Horne, Ian Elliott, and Jessica Woodhams, *"Inter-rater reliability of the Extremism Risk Guidelines 22+ (ERG22+)"* (London, UK: Ministry of Justice Analytical Series, 2019). https://www.gov.uk/government/publications/inter-rater-reliability-of-the-extremism-risk-guidelines-22-erg-22
[43] Rita A. Knudsen, "Measuring radicalisation: risk assessment conceptualisations and practice in England and Wales," *Behavioral Sciences of Terrorism and Political Aggression* 12, no. 1, (2018): 37-54.
[44] Ibid.
[45] Martine Herzog-Evans, "A comparison of two structured professional judgment tools for violent extremism and their relevance in the French context," *European Journal of Probation* 10, no. 1 (2018): 3–27.
[46] Andrew Silke, "Risk assessment of terrorist and extremist prisoners," in *Prisons, terrorism and extremism: Critical issues in management, radicalisation and reform*, ed. Andrew Silke (London, Routledge, 2014), 108-121.
[47] Terrorist offences are those that fall under terrorism legislation (e.g., engage in the preparation of terrorist acts, membership of a proscribed organisation, dissemination of terrorist publications etc.).
[48] Terrorist-related offences are those that fall under other legislation, but where the motivation is considered extremist (e.g., murder, causing an explosion etc.).
[49] At the time of the study, the SRG and ERG22+ assessments had not been used within the Northern Ireland or Scottish Prison Service.
[50] Findings from this study required ministerial approval to disseminate and have only now become available for publication.
[51] Silke, "Risk assessment of terrorist and extremist prisoners"
[52] Fernando Reinares, Carola García-Calvo, and Alvaro Vicente, "Differential association explaining jihadi radicalisation in Spain: A quantitative study," *CTC Sentinel* 10, no. 6 (2017): 29-34.
[53] Paul Gill, and Emily Corner, "Lone-actor terrorist use of the Internet and behavioural correlates," in *Terrorism online: Politics, law, technology and unconventional violence*, eds. Lee Jarvis, Stuart Macdonald and

Thomas Chen, (London: Routledge, 2015), 35-53; Paul Gill, John Horgan, and Paige Deckert, "Bombing alone: tracing the motivations and antecedent behaviors of lone-actor terrorists," *Journal of Forensic Science* 59, no. 2 (2014): 425-435; Gill et al., "Terrorist use of the Internet by the Numbers"; Whittaker, "The online behaviors of Islamic state terrorists"

[54] Megan A. Moreno, Katie G. Egan, and Libby Brockman, (2011) "Development of a researcher codebook for use in evaluating social networking site profiles," *Journal of Adolescent Health* 49, no. 1 (2011): 29–35.

[55] Silke, "Risk assessment of terrorist and extremist prisoners"

[56] Paul Gill et al., "Bombing alone: tracing the motivations and antecedent behaviours"

[57] Gill and Corner, "Lone-actor terrorist use of the Internet and behavioural correlates"

[58] A dichotomous coding framework of 'yes' and 'no evidence' was preferred to a trichotomous coding framework of 'yes', 'no' and 'no evidence' as it was difficult to distinguish between missing data and variables that should be coded as 'no'.

[59] Watkin and Whittaker, "Evolution of terrorists' use of the Internet"

[60] Ibid.

[61] Koehler, "The radical online: Individual radicalization processes"

[62] Von Behr et al., "Radicalisation in the digital era"

[63] Whittaker, "The online behaviors of Islamic state terrorists"

[64] Gill et al., "What are the roles of the internet in terrorism," 35.

[65] Daniele Valentini, Anna M. Lorusso, and Achim Stephan, "Onlife extremism: Dynamic integration of digital and physical spaces in radicalisation," *Frontiers in Psychology*, 11, (2020): 524.

[66] Gill et al., "What are the roles of the internet in terrorism"

[67] Watkin and Whittaker, "Evolution of terrorists' use of the Internet"

[68] UK Home Office, *"Online harms white paper"* (Paper presented to Parliament by the Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department by command of Her Majesty, 2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf 12

[69] Stuart Macdonald, Daniel Grinnell, Anina Kinzel, and Nuria Lorenzo-Dus, "Daesh, Twitter and the Social Media Ecosystem," *The RUSI Journal* 164, No. 4 (2019): 60-72.

[70] Bennett Clifford, and Helen Powell, *"Encrypted Extremism: Inside the English-speaking Islamic State ecosystem on Telegram"* (Program on Extremism, the George Washington University, June 2019). https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf

[71] Samantha Weirman, and Audrey Alexander, "Hyperlinked Sympathizers: URLs and the Islamic State," *Studies in Conflict & Terrorism* 43, No. 3 (2020): 239-257.

[72] Scrivens and Conway, "The roles of 'old' and 'new' media tools and technologies"

[73] Bastug et al., "Exploring the 'demand side' of online," 169.

[74] Jensen et al., "The use of social media by United States extremists"

[75] Facebook, *"Dangerous individuals and organizations,"* (2020). https://www.facebook.com/communitystandards/recentupdates/dangerous_individuals_organizations

[76] Twitter, *"Violent organizations policy,"* (2020). https://help.twitter.com/en/rules-and-policies/violent-groups

[77] Stevens and Neumann, "Countering online radicalisation: A strategy for action"

[78] YouTube, *"Our Commitments,"* (undated). https://www.youtube.com/intl/ALL_uk/howyoutubeworks/?utm_campaign=1008960&utm_source=paidsearch&yt_product=ytgen&yt_goal=eng&utm_medium=googlesearch&utm_content=txt&yt_campaign_id=hyw&yt_creative_id=s&utm_keyword=youtube%20community%20guidelines&utm_matchtype=e&gclid=EAIaIQobChMIqYyiur2S8wIVjLTtCh26-g0tEAAYASABEgJccfD_BwE#our-products-and-policies

[79] Scrivens and Conway, "The roles of 'old' and 'new' media tools and technologies"

[80] J.M. Berger, and Jonathon Morgan, *"The ISIS Twitter Census - Defining and describing the population of ISIS supporters on Twitter,"* The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper, no. 20 (March 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

[81] Ibid.

[82] Elizabeth Pearson, and Emily Winterbotham, "Women, Gender and Daesh Radicalisation," *The RUSI Journal* 162, no. 3 (2017): 60-72. https://cronfa.swan.ac.uk/Record/cronfa43209

[83] Ibid.

[84] Jessica Davis, *"The future of the Islamic State's Women: assessing their potential threat,"* (ICCT Policy Brief, June 2020). https://icct.nl/publication/the-future-of-the-islamic-states-women-assessing-their-potential-threat/

[85] Gill, et al., "What are the roles of the internet in terrorism?"

[86] Scrivens et al., "Comparing the online posting behaviors of violent and non-violent right-wing extremists"

[87] Jensen et al., "The use of social media by United States extremists"
[88] Tanya Silverman, Christopher J. Stewart, Zahed Amanullah, and Jonathan Birdwell, "The impact of counter-narratives," *Institute for Strategic Dialogue*, (2016), https://www.isdglobal.org/wp-content/uploads/2016/08/Impact-of-Counter-Narratives_ONLINE_1.pdf
[89] National Counter Terrorism Security Office, *"Guidance online radicalisation"* (September 17, 2015). https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation
[90] Christian Montag, Haibo Yang, and Jon D. Elhai, "On the psychology of TikTok use: A first glimpse from empirical findings," *Frontiers in Public Health* 9, (2021): 641-673.
[91] Claudia Carvalho, "Okhti online: Spanish Muslim women engaging online jihad – a Facebook case study," *Online-Heidelberg Journal of Religions on the Internet* 6, (2014): 24–41; Sergio Sanchez, "*The Internet and the radicalisation of Muslim women"* (Paper presented at Annual Meeting of the Western Political Science Association, Seattle, Washington, April 2014). www.wpsanet.org/papers/docs/The%20Internet%20and%20the%20Radicalization%20of%20Muslim%20Women.pdf
[92] Radicalisation Awareness Network, "*RAN young issue paper – Policy recommendations"* (March, 2018). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/ran_young_policy_recommendations_032018_en.pdf