Computers in Human Behavior 168 (2025) 108646

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Identifying distinct types of internet use that predict the likelihood of planning or committing a terrorist attack: Findings from an analysis of individuals convicted on terrorism(-related) charges in England and Wales

Sandy Schumann [a,*], Jonathan Kenyon [b], Jens Binder [c]

[a] Department of Security and Crime Science, University College London, 35 Tavistock Square, London, WC1H 9EZ, United Kingdom
[b] HMPPS Counter Terrorism–Assessment and Rehabilitation Centre, Floor 8, 102 Petty France, London, SW1H 9AJ, United Kingdom
[c] Department of Psychology, Nottingham Trent University, Goldsmith St, Nottingham, NG1 4BU, United Kingdom

ARTICLE INFO

Handling editor: Marianna Sigala

Keywords:
Internet use
Terrorism
Radicalisation
Mobilisation
Risk assessment

ABSTRACT

Previous research has documented that the internet plays an increasingly important role in facilitating involvement in terrorism. However, the level of specificity of this literature is low. Advancing current insights, we examined how three concrete examples of active (i.e., generate/disseminate terrorist propaganda; interact with co-ideologues) and two examples of passive (i.e., learn about terrorist ideologies/actors; learn tactical information) internet use are related to distinct distal and proximal dynamics of radicalisation. Additionally, we assessed associations between the different types of internet use and the likelihood of having planned/committed a terrorist attack. We analysed a unique dataset based on closed-source risk assessment reports of individuals convicted of terrorism(-related) offences in England and Wales ($N = 377$). Results of this secondary data analysis pointed to three internet use repertoires: (1) learning about tactical information and terrorist ideologies/actors; (2) only learning about terrorist ideologies/actors; (3) active internet use and learning about terrorist ideologies/actors. Learning about tactical information and terrorist ideologies/actors was (compared to the other two repertoires) associated with a higher likelihood of having planned/committed an act of terrorism. Additionally, levels of capability were higher if individuals learnt both tactical and ideological information online compared to using the internet actively and browsing content about terrorist ideologies/actors. Individuals characterised by either internet use repertoire did, however, not vary significantly regarding their levels of engagement with extremist ideas and actors and the degree to which they had developed an extremist mindset. The results can inform terrorist/violent extremist risk assessment.

1. Introduction

Terrorism remains a threat to national and international security (Institute for Economics & Peace, 2024). Seeking to prevent and counter terrorist attacks, a burgeoning body of research has identified factors at the micro-, meso-, and macro-level that are thought to enhance or reduce individuals' propensity to adopt extremist beliefs (i.e., cognitive radicalisation) or commit acts of terrorism (i.e., behavioural radicalisation; Clemmow et al., 2020; LaFree & Schwarzenbach, 2021; Lösel et al., 2018; Sarma, Carthy, & Cox, 2022; Wolfowicz et al., 2021). The present study focuses on one individual-level risk factor that has received ample attention from scholars and practitioners alike (Whittaker, 2022; Wolfowicz et al., 2022): using the internet, for instance, to interact with co-ideologues, disseminate propaganda, as well as to access, be it through incidental exposure, ideological materials from terrorist actors (Baugut & Neumann, 2020; Gaudette, Scrivens, & Venkatesh, 2022; Kenyon et al., 2022; 2023) or information relevant for attack planning and preparation (Gill et al., 2017; Neumann, 2013; von Behr, Reding, Edwards, & Gribbon, 2013).

Summarising the literature, internet use – including all aforementioned examples – is viewed as a force enabler of involvement in terrorism (Binder & Kenyon, 2022). However, the level of specificity of the research is low (Brown et al., 2022). In other domains, it has been demonstrated that different modes of active and passive internet use are associated with differential outcomes as it pertains to civic and political participation, social capital, and mental health or wellbeing (Burke,

* Corresponding author.
E-mail address: s.schumann@ucl.ac.uk (S. Schumann).

https://doi.org/10.1016/j.chb.2025.108646
Received 20 December 2024; Received in revised form 11 March 2025; Accepted 16 March 2025
Available online 26 March 2025

Kraut, & Marlow, 2011; Kruikemeier et al., 2014; Orben et al., 2024; Verduyn et al., 2017, Verduyn, Gugushvili, & Kross, 2021; Wilkins et al., 2019). Similar insights have not been put forward when exploring the radicalising potential of the internet (Whittaker, 2021). We addressed this gap and assessed the extent to which three different types of active and passive internet use serve as distinct indicators or predictors of three distal and proximal dynamics of cognitive and behavioural radicalisation and, ultimately, a concrete terrorist activity, that is, planning or committing a terrorist attack (rather than being involved in terrorism in another way).

More precisely, generating or disseminating terrorist propaganda and interacting with co-ideologues – all examples of active internet use – indicate substantial motivation to adopt and engage with extremist beliefs or actors as well as a mindset that permits the use of violence (i.e., distal risk factors of cognitive radicalisation; Köhler, 2014; Mølmen & Ravndal, 2023; Smith et al., 2020). Employing the internet to learn about extremist/terrorist ideology – an example of passive internet use – also signifies that the person already endorses extremist beliefs and actors (Reeve, 2021; Schumann et al., 2024). However, to commit an act of terrorism, neither an elevated level of engagement with extremist/terrorist ideologies or actors nor an extremist mindset is sufficient. Individuals also require certain skills, knowledge, or material resources to select targets and employ weapons accurately (i.e., capability, a proximal risk factor of behavioural radicalisation; Beck, 2008; Brown et al., 2024; Edwards & McCarthy, 2004). Generating or disseminating terrorist propaganda, learning about ideological content, and interacting with co-ideologues, especially the former three, are not expected to facilitate increased levels of capability. By contrast, we hypothesised that in the absence of such information from sources 'offline', passive internet use to learn tactical information predicts enhanced levels of capability and is, compared to the other mentioned modes of internet use, also associated with a higher likelihood of preparing or committing a terrorist attack.

We tested our hypotheses by analysing a dataset that draws on closed-source information, namely, nearly all risk assessment reports completed between 2010 and 2021 of individuals convicted for terrorism or terrorism-related offences in England and Wales (Kenyon et al., 2022; 2023). Research based on such offender data is unique (Schuurman et al., 2018). Given the high ecological validity of this secondary data analysis, our results contribute to the literature exploring the radicalising potential of the internet and provide as well valuable practical insights for terrorist/violent extremist risk assessment.

2. Literature review

2.1. Internet use as a force enabler of radicalisation

Mirroring the ubiquity of digital and mobile technology in everyday life, the internet plays an increasingly important role in the preparation and planning of terrorist attacks as well as in the radicalisation process (e.g., Gill et al., 2017; Jensen, James, LaFree, Safer-Lichtenstein, & Yates, 2018; Kenyon et al., 2022; 2023). Gill and Corner (2015), for instance, examined online activities of 119 lone actors, convicted on terrorism charges between 1993 and 2011, and highlighted that from 1998 onwards, individuals had learnt more frequently from online sources about the ideology they endorsed or attack methods and had interacted more often with co-ideologues online. A study of individuals convicted of terrorism or terrorism-related offences in England and Wales between the early 2000s and 2021 further showed a steep incline in cases that were radicalised primarily or exclusively online since 2015; this group constituted 59 percent of individuals sentenced between 2019 and 2021(Kenyon et al., 2022).

Having said this, engaging with propaganda or interactions with like-minded others online does likely not outright replace but complements and extends 'offline drivers' of radicalisation (Herath & Whittaker, 2023). Internet activities might even have a weaker impact than offline influences: individuals convicted on terrorism(-related) charges whose radicalisation was solely or primarily driven by online sources rather than face-to-face contacts were found not only to be less engaged with an extremist group or cause but also displayed lower levels of intent and capability to commit a terrorist attack (Kenyon, Binder, & Baker-Beall, 2023). Moreover, regarding exposure to radicalising information, online and offline activities can be positively correlated (Whittaker, 2021). For example, individuals may be directed toward online materials after participating in offline interactions (Wojcieszak, 2009), and extremist online discussion forums can aid with forming connections and promote participation in offline meetings with co-ideologues (Gaudette et al., 2022). Lastly, Whittaker (2022) pointed out that "many of the behavio (u)rs that one might consider belonging to one domain cannot be easily demarcated" (p. 32). For instance, several cases of so-called viewing parties have been reported, where people would watch beheading videos on a phone together, offline (Baugut & Neumann, 2020). The term 'Onlife' (Floridi, 2015) has been introduced in this context to denote a hybrid space in which activities taking place in online and offline spheres are seamlessly fused (Valentini et al., 2020).

2.2. Specificity in research on online radicalisation

Taken together, previous research highlights that a wide range of online activities could constitute relevant, albeit not the sole, predictors or drivers of involvement in terrorism (e.g., Baugut & Neumann, 2020; Gaudette et al., 2022; Gill et al., 2017; Kenyon et al., 2022; 2023; Neumann, 2013; von Behr et al., 2013). Despite burgeoning work in this domain in recent years, one challenge has yet to be addressed: the level of specificity of studies on 'online radicalisation' remains low. For instance, Whittaker (2021) showed that among a sample of 231 US-based individuals who were affiliated with Islamic State and who had either committed or planned an attack or travelled to join ISIS more than four-fifths had interacted online with co-ideologues, more than a third had disseminated propaganda online, and 60 percent had used the internet for tactical purposes. Although insightful, these results do not allow conclusions as to whether interacting with co-ideologues online, for example, was equally relevant for prompting individuals to commit an attack as it was for facilitating travel to Syria or Iraq. Similarly, it is unknown whether retrieving tactical information online and interacting with co-ideologues enhanced someone's likelihood to plan an attack equally strongly.

Studies that investigated such questions – that is, specifying links between concrete independent (i.e., types or repertoires of internet use) and dependent variables (see Brown et al., 2022) – have been put forward in other domains (e.g., Burke et al., 2011; Kruikemeier et al., 2014). Verduyn and colleagues (2017), for example, proposed that activities on social media that enabled connections with other users foster social capital and a sense of connectedness, which would enhance the person's wellbeing. In turn, passively observing others' activities on social media without engaging with them was proposed to elicit upward social comparison and envy, reducing subjective wellbeing (Verduyn et al., 2017). A recent meta-analysis failed to support these precise mechanisms consistently but pointed nonetheless to differential associations between active and passive social media use and 13 wellbeing outcomes (Godard & Holtzman, 2024). The literature on social media use and wellbeing has also emphasised that crude measures of internet or social media use are not helpful in capturing dynamics accurately (Meier & Reinecke, 2020; Orben et al., 2024; Valkenburg et al., 2022).

Drawing on these insights, the present research sought to advance research on the radicalising potential of internet use. In doing so, unhelpful over-generalisation (i.e., statements like 'the internet facilitates radicalisation') is avoided. Instead, the conceptual understanding of *how* internet use shapes certain aspects of cognitive and behavioural radicalisation is improved, informing the development of holistic theoretical frameworks as well as the design of targeted countermeasures.

3. The present research

More precisely, we examined links between three specific modes of active and passive internet use, three concrete distal and proximal dynamics of cognitive and behavioural radicalisation, as well as one form of involvement in terrorism. Speaking to the former, we took into account using the internet to generate or disseminate terrorist propaganda or to interact with co-ideologues (i.e., active), to learn about extremist/terrorist ideology or actors, or to learn tactical information (i.e., passive).

The distal and proximal dynamics of radicalisation that we considered were conceptualised based on the Extremism Risk Guidance (ERG22+; Lloyd & Dean, 2015) that informs violent extremist/terrorist risk assessment in England and Wales – the context in which the data for the present study was collected. The ERG22+ examines 22 factors "which are believed to be related to extremist offending (the "+" in the title is a reflection that the model will consider other factors beyond the 22 if they are shown to be relevant to a particular case)" (Silke, 2024, p. 2) on three domains: Engagement, Intent, and Capability (Table 1). The dimension 'engagement' represents factors that enhance individuals' susceptibility to adopt extremist beliefs and the degree of involvement or identification with an extremist/terrorist actor (i.e., a process of commitment); the dimension 'intent' reflects the establishment of a mindset that permits and endorses the use of violence to advance an extremist/terrorist ideology and cause (i.e., emerging readiness to offend); having accumulated the necessary skills, capacity, resources, and networks to execute a terrorist attack is expressed through the dimension 'capability' (Lloyd & Dean, 2015). The dimensions and factors of the ERG22+ were developed based on theory, empirical evidence, as well as case experiences (Elliot et al., 2023; Powis et al., 2019; Silke, 2024). Importantly, it is not expected that all factors are present in all individuals who are involved in terrorism but that for all individuals some combination of factors facilitates their offending pathways.

3.1. Specifying associations: engagement and intent

To date, and to our knowledge, no study has systematically examined whether concrete online activities can indicate or predict increased engagement with terrorist actors and ideologies as well as the adoption of an extremist mindset. Nonetheless, previous research articulates a collection of relevant relationships. Notably, individuals who experience a loss of significance, social alienation and isolation, or uncertainty may be drawn to extremist online communities (e.g., forums, chats, channels) to interact with likeminded others who provide a sense of emotional support (De Koster & Houtman, 2008; Gaudette et al., 2022). Recognising that perceived individual or collective grievances are shared by others validates these sentiments and has been shown to elicit a sense of belonging to and identification with the relevant online community (Bliuc et al., 2019). Importantly, interactions in homogenous online communities enable social learning processes that can foster the consolidation of an extremist mindset (Köhler, 2014; Mølmen & Ravndal, 2023; Pauwels & Schils, 2016; von Behr et al., 2013). Smith and colleagues (2020) also highlighted that taking part in interactions with fellow ISIS supporters – especially interactions that focused on voicing anger, harm, and perceived threat, and that pointed to actions that can be taken to address grievances – predicted increased use of vernacular and linguistic style that conformed with that of the terrorist actor.

Generating and disseminating content that promotes extremist/terrorist ideology online is also expected to indicate a substantial level of engagement with terrorist actors and their worldview as individuals would otherwise experience cognitive dissonance (Festinger, 1957). Additionally, individuals should be aware that promoting extremist/terrorist ideology online is illegal, and they must consider the rewards of the activity higher than its risks. On the one hand, generating and disseminating content that promotes extremist/terrorist ideology could serve to vent frustrations, offering relief and making it possible to hold those who are thought to be responsible for the injustices accountable (Brady et al., 2021; Crockett, 2017). On the other hand, individuals may be encouraged to disseminate extremist/terrorist ideological content because they hope to receive endorsement from others who also support extremist views, which can boost their sense of significance (Köhler, 2014) and self-worth (De Koster & Houtman, 2008).

Learning (i.e., seeking information) about terrorist actors or ideologies is an example of passive internet use that has as well been found to be positively related to individuals' endorsement of violent extremist beliefs and violent extremist behavioural intentions (Schumann and Klein, 2015). Indeed, as individuals typically select information that aligns with their existing attitudes, browsing ideological content would suggest that a person supports extremist ideas and actors to an elevated extent (Slater, 2015). Furthermore, it has been documented, that those who choose to engage with online materials of extremist groups are more inclined to prefer hierarchy and dominance in society and exhibit stronger levels of outgroup hostility, that is, indicators of an extremist mindset (Reeve, 2021). In other words, similar to the aforementioned active forms of internet use, learning about extremist/terrorist actors and their ideologies could suggest that the individual has evolved in their engagement and might (come to) hold a mindset that permits the use of violence.

Table 1
Factors of the three ERG22+ dimensions.

Engagement	Intent	Capability
Need to redress injustice and express grievance	Over-identification with group and/or cause	Personal knowledge, skills, and competencies
Need to defend against threats	Us & them thinking	Access to networks, funding, and equipment
Identity, meaning & belonging	Dehumanisation of the enemy	Criminal history
Need for status	Attitudes that justify offending	
Excitement, comradeship & adventure	Harmful means to an end	
Need to dominate others	Harmful end objectives	
Susceptibility to indoctrination		
Political, moral motivation		
Opportunistic involvement		
Family and/or friends support extremism		
Transitional periods		
Group influence and control		
Mental health issues		

3.2. Specifying associations: capability

Both, elevated levels of engagement and intent, could predict a range of behaviours in support of terrorism, such as granting financial support or recruiting members for terrorist actors (Silke, 2024). However, developing a strong commitment to a terrorist ideology and intent to commit a terrorist attack are only necessary but not sufficient distal processes to enable the planning or execution of an act of terrorism. For the latter, individuals also need to develop capability, that is, gain relevant tactical, technical, and strategic knowledge (Oliver & Marwell, 1992), as well as gather material resources to acquire or construct weapons (i.e., resource mobilisation accounts of social movement theories; Beck, 2008; see also Brown et al., 2024). This knowledge and resources are not readily available to all individuals (Edwards & McCarthy, 2004). Having said this, the internet can alleviate some of the constraints, providing access to a wide range of internal and external sources (Cress & Snow, 1996). In fact, it has been shown that individuals

who committed more sophisticated terrorist attacks had more frequently researched information about weapons online (Gill et al., 2017).

3.3. Hypotheses

Summarising, we, thus, conclude the following hypotheses that stipulate unique and common patterns of association between three types of internet use, three distal and proximal processes of radicalisation, and one concrete form of involvement in terrorism. First, individuals who have employed the internet to learn tactical information are expected to have higher levels of capability than individuals who used the internet solely to interact with co-ideologues, to generate and disseminate content that endorses terrorist actors or ideologies, or to only learn about extremist/terrorist actors/ideologies (**Hypothesis 1**). Consequentially, and in line with resource mobilisation accounts (Beck, 2008; Edwards & McCarthy, 2004), individuals who drew on the internet to learn tactical information (as compared to engaging in other modes of internet use) should also exhibit a higher likelihood of having prepared or committed a terrorist attack (rather than being involved in terrorism in another way) (**Hypothesis 2**).

Lloyd and Dean (2015) noted that an elevated level of capability suggests a readiness to commit a terrorist attack, even if the reverse is not the case. In other words, learning about weapons and targets online is likely also associated with substantial levels of engagement and intent to commit a terrorist attack. Hence, as it pertains to the levels of engagement with terrorist ideology and the adoption of an extremist mindset, we have no reason to expect significant differences between those who used the internet to promote terrorist ideologies/actors or to interact with others who endorse terrorist ideologies, those who only learnt about terrorist actors/ideologies, and those who accessed tactical information online (**Hypothesis 3**).

4. Method

4.1. Data

To examine these hypotheses, we conducted a secondary analysis of a dataset that includes information about $N = 490$ individuals who were sentenced for an offence in England and Wales that was "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" (National Offender Management Service, 2011) or where there was sufficient concern that the individuals may have been drawn into terrorism (Kenyon et al., 2022; 2023). To compile this dataset, information on a wide range of variables was extracted from risk assessment reports, specifically, case formulations and background information from 488 Extremism Risk Guidance reports and two Structured Risk Guidance reports (Lloyd & Dean, 2015), which were completed between October 2010 and December 2021 by Registered Psychologists and qualified Probation Officers of His Majesty's Prison and Probation Service in England and Wales. The information provided in the reports draws on closed-source information as well as (with few exceptions) interviews and refers to the period during which the person had committed the offence. The full data collection and variable coding procedures are described in more detail in Kenyon et al. (2022). Approval was granted from the HM Prison and Probation Service National Research Committee to create a dataset based on data from the ERG22+ reports.

4.2. Sample

We excluded from the original dataset individuals for whom there was clear evidence that they had not entered prison holding extremist views. Further, we excluded cases where there was no evidence of any online activities pertaining to the individuals' radicalisation or attack planning. The final analytical sample included $N = 377$ individuals.

The majority of individuals were male (89 %; 11 % female). They were on average $M = 28$ ($SD = 8.6$) years old (range: 15–63); 69 % had been born in the UK (for 3 % of the sample this information was not reported). The risk assessment reports were completed between October 2010 and December 2021 but 12 % of individuals had been sentenced before that period. A total of 32 % of individuals had been sentenced between 2010 and 2015, 39 % were sentenced between 2016 and 2018, and 17 % had received their sentence between 2019 and 2021. An overview of the persons' index offences is presented in Supplementary Material (S1), which is available here: https://osf.io/k7wjz/?view_only=436ddb003bd84f898400251e7b61ea67. Individuals supported a range of ideologies: 75 % were classified as Islamist extremists, 18 % as right-wing extremists, 3 % were extremists who promoted animal rights, and 4 % endorsed various other political ideologies. Most individuals were affiliated with a larger group that included four or more people (53 %); 30 % were 'lone'; 16 % belonged to a small cell (two to three people) (for two cases this information was not reported).

4.3. Variables

We selected from the full dataset the following variables (further variables are presented in Kenyon et al., 2022).

4.3.1. Independent variables

A dichotomous variable indicated whether there was evidence that the individual had engaged either *in some form of active* or *only passive internet use*. Active internet use was operationalised as evidence of having: Interacted with co-ideologues online, Generated their own terrorist/extremist propaganda online (e.g. posting materials/videos online), or Disseminated propaganda. Passive internet use was operationalised as having either learnt about extremist/terrorist groups/ideology or attack methods/targets from online sources (but not through interactions with co-ideologues online). If there was any evidence of active use, this classification was chosen even if evidence for passive internet use was also identified. A further dichotomous variable specified whether passive internet use referred to *having learnt about extremist/terrorist groups/ideology* or *tactical information*.

4.3.2. Dependent variables

The dependent variable, *having planned or committed a terrorist attack*, reflected whether or not the individual had been 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 and was considered to be motivated by extremist views/beliefs (i.e., dichotomous variable). As a reminder, working with this specific dataset implies that all individuals engaged, in one way or another, in activities associated with terrorism; however, not all committed a terrorist attack. The key outcome variable of our analyses is not 'any involvement in terrorism' compared to 'no involvement in terrorism' but the likelihood of having prepared/planned or executed a terrorist incident rather than being involved in terrorism in another manner (see Table S1.1 in the Supplementary Material for index offences).

To capture the extent to which individuals exhibited *engagement with an extremist/terrorist ideology, cause, or actor*, we relied on the overall rating of the 'engagement' dimension of the ERG22+ assessment (e.g., Low, Low-medium, Medium, Medium -High, High). Additionally, the overall ratings of the dimension *intent*, that is, "the mind-set associated with a readiness to carry out or contribute to an extremist offence" (Lloyd & Dean, 2015, p. 42; Low, Low-medium, Medium, Medium-High, High) as well as the dimension *capability* to commit a terrorist offence with the potential to cause serious harm (Minimal, Minimal-some, Some, Some-significant, Significant) as reported in the ERG22+ were employed for the analysis. These overall ratings are not merely the sum of ratings of the dimension's factors but reflect the assessor's professional judgment and their full impression of the person's "risk 'story'"

(Lloyd & Dean, 2015, p. 46). For robustness checks, we included a further dichotomous variable that indicated whether there was evidence that the individual's radicalisation had taken place *exclusively/primarily online* or included *also face-to-face contact* (i.e., hybrid).

5. Results

Due to its sensitivity and it having been developed based on closed-source information, the dataset is not publicly available and cannot be shared upon request. The data owner is His Majesty's Prison and Probation Service, and they have facilitated this research.

5.1. Descriptive analysis

A total of $n = 109$ individuals (29 % of the sample) had either prepared or committed a terrorist attack; $n = 31$ of those completed the attack and $n = 78$ were intercepted. A larger proportion of the sample was described as an active ($n = 275$) rather than solely a passive ($n = 102$) internet user. To explore the distribution of active and passive internet use further, we examined trends over the last two decades (i.e., as per individual's sentencing date). Table 2 documents that the number of people being sentenced as well as the relative proportion of active internet users amongst those who were sentenced has increased steadily over time.

Importantly, and as alluded to in previous research (Schuurman, 2020), for $n = 238$ of the $n = 275$ active internet users, there was evidence that they had also used the internet to learn about extremist/terrorist ideology or groups ($n = 190$) or to learn tactical information ($n = 48$). Of the $n = 102$ individuals who were classified as passive internet users (i.e., there was no evidence of active internet use), the majority browsed only ideological content ($n = 67$), and $n = 33$ individuals used the internet to learn about tactical information (note: there is strong evidence that most of these individuals also learnt about extremist/terrorist ideology and actors). These findings highlight one of the intricacies of working with observational data that we will reflect on when discussing the results, that is, the sub-samples of individuals who used the internet in different ways overlap partially or, in other words, different types of internet use behaviours were often combined. For the hypotheses tests it is, therefore, more accurate to state that we compared in the present research sub-samples who: a) employed the internet to only access ideological content, b) learnt primarily tactical information but also about extremist/terrorist ideology and actors, and c) engaged with co-ideologues and disseminated extremist/terrorist propaganda as well as learnt about extremist/terrorist ideology/actors online.

The relative frequencies of overall engagement, intent, and capability ratings are outlined in Table 3. The sample was highly engaged and characterised by substantial levels of intent as well as capability. It should be noted that this granular description (Table 3) was chosen to present more nuance. Going forward, the dimension ratings were treated as continuous variables.

5.2. Hypotheses tests

Hypothesis 1 proposed that the level of capability is higher for those who used the internet to learn about tactical information as compared to individuals who learnt only about extremist/terrorist ideology/actors online or who engaged in any form of active internet use. An univariate analysis of variance with a Bonferroni-corrected alpha of .017 as a threshold pointed indeed to a significant between-group difference ($F(2, 323) = 6.17$, $p = 0.002$, $\eta_p^2 = 0.04$; Fig. 1). Post-hoc tests with Tukey HSD correction further confirmed that overall capability ratings were significantly lower in the sub-sample of active internet users ($M = 1.97$; $SD = 1.21$) than the sub-sample of passive internet users who retrieved tactical information ($M = 2.77$; $SD = 1.33$); mean difference = 0.80 ($SE = 0.24$), $p = 0.003$. Other between-group comparisons, namely, with the sub-sample of passive internet users who only accessed ideological materials ($M = 2.26$; $SD = 1.28$), did, however, not yield statistically significant outcomes (active vs. passive (access only ideological materials) internet users: mean difference = 0.29 ($SE = 0.18$), $p = 0.249$; passive (retrieve tactical information) vs. passive (access only ideological materials) internet users: mean difference = −0.51 ($SE = 0.28$), $p = 0.16$). Thus, Hypothesis 1 was only partially supported.

As a robustness test, we examined Hypothesis 1 separately for individuals whose radicalisation pathway was set exclusively/primarily online and for those who were radicalised in hybrid settings – the latter could suggest that offline sources elevated levels of capability. For individuals whose radicalisation was exclusively or primarily driven by information or actors with whom they engaged online ($n = 97$; $n = 80$ were active internet users), the main effect of between-group difference was not replicated ($F(2, 94) = .27$, $p = .766$, $\eta_p^2 = .006$), even though the general trends of average capability ratings in each sub-sample reflected those of the main analysis (active internet use: $M = 1.50$ [$SD = 1.14$]; passive (access only ideological materials): $M = 1.50$ [$SD = 1.16$]; passive (retrieve tactical information): $M = 2.00$ [$SD = 2.00$]). The same nil main effect was shown in the sub-sample characterised by a hybrid radicalisation pathway ($n = 176$; $n = 125$ were active internet users): $F(2, 173) = 2.20$, $p = .114$, $\eta_p^2 = .025$) (active internet use: $M = 2.09$ [SD

Table 2
The proportion of active and passive internet users in the sample as per sentencing date.

Sentencing Date	*n*	Active internet users (%)	Passive internet users (%)
Pre 2007	4	0	100
2007–2009	40	55	45
2010–2012	36	67	33
2013–2015	85	56	44
2016–2018	147	85	15
2019–2021	65	86	14

Table 3
Overall engagement, intent, and capability ratings.

Overall rating	Engagement ($n = 316$)	Intent ($n = 322$)	Overall rating	Capability ($n = 326$)
Low	5.4 %	16.5 %	Minimal	16.9 %
Low-medium	1.6 %	2.8 %	Minimal-some	1.5 %
Medium	37.0 %	44.1 %	Some	58.6 %
Medium-high	4.7 %	2.8 %	Some-significant	1.2 %
High	51.3 %	33.9 %	Significant	21.8 %

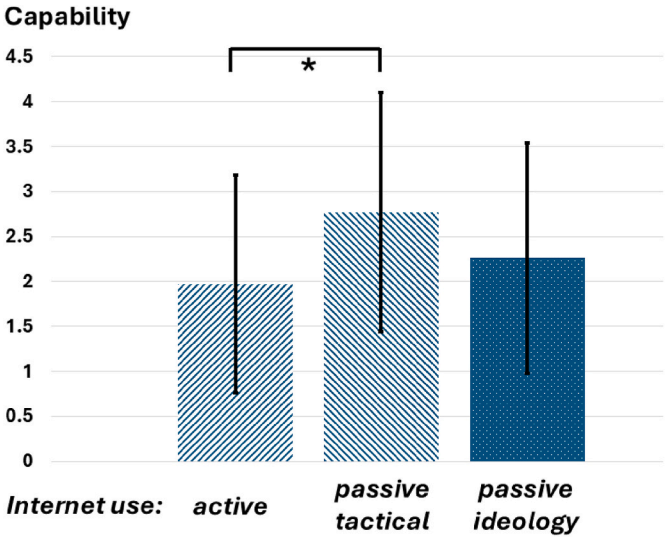

Fig. 1. Between-group differences in capability ratings.

= 1.15]; passive (access only ideological materials): $M = 2.44$ [$SD = 1.28$]; passive (retrieve tactical information): $M = 2.60$ [$SD = 1.18$]). These outcomes are puzzling but might be explained by the (lower) statistical power in the two analyses, which, due to the observational nature of the data, were based on unequal group sizes. In fact, the analysis of those who were exclusively or primarily radicalised online included only three persons who had used the internet to learn about tactical information, rendering these results less informative than we had hoped.

To test Hypothesis 2, we first conducted a two-sided chi-square test comparing 'active/passive internet users' with respect to the likelihood of having planned or committed a terrorist attack rather than being involved in terrorism in another way. Results highlighted that active internet users were significantly less likely to have planned or committed an attack than passive internet users (49 % passive internet users compared to 21 % active internet users); $\chi^2(1) = 27.51$, $p < .001$ (Fig. 2). These patterns were supported in a robustness test, replicating the analyses in the sub-sets of individuals who were either described as having had a primarily online or a hybrid radicalisation pathway (online pathway ($n = 107$): χ^2 (1) = 4.93, $p = .026$; hybrid pathway ($n = 204$): χ^2 (1) = 17.00, $p < .001$). Importantly, and in line with Hypothesis 2, an additional chi-square test demonstrated that individuals who used the internet passively to learn about targets or attack methods were more likely to have prepared or executed an attack than individuals who used the internet only to retrieve ideological content or those who used the internet to generate/disseminate content and interact with co-ideologues, χ^2 (2) = 62.41, $p < .001$ (retrieving tactical information: 86 % had prepared/committed an attack; learning ideological content: 30 % had prepared/committed an attack; active internet use: 21 % had prepared/committed an attack).

Lastly, we conducted two univariate analyses of variance to assess Hypothesis 3, that is, differences in overall engagement and intent ratings. As expected, and endorsing Hypothesis 3, considering the three sub-samples that represented different internet use repertoires, we identified no significant between-group differences for these two dependent variables (engagement: $F(2, 313) = .126$, $p = .882$, $\eta_p^2 = .001$; intent: $F(2, 319) = 1.26$, $p = .284$, $\eta_p^2 = .008$).

5.3. Further exploratory analyses

As the sample represented individuals with a range of ideological leanings, we concluded the analyses by exploring whether the previously shown trends could be identified in the two larger ideological sub-samples: right-wing extremists ($n = 68$) and Islamist extremists ($n = 281$).

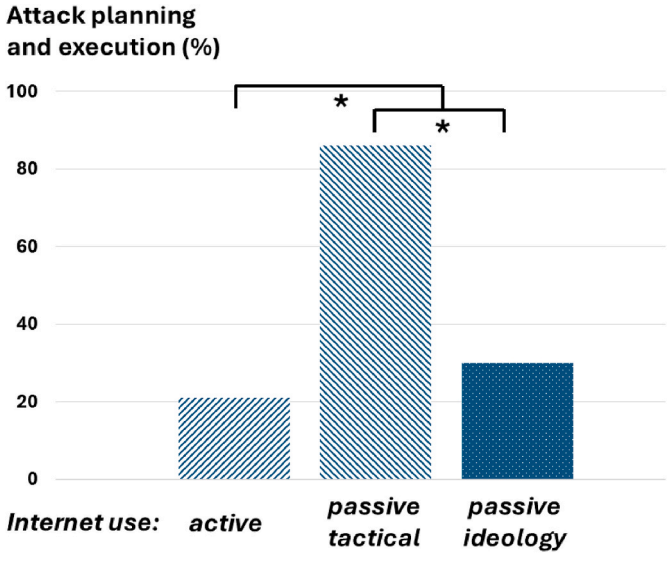

Fig. 2. Between-group differences in the likelihood to have planned/prepared an attack.

For the right-wing extremist sub-sample ($n = 68$; $n = 47$ active internet users, $n = 5$ passive (access only ideological materials), $n = 7$ passive (retrieve tactical information)), we showed no significant between-group differences regarding engagement ($F(2, 56) = 1.15$, $p = .325$, $\eta_p^2 = .039$), intent ($F(2, 57) = 1.36$, $p = .266$, $\eta_p^2 = .045$), and capability ($F(2, 56) = 2.58$, $p = .085$, $\eta_p^2 = .084$) ratings. Again, we must consider the low statistical power of these analyses. Having said this, those who used the internet passively to learn about targets or attack methods were more likely to have prepared or committed a terrorist attack than individuals who used the internet only to retrieve ideological content or to generate/disseminate content and interact with co-ideologues, χ^2 (2) = 11.17, $p < .05$ (retrieving tactical information: 88 % had prepared/committed an attack; learning ideological content: 60 % had prepared/committed an attack; active internet use: 29 % had prepared/committed an attack).

Similarly, in the sub-sample of Islamist extremists ($n = 281$; $n = 173$ active internet users, $n = 51$ passive (access only ideological materials), $n = 18$ passive (retrieve tactical information)), individuals who were characterised by different internet use behaviours did not differ regarding the overall engagement ($F(2, 229) = 1.20$, $p = .303$, $\eta_p^2 = .010$) and intent ($F(2, 233) = 2.08$, $p = .128$, $\eta_p^2 = .018$). However, we documented a main effect (albeit exactly at the Bonferroni-corrected alpha level) for the dependent variable 'capability', $F(2, 239) = 4.14$, $p = .017$, $\eta_p^2 = .033$. Tukey HSD corrected post-hoc tests showed that active internet users had overall lower capability ratings ($M = 1.84$; $SD = 1.20$) than those who used the internet passively to retrieve tactical information ($M = 2.61$; $SD = 1.34$); mean difference = −.77 (SE = .31), $p = .032$. Between-group differences pertaining to the sub-sample of passive internet users who only accessed ideological materials ($M = 2.18$; $SD = 1.29$) were not statistically significant (active vs. passive (access only ideological materials) internet users: mean difference = −.34 (SE = .20), $p = .199$; passive (retrieve tactical information) vs. passive (access only ideological materials) internet users: mean difference = .43 (SE = .34), $p = .404$). Employing the internet passively to learn about targets or attack methods was associated with a higher likelihood of having prepared or committed an act of terrorism than using the internet only to retrieve ideological content or using the internet actively, χ^2 (2) = 44.62, $p < .001$ (retrieving tactical information: 86 % had prepared/committed an attack; learning ideological content: 27 % had prepared/committed an attack; active internet use: 19 % had prepared/committed an attack).

6. Discussion

Drawing on a unique dataset that was compiled based on closed-source information, the present study contributes to a burgeoning literature that documents that the internet plays an increasingly important role in facilitating involvement in terrorism (Baugut & Neumann, 2020; Gaudette et al., 2022; Gill et al., 2017; Kenyon et al., 2022; 2023; von Behr et al., 2013). Namely, we examined associations between three concrete types of internet use, three distal and proximal dynamics of radicalisation, and one specific form of involvement in terrorist activities to illustrate how more specificity can be introduced in studies that address this problem space. Below we discuss all key findings and reflect on why our analytical approach is valuable. We also explore limitations and wider implications.

6.1. Review of key findings

Firstly, descriptive analyses demonstrated that the assessed examples of active internet use – generating and disseminating content that supports extremist/terrorist ideologies or interacting with co-ideologues – became more prevalent over time and were since the mid-2000s more

common than mere passive internet use among individuals convicted on terrorism(-related) offences in England and Wales. It must be noted that this trend likely reflects changes in behaviour as much as changes in terrorism legislation (i.e., the introduction of the Terrorism Act 2006), that is, the dissemination of extremist/terrorist content is now an index offence based on which individuals are convicted. Nonetheless, the observation also confirms previous work conducted in other jurisdictions. Jensen and colleagues (2018) found, based on data gathered in the US between 2005 and 2016, that about half of a sample of extremists had shared extremist materials or interacted with co-ideologues online respectively, and around 20 percent had generated extremist content themselves. Drawing on a typology of individuals who engage with/-promote hate speech online (Jacks & Adler, 2015), our results suggest that a substantial proportion of the individuals that were included in the present analysis can be described as Commentators (i.e., sharing content produced by others), Activists (i.e., sharing their own content), and possibly Leaders (i.e., establishing the infrastructure for extremist/terrorist content online). Additionally, and perhaps stating the obvious, just like digital technology itself, we conclude that the ways in which individuals use the internet to be involved in terrorism change over time, requiring scholars and practitioners to continuously update the online practices that they consider (e.g., live streaming of attacks or the use of generative artificial intelligence are a (not so) recent examples of internet use by terrorist actors).

Reviewing the prevalence of different types of active and passive internet use, it was also apparent that most of those who we had categorised as active internet users also used the internet passively to browse ideological materials. Further, most who retrieved tactical information online also learnt about extremist/terrorist ideology or actors. On the one hand, we confirm that consuming ideological content is common among the vast majority of individuals who were convicted of terrorism(-related) offences in England or Wales; this is, however, not to say that accessing and being exposed to extremist/terrorist ideological materials *causes* cognitive or behavioural radicalisation directly (Schumann et al., 2024). On the other hand, and although we sought to impose a classification of either active or passive internet use, it is evident that individuals typically engaged in several different internet use behaviours pertaining to terrorist actors, ideologies, and methods. The three documented patterns (i.e., active use and passive use to learn about extremist/terrorist ideology/actors, passive use only to access ideological materials and information about extremist/terrorist ideology/actors, passive use primarily to learn tactical information but also to access ideological materials and learn about extremist/terrorist ideology/actors) are, therefore, best conceptualised as media repertoires, a term that describes the combinations of sources and content that individuals regularly employ to address various needs (Ferguson & Perse, 1993; Yuan, 2011). There is evidence to suggest that particular media repertoires are associated with distinct user characteristics as well as behavioural outcomes (e.g., Dvir-Gvirsman, 2022; Kim, 2014). Notably, Dvir-Gvirsman (2022) identified four profiles of social media and traditional media news users and showed between-class differences in levels of political participation.

Similarly, in line with Hypothesis 2, we demonstrated that the likelihood of having prepared or committed a terrorist attack rather than being involved in terrorism in another way was significantly higher for the sub-sample that had used the internet passively to primarily retrieve tactical information and to access as well ideological content. In turn, and resonating with previous research (Brown et al., 2024), we highlighted that merely browsing ideological content – which is typically not easily observable – as well as an active internet use repertoire – which is more observable and perhaps appealing to analyse (e.g., Smith et al., 2020; Torregrosa, Thorburn, Lara-Cabrera, Camacho, & Trujillo, 2020) – are perhaps less valid indicators of a person's higher risk of engaging in a terrorist attack.

The results complement a small number of studies that identified unique patterns of posting behaviour in online forums for violent and non-violent extremists. For instance, over time, the frequency of posting declined for violent right-wing extremists but remained fairly stable for non-violent right-wing extremists (Scrivens et al., 2022, 2023). Further, written posts of non-violent right-wing extremists did not differ from those of violent individuals with respect to the prevalence of ideological content (Brown et al., 2024). Violent right-wing extremists, however, were more likely to discuss violent action directly (Brown et al., 2024). Emphasising the advantage of increased specificity in study designs, that is, comparing trends for several concrete internet use behaviours or repertoires, this research and our results point out that certain online activities signal individuals' potential use of violence, while others are less likely to help distinguish between those who 'only' hold extremist beliefs and those who will act on them violently. Frontline practitioners benefit from these conclusions, which will be discussed in more detail below.

Before doing so, it is important to note that our study did not test why those who used the internet passively primarily to learn tactical information and access ideological content were also more likely to plan or commit a terrorist attack. The observational nature of the data would not allow such strong causal conclusions, and the small sub-samples hamper the implementation of path models to investigate indirect effects. However, we can carefully put forward one and reject two avenues of explanation, referring to the three distal and proximal dynamics of radicalisation that we explored. Firstly, supporting Hypothesis 3, we showed that neither of the assessed repertoires of internet use predicted significantly elevated levels of engagement with terrorist ideology and actors nor a significantly stronger extremist mindset. For instance, those who only browsed ideological content were not significantly less committed to an extremist/terrorist actor than those who used the internet as well actively to interact with co-ideologues or disseminate content. These nil findings are not trivial as they denote that for a sample that was convicted on terrorism(-related) charges, the three internet use repertoires did not reflect variation in distal processes of radicalisation. In turn, we speculate that differences in levels of engagement and intent do *not* underlie, or mediate, the association between passive internet use that includes the retrieval of tactical information and the increased likelihood of attack preparation and execution that we observed.

Having said this, and partially endorsing Hypothesis 1, capability ratings were higher for those who learnt about tactical information (and ideological materials) online than for individuals who were classified as active internet users, including in a sub-sample that was exclusively or primarily radicalised online and where there was a lack of evidence that offline sources could have provided insights about weapons, targets, or resources. In line with resource mobilisation accounts (Beck, 2008; Cress & Snow, 1996; Edwards & McCarthy, 2004), this finding could be interpreted as such that the retrieval of tactical information elevated levels of capability and, therefore, increased the likelihood of the planning/execution of attacks. This conclusion, however, would be too simplistic. We agree that we provide evidence that suggests that discussions on the radicalising potential of the internet should focus more on proximal processes, especially on the ability to increase individuals' capability (Brown et al., 2024), rather than assess only changes in attitudes or group identification (Schumann et al., 2021; Smith et al., 2020). Nonetheless, confounding processes must be acknowledged. Crucially, although browsing tactical information can elevate the level of capability, it jeopardises individuals' operational security, a concern voiced by former extremists (Gaudette et al., 2022). In fact, a previous study showed that individuals who employed the internet to interact with co-ideologues, to disseminate propaganda, or for attack planning were overall more likely to have been known to security services or be arrested (Whittaker, 2021).

6.2. Limitations

This discussion of the results must be considered in light of the following challenges. As noted earlier, to test our hypotheses strictly, a

clear differentiation of the sample into a group of active and passive internet users would have been required. The observational data did not allow for such a strict distinction. We accept this limitation given the high ecological validity of the observational data. Relatedly, it must be noted that the observed between-group differences do not point to causal effects, and even correlational predictive associations must be taken carefully as confounding and intermediate mediating variables were not included as covariates.

The procedure that was employed to construct the dataset is not without limitations either (see also Kenyon et al., 2022). Namely, the data is based on risk assessment reports. Although the reports included more information than open-source data that previous studies have often employed (e.g., Gill et al., 2017; von Behr et al., 2013), both types of data struggle to distinguish missing from absent data. Missing data could be the result of information not being provided or not being recorded accurately. In our study, this limitation will likely affect especially the variables that identified internet use behaviour and repertoires. Thus, some individuals in our sample were perhaps misclassified as passive internet users or as *not* having browsed for tactical information; others might have been excluded altogether because no internet use was recorded in the risk assessment report.

Additionally, we focused the analyses on a specific period and location. Without conceptual replication, results should not be generalised to other settings where legislation defines terrorism and terrorism (-related) offences differently. We also recommend an updated analysis at a later point with individuals who were convicted in England and Wales as internet use behaviours might have changed further.

6.3. Implications and conclusion

Despite these challenges, we believe that our work makes an important contribution to the literature. Reflecting on our results suggests an avenue for future research that would contribute to developing an overarching theoretical framework that articulates the role of the internet for cognitive and behavioural radicalisation. As a reminder, we documented that higher specificity of study designs in this problem space is valuable as it points out internet use behaviours or repertoires that indicate increased levels of risk of violence as well as candidates of relevant underlying mechanisms. We suggest that this work is extended to assess a broader set of independent and dependent variables and apply a temporal perspective to distinguish different (iterative) phases of the radicalisation process. Orben and colleagues' (2024) review article provides an example of a guiding framework. Referring to the well-being implications of young people's social media use, affordances such as anonymity, editability, and synchronicity are, based on empirical evidence, linked with concrete neurobiological, cognitive, and behavioural mechanisms and outcomes that are known to increase young people's mental health vulnerability (Orben et al., 2024). In the first instance, we encourage work that similarly systematises and quantifies how specific affordances of digital technology, as well as concrete repertoires of internet use for involvement in terrorism, relate to established or proposed risk and protective factors of cognitive and behavioural radicalisation, such as a quest for significance, cognitive inflexibility, or inclusion in homogenous communities (Wolfowicz et al., 2021; see Binder & Kenyon, 2022 for a narrative review). Much of this work will likely be interdisciplinary and draw on research in communication science and media studies. This review exercise will reveal what further primary research is required to consolidate functional links that have thus far been ignored.

Moving to a discussion of the study's relevance for practice, the findings underscore the need for more nuanced, behaviour-based monitoring practices in threat and risk assessment that account for diverse internet use repertoires among individuals involved in terrorism-related activities. Specifically, policies that prioritise identifying individuals who engage in the retrieval of tactical information may improve the accuracy of threat detection. For intervention, rehabilitation, and reintegration, policies could more effectively target internet use patterns correlated with recidivism risk, particularly for younger audiences and vulnerable populations. Structured internet use restrictions in the form of licence conditions or controlled re-entry into safe online spaces coupled with media literacy and digital behaviour modification strategies could also be implemented, guided by the documented risk associated with certain internet behaviours. Moreover, law enforcement agencies could benefit from adopting a capability-oriented approach to threat assessment, focusing on online behaviours such as researching weapons and targets, rather than the consumption of ideological content. Supporting this shift may require investment in training programmes to equip frontline practitioners with the skills to recognise diverse internet use patterns, thereby improving their ability to identify individuals at heightened risk of violent action.

In conclusion, drawing on a unique dataset of individuals who were convicted on terrorism(-related) charges in England and Wales, we illustrated how more specificity can be introduced in research that examines the radicalising potential of the internet. In doing so, we identified an internet use repertoire – primarily retrieving tactical information and browsing ideological materials – that was associated with increased levels of capability as well as a higher likelihood of having planned or executed a terrorist attack. Pointing to concrete internet use that signals an elevated risk of violence is crucial for practitioners who will benefit from considering these activities in the context of wider risk assessment to prevent and counter the threat of terrorism.

CRediT authorship contribution statement

Sandy Schumann: Writing – review & editing, Writing – original draft, Project administration, Conceptualization. **Jonathan Kenyon:** Writing – review & editing, Formal analysis, Data curation, Conceptualization. **Jens Binder:** Writing – review & editing, Methodology, Data curation, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.chb.2025.108646.

Data availability

The data that has been used is confidential.

References

Baugut, P., & Neumann, K. (2020). Online propaganda use during Islamist radicalization. *Information, Communication & Society, 23*(11), 1570–1592. https://doi.org/10.1080/1369118X.2019.1594333

Beck, C. J. (2008). The contribution of Social Movement Theory to understanding terrorism. *Sociology Compass, 2*(5), 1565–1581. https://doi.org/10.1111/j.1751-9020.2008.00148.x

Binder, J. F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in Psychology, 13*, Article 997390. https://doi.org/10.3389/fpsyg.2022.997390

Bliuc, A.-M., Betts, J., Vergani, M., Iqbal, M., & Dunn, K. (2019). Collective identity changes in far-right online communities: The role of offline intergroup conflict. *New Media & Society, 21*(8), 1770–1786. https://doi.org/10.1177/1461444819831779

Brady, W. J., McLoughlin, K., Doan, T. N., & Crockett, M. J. (2021). How social learning amplifies moral outrage expression in online social networks. *Science Advances, 7*(33), Article eabe5641. https://doi.org/10.1126/sciadv.abe5641

Brown, O., Smith, L. G. E., Davidson, B. I., & Ellis, D. A. (2022). The problem with *the internet*: An affordance-based approach for psychological research on networked technologies. *Acta Psychologica, 228*, Article 103650. https://doi.org/10.1016/j.actpsy.2022.103650

Brown, O., Smith, L. G. E., Davidson, B. I., Racek, D., & Joinson, A. (2024). Online signals of extremist mobilization. Retrieved from https://journals.sagepub.com/doi/full/10.1177/01461672241266866.

Burke, M., Kraut, R., & Marlow, C. (2011). Social capital on facebook: Differentiating uses and users. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* (pp. 571–580). https://doi.org/10.1145/1978942.1979023

Clemmow, C., Schumann, S., Salman, N. L., & Gill, P. (2020). The Base Rate Study: Developing base rates for risk factors and indicators for engagement in violent extremism. *Journal of Forensic Sciences, 65*(3), 865–881. https://doi.org/10.1111/1556-4029.14282

Cress, D. M., & Snow, D. A. (1996). Mobilization at the margins: Resources, benefactors, and the viability of homeless social movement organizations. *American Sociological Review, 61*(6), 1089–1109. https://doi.org/10.2307/2096310

De Koster, W., & Houtman, D. (2008). 'STORMFRONT IS LIKE A SECOND HOME TO ME' On virtual community formation by right-wing extremists. *Information, Communication & Society, 11*(8), 1155–1176.

Dvir-Gvirsman, S. (2022). Understanding news engagement on social media: A media repertoire approach. *New Media & Society, 24*(8), 1791–1812. https://doi.org/10.1177/1461444820961349

Edwards, B., & McCarthy, J. D. (2004), *The Blackwell companion to social movementsResources and social movement mobilization* (pp. 116–152).

Elliott, I. A., Randhawa-Horne, K., & Hambly, O. (2023). Extremism Risk Guidance 22+: An exploratory psychometric analysis. *Ministry of Justice Analytical Series*. Available at: https://www.gov.uk/government/publications/extremism-risk-guidance-22-an-exploratory-psychometric-analysis.

Ferguson, D. A., & Perse, E. M. (1993). Media and audience influences on channel repertoire. *Journal of Broadcasting & Electronic Media, 37*(1), 31–47. https://doi.org/10.1080/08838159309364202

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.

Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era.* Springer nature.

Gaudette, T., Scrivens, R., & Venkatesh, V. (2022). The role of the internet in facilitating violent extremism: Insights from former right-wing extremists. *Terrorism and Political Violence, 34*(7), 1339–1356. https://doi.org/10.1080/09546553.2020.1784147

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers. *Criminology & Public Policy, 16*(1), 99–117. https://doi.org/10.1111/1745-9133.12249

Godard, R., & Holtzman, S. (2024). Are active and passive social media use related to mental health, wellbeing, and social support outcomes? A meta-analysis of 141 studies. *Journal of Computer-Mediated Communication, 29*(1), Article zmad055. https://doi.org/10.1093/jcmc/zmad055

Herath, C., & Whittaker, J. (2023). Online radicalisation: Moving beyond a simple dichotomy. *Terrorism and Political Violence, 35*(5), 1027–1048. https://doi.org/10.1080/09546553.2021.1998008

Institute for Economics & Peace. (2024). *Global Terrorism Index Report*. Available at: https://www.visionofhumanity.org/maps/global-terrorism-index/#/.

Jacks, W., & Adler, J. R. (2015). *A proposed typology of online hate Crime* (Vol. 7).

Jensen, Michael, James, Patrick, LaFree, Gary, Safer-Lichtenstein, Aaron, & Yates, Elizabeth (2018). *The use of social media by United States extremists*. National Consortium for the Study of Terrorism and Responses to Terrorism. https://www.start.umd.edu/publication/use-social-media-united-states-extremists.

Kenyon, J., Baker-Beall, C., & Binder, J. (2023). Lone-Actor terrorism – a systematic literature review. *Studies in Conflict & Terrorism*. https://www.tandfonline.com/doi/abs/10.1080/1057610X.2021.1892635.

Kenyon, J., Binder, J., & Baker-Beall, C. (2022). Understanding the role of the internet in the process of radicalisation: An analysis of convicted extremists in England and Wales. *Studies in Conflict & Terrorism, 0*(0), 1–25. https://doi.org/10.1080/1057610X.2022.2065902

Kenyon, J., Binder, J. F., & Baker-Beall, C. (2023). Online radicalization: Profile and risk analysis of individuals convicted of extremist offences. *Legal and Criminological Psychology, 28*(1), 74–90. https://doi.org/10.1111/lcrp.12218

Kim, S. J. (2014). *A repertoire approach to cross-platform media use behavior*. New Media & Society. https://doi.org/10.1177/1461444814543162

Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the internet. *Journal for Deradicalization, 1*, Article 1.

Kruikemeier, S., van Noort, G., Vliegenthart, R., & de Vreese, C. H. (2014). Unraveling the effects of active and passive forms of political Internet use: Does it affect citizens' political involvement? *New Media & Society, 16*(6), 903–920. https://doi.org/10.1177/1461444813495163

LaFree, G., & Schwarzenbach, A. (2021). Micro and macro-level risk factors for extremism and terrorism: Toward a criminology of extremist violence. *Monatsschrift für Kriminologie und Strafrechtsreform, 104*(3), 184–202. https://doi.org/10.1515/mks-2021-0127

Lloyd, M., & Dean, C. (2015). The development of structured guidelines for assessing risk in extremist offenders. *Journal of Threat Assessment and Management, 2*(1), 40–52. https://doi.org/10.1037/tam0000035

Lösel, F., King, S., Bender, D., & Jugl, I. (2018). Protective factors against extremism and violent radicalization: A systematic review of research. *International Journal of Developmental Science, 12*(1–2), 89–102. https://doi.org/10.3233/DEV-170241

Meier, A., & Reinecke, L. (2020). Computer-mediated communication, social media, and mental health: A conceptual and empirical meta-review. *Communication Research*. https://doi.org/10.1177/0093650220958224

Mølmen, G. N., & Ravndal, J. A. (2023). Mechanisms of online radicalisation: How the internet affects the radicalisation of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression, 15*(4), 463–487. https://doi.org/10.1080/19434472.2021.1993302

Neumann, P. R. (2013). Options and strategies for countering online radicalization in the United States. *Studies in Conflict & Terrorism, 36*(6), 431–459. https://doi.org/10.1080/1057610X.2013.784568

Oliver, P. E., & Marwell, G. (1992). Mobilizing technologies for collective action. *Frontiers in Social Movement Theory*, 251–272.

Orben, A., Meier, A., Dalgleish, T., & Blakemore, S.-J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology, 3*(6), 407–423. https://doi.org/10.1038/s44159-024-00307-y

Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence, 28*(1), 1–29. https://doi.org/10.1080/09546553.2013.876414

Powis, B., Randhawa-Horne, K., Elliott, I., & Woodhams, J. (2019). Inter-rater reliability of the extremism risk guidelines 22+ (ERG 22+). Available at: https://www.gov.uk/government/publications/inter-rater-reliability-of-the-extremism-risk-guidelines-22-erg-22.

Reeve, Z. (2021). Engaging with online extremist material: Experimental evidence. *Terrorism and Political Violence, 33*(8), 1595–1620. https://doi.org/10.1080/09546553.2019.1634559

Sarma, K. M., Carthy, S. L., & Cox, K. M. (2022). Mental disorder, psychological problems and terrorist behaviour: A systematic review and meta-analysis. *Campbell Systematic Reviews, 18*(3), Article e1268.

Schumann, S., & Klein, O. (2015). Substitute or stepping stone? Assessing the impact of low-threshold online collective actions on offline participation. *European Journal of Social Psychology, 45*(3), 308–322. https://doi.org/10.1002/ejsp.2084

Schuurman, B. (2020). Research on terrorism, 2007–2016: A review of data, methods, and authorship. *Terrorism and Political Violence, 32*(5), 1011–1026. https://doi.org/10.1080/09546553.2018.1439023

Schuurman, B., Bakker, E., Gill, P., & Bouhana, N. (2018). Lone actor terrorist attack planning and preparation: A data-driven analysis. *Journal of Forensic Sciences, 63*(4), 1191–1200. https://doi.org/10.1111/1556-4029.13676

Scrivens, R., Osuna, A. I., Chermak, S. M., Whitney, M. A., & Frank, R. (2023). Examining online indicators of extremism in violent right-wing extremist forums. *Studies in Conflict & Terrorism, 46*(11), 2149–2173. https://doi.org/10.1080/1057610X.2021.1913818

Scrivens, R., Wojciechowski, T. W., Freilich, J. D., Chermak, S. M., & Frank, R. (2022). Differentiating online posting behaviors of violent and nonviolent right-wing extremists. *Criminal Justice Policy Review, 33*(9), 943–965. https://doi.org/10.1177/08874034221095398

Silke, A. (2024). Factors in terrorist risk assessment: A rapid evidence assessment of the extremism risk guidance (ERG22+) factors. *Journal of Criminal Psychology*. https://doi.org/10.1108/JCP-04-2024-0035. *ahead-of-print*(ahead-of-print).

Slater, M. D. (2015). Reinforcing spirals model: Conceptualizing the relationship between media content exposure and the development and maintenance of attitudes. *Media Psychology, 18*(3), 370–395.

Smith, L. G. E., Wakeford, L., Cribbin, T. F., Barnett, J., & Hou, W. K. (2020). Detecting psychological change through mobilizing interactions and changes in extremist linguistic style. *Computers in Human Behavior, 108*, Article 106298. https://doi.org/10.1016/j.chb.2020.106298

Torregrosa, J., Thorburn, J., Lara-Cabrera, R., Camacho, D., & Trujillo, H. M. (2020). Linguistic analysis of pro-ISIS users on Twitter. *Behavioral Sciences of Terrorism and Political Aggression, 12*(3), 171–185. https://doi.org/10.1080/19434472.2019.1651751

Valentini, D., Lorusso, A. M., & Stephan, A. (2020). Onlife extremism: Dynamic integration of digital and physical spaces in radicalization. *Frontiers in Psychology, 11*. https://doi.org/10.3389/fpsyg.2020.00524

Valkenburg, P. M., Meier, A., & Beyens, I. (2022). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. *Current Opinion in Psychology, 44*, 58–68. https://doi.org/10.1016/j.copsyc.2021.08.017

Verduyn, P., Gugushvili, N., & Kross, E. (2021). The impact of social network sites on mental health: distinguishing active from passive use. *World Psychiatry, 20*(1), 133–134.

Verduyn, P., Ybarra, O., Résibois, M., Jonides, J., & Kross, E. (2017). Do social network sites enhance or undermine subjective well-being? A critical review. *Social Issues and Policy Review, 11*(1), 274–302. https://doi.org/10.1111/sipr.12033

von Behr, Ines, Reding, Anais, Edwards, Charles, & Gribbon, Luke (2013). *Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Santa Monica, CA: RAND. Retrieved from http://rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf.

Whittaker, J. (2021). The online behaviors of Islamic state terrorists in the United States. *Criminology & Public Policy, 20*(1), 177–203. https://doi.org/10.1111/1745-9133.12537

Whittaker, J. (2022). Rethinking online radicalization. *Perspectives on Terrorism, 16*(4), 27–40.

Wilkins, D. J., Livingstone, A. G., & Levine, M. (2019). All click, no action? Online action, efficacy perceptions, and prior experience combine to affect future collective action. *Computers in Human Behavior, 91*, 97–105. https://doi.org/10.1016/j.chb.2018.09.007

Wojcieszak, M. (2009). "Carrying online participation offline"—mobilization by radical online groups and politically dissimilar offline ties. *Journal of Communication, 59*(3), 564–586. https://doi.org/10.1111/j.1460-2466.2009.01436.x

Wolfowicz, M., Hasisi, B., & Weisburd, D. (2022). What are the effects of different elements of media on radicalization outcomes? A systematic review. *Campbell Systematic Reviews, 18*(2), Article e1244. https://doi.org/10.1002/cl2.1244

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews, 17*(3), Article e1174. https://doi.org/10.1002/cl2.1174

Yuan, E. (2011). News consumption across multiple media platforms: A repertoire approach. *Information, Communication & Society, 14*(7), 998–1016. https://doi.org/10.1080/1369118X.2010.549235