EXECUTIVE SUMMARY

Online Radicalisation: A Rapid Review of the Literature

Rosamund Mutton, James Lewis & Sarah Marsden

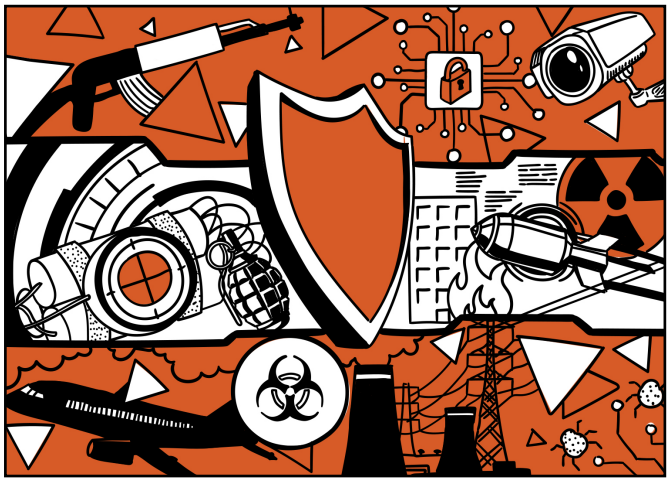
OVERVIEW

This guide sets out the evidence base for 'online radicalisation', examining how individual use of the Internet, in conjunction with offline influences, can facilitate radicalisation processes. The UK is the main context of concern, however comparable evidence is found in studies with samples from the USA, Canada, Belgium, Germany, Austria, and Israel.

Radicalisation remains a contentious concept and few studies explicitly define 'online radicalisation'. For the purposes of this guide, 'radicalisation' is understood as leading to cognitive outcomes reflected in changes in beliefs and ideas, and/or behavioural outcomes which manifest in changes in behaviour.

METHODOLOGY

Two systematic literature reviews (Hassan et al., 2018; Carthy et al., 2020) directed initial searches for relevant research. Further literature was identified through forward and backward citation searching, and narrower key word searches conducted in Google Scholar. Literature searches were completed between June and August 2022. The guide primarily examines literature published between January 2017 and July 2022. Although the evidence base remains modest in size, the research underpinning this guide is assessed to be good quality. There is a growing body of evidence that uses qualitative and quantitative methods to examine a range of factors which are relevant to online radicalisation.



KEY FINDINGS

- Online and offline activities and domains interact, challenging the 'online/offline dichotomy' popular in early research into online radicalisation. Radicalisation processes rarely take place in either the online domain or the offline sphere exclusively, but instead are characterised by complex and dynamic interactions between the two.

- Research that sought to distinguish between online and offline processes may have over-estimated the extent to which the Internet contributes to radicalisation processes. This tendency to focus on the role of the Internet may have come at the expense of recognising the role of offline factors and the importance of the interaction between online and offline contexts.

- The Internet in isolation does not cause radicalisation and is better understood as playing a role in facilitating this process. While the Internet can

contribute to an individual's radicalisation, it cannot drive the process on its own.

BEHAVIOURAL RADICALISATION

- Use of the Internet can enable behavioural outcomes including event planning and preparatory activities, communication and networking behaviours (including arranging offline activities) and ideology-seeking actions.
- Pathways into violent extremism have been characterised as primarily offline, mainly online, and hybrid. Hybrid pathways seem to be the most common.
- There is no single profile of, or standard trajectory taken by, individuals whose use of the Internet influenced their radicalisation. However different pathways seem to be associated with differing levels of intent, capability, and engagement. Hybrid pathways demonstrate greatest engagement and intent; offline pathways, greatest capability; and online, the lowest levels of engagement, intent and capability.

COGNITIVE RADICALISATION

- Empirical research analysing the influence of online interactions and exposure to extremist content on violent extremist behaviour remains limited.
- Video-sharing platforms and social networking sites are spaces where individuals are most likely to encounter extremist content online.
- The individual is an active rather than passive actor in the radicalisation process. It is the individual's behaviour and how they utilise the Internet that informs its relevance to radicalisation.
- There is little robust evidence about whether and how recruiters try to identify or engage with those seeking out online extremist material.
- Individuals who actively seek out violent extremist material online seem to be at greater risk of radicalising and engaging in violence, compared to passive consumers.
- Research on the role exposure to violent extremist content online plays in cognitive radicalisation has suggested that initial exposure to extremist content online has the potential to trigger an interest in extreme ideologies, and that exposure to content from a combination of online and offline spheres may be more influential than exposure via one or the other.
- The amount of time spent online and willingness to express political views on the Internet seem to be associated with greater exposure to extremist material.
- A study that looked at personality traits, specifically the role of empathy, hostility, and aggression, found that aggression may be more influential than exposure to extremist propaganda in influencing extremist cognitions. However, research on the dynamics of these processes remains limited.

ONLINE INDICATORS OF BEHAVIOURAL RADICALISATION

- Robust empirical evidence on how online activities might be used to identify individuals at risk of behavioural radicalisation is comparatively weak.
- There is some evidence that exposure to extremist content online has a stronger link to radicalisation in comparison with other kinds of media-related risk factors, such as different platforms, mediums (e.g., Internet, newspaper etc.), content, activities, and attitudes.
- Recruiters may use different kinds of online extremist material to first nurture cognitive radicalisation and then try and move people towards violence.
- Some research suggests that posting patterns on social media may be able to differentiate between violent and non-violent extremists, and between behavioural and cognitive outcomes, but further research is needed to fully understand these processes.
- Future research is likely to benefit from combining computational and social science methods, and developing robust, publicly available standardised datasets which are free from bias.

INTERVENTION STRATEGIES

- The effectiveness of counter-narratives varies according to the intervention technique used and the type of outcome targeted.

- There is insufficient evidence to determine whether counter-narratives can prevent violence, however they may be able to address some of the risk factors associated with radicalisation.

- Inoculation theory may provide a foundation for developing deterrence strategies. This approach introduces individuals to weakened versions of an argument whilst providing evidence to refute it. Preliminary experiments indicate that 'active' inoculation methods (where the individual actively engages in a task such as a computer game) can improve critical thinking skills and reduce vulnerability to radicalisation. This research is at an early stage that will benefit from more attention before the potential risks, implications and scalability of this approach is understood.

- Although the evidence base is very limited, interventions may benefit from adopting a fine-grained approach that is tailored to specific audiences and online contexts, including audience segmentation and micro-targeting.

- Interventions have the potential to produce unintended outcomes, including further entrenching extremist views, for example where activists initiate arguments in response to extremist positions.

- There is some, limited evidence to suggest that highlighting the personal impact of involvement in extremism may be more effective than challenging extremist ideas or arguments, and that online interventions may be less effective with those with more entrenched views.

- Intervention providers working online will benefit from training and support to mitigate the risks associated with this work, and to ensure their approach is evidence-informed.

CHALLENGES TO UNDERSTANDING ONLINE RADICALISATION

- Accessing and gathering valid empirical data is one of the main barriers to producing robust research able to evidence whether, and to what extent, online activity influences violent offline behaviour. Similar difficulties arise in efforts to assess which factors influence attitudinal change.

- It can be difficult to generalise the findings of research drawn from small-n sample sizes collected using qualitative methods, or which focuses on a specific ideology or geographical context. Drawing broader conclusions to groups or settings beyond the data sample should be undertaken with caution.

- Large-n computational methods have the potential to identify broader trends in the data but can risk over-simplifying radicalisation processes.

- Efforts to understand the impact of online interventions face similar challenges to evaluations of offline P/CVE programmes. These include the difficulty understanding an intervention's impact; accessing appropriate data; ethical and security risks; and the difficulty identifying and evidencing the causal factors that shape outcomes.

- Methodological differences in how data are collected, used and analysed can be difficult to translate across disciplines.

- Ambiguous and/ or contested definitions of 'online radicalisation' can make it challenging to draw comparisons across studies which may be focused on different phenomena.

RECOMMENDATIONS FOR POLICY AND PRACTICE

- P/CVE interventions are likely to benefit from taking account of the hybrid nature of radicalisation processes and developing ways of targeting online and offline domains simultaneously, rather than separately. For example, by working in offline contexts to help develop digital literacy skills if the online space seems to be an important source of information for those engaged in primary or secondary interventions.

- Intervention strategies which provide an alternative source of meaning and association to replace the relational networks offered by extremist groups, both online and offline, appear promising.

- There is some evidence to suggest it may be beneficial to prioritise interventions which focus on those who actively seek extremist content online, as they may be at greater risk of radicalisation to violence.

- The gamification (or use of mechanisms used in games) of interventions has the potential to appeal to those who actively seek extremist content. These types of intervention can encourage the development of critical thinking skills and may provide an element of interaction that active seekers are looking for.

- Interventions targeting video-sharing platforms and social networking sites may have a greater impact than targeting other areas online. However, there are risks to this approach. Counter-messaging videos and extremist content can share key words. This means that the algorithms which drive automated recommendation systems may direct users to extremist content, rather than to counter-messaging videos.

- Counter-narratives will benefit from careful targeting, taking account of the specific audience; the extent to which they may already be persuaded by extremist ideas; the risk factors the intervention is seeking to influence and the mechanisms by which positive outcomes might be enabled.

- Evidence regarding the impact of removing extremist content is limited. Taking down material may help to reduce its accessibility. However, there is some limited evidence that where material is removed from non-encrypted, more accessible online spaces, this has the potential to encourage users to move to encrypted platforms which are more difficult to monitor and moderate.

- Interventions should take account of unintended outcomes, including the potential to further entrench extremist views; generate risks to freedom of speech; and create incentives for tech companies to 'over-censor' content to avoid sanction.

- Intervention providers working online should receive appropriate training, professional development opportunities, and support.

DIRECTIONS FOR FUTURE RESEARCH

KEY AREAS OF FUTURE RESEARCH INCLUDE:

- Further work to understand the role of the Internet in pathways into extremism, including research able to interpret how online and offline dynamics interact.

- Research that draws on first-hand accounts of how the Internet shaped an individual's thinking and behaviour has the potential to elucidate the experiential aspects of radicalisation processes.

- Studies examining the impact of the COVID-19 pandemic on online radicalisation could try to assess the impact of lockdowns and whether associated feelings of isolation and the increased use of technology as a substitute for physical, face-to-face interactions led to greater exposure to, or engagement with, extremist content.

- Research which bridges computational approaches which analyse large amounts of data with social science-based methods able to interpret the experiential and subjective experiences of online users may provide greater insights and overcome the disjuncture between disciplines.

- Studies focused on a specific ideology could be carried out with data on a different ideology. This would help to determine whether findings can be generalised or are ideologically specific, and whether targeted interventions would benefit from being tailored to specific ideologies.

- Further research into the role of individual personality traits, pre-existing beliefs and other psychological factors that may shape responses to extremist content and radicalisation. This would help tailor and target interventions in ways which are appropriate for particular groups or individuals, and help to avoid unintended or negative outcomes.

- Areas where results are limited, mixed or inconclusive would benefit from further research. These include:

    a. The relationship between exposure to extremist content online and cognitive radicalisation.

    b. Approaches able to interpret whether patterns of online engagement have the potential to identify individuals at risk of cognitive or behavioural radicalisation.

- Further work to understand the impact of interventions is important, assessing:

    a. What effect the removal of online extremist content has, and what risks this strategy carries.

    b. The potential of realist evaluation to develop a better understanding of which counter-narrative interventions work, for whom, under what circumstances, and why.

    c. The unintended consequences of different kinds of intervention strategy, including direct engagement online; efforts to direct people to counter messages; and counter-narrative material.

ABOUT THIS PROJECT

This Executive Summary comes from part of a CREST project to inform the refresh of the CONTEST strategy. The project provides updates to the evidence base behind key CONTEST topics. To read the Full Report this executive summary was produced from, as well as other outputs from this project, visit our website: *crestresearch.ac.uk/project/contest*

CREST is funded by the UK's Home Office and security and intelligence agencies to identify and produce social science that enhances their understanding of security threats and capacity to counter them. Its funding is administered by the Economic and Social Research Council (ESRC Award ES/V002775/1).