RADICALISATION IN THE DIGITAL ERA

The role of the internet in radicalisation and terrorism

Anaïs Reding,
Charlie Edwards,
Luke Gribbon,
RAND Europe,
May 2013

Radicalisation in the Digital Era

Introduction

We live in an era in which 76 percent of European households have access to the internet, 60 percent of which use it daily, including 54 percent of which use it for essential services like banking (European Union, 2012). This widespread connectivity has led to important changes in the way in which society is organized. Violent extremists and terrorists form part of this society, and it is widely assumed that the changes in connectivity have also affected their radicalisation process (von Behr et al., 2013); or in other words, 'the process by which a person comes to support terrorism and forms of extremism leading to terrorism' (Home Office, 2011).

There is, however, very limited evidence available to explore whether the internet has actually affected the radicalisation process, and if so, in what way. A significant part of the literature that looks at the role of the internet in radicalisation focuses on identifying the material available on the internet to violent extremists and terrorists, from there drawing assumptions about the way in which this material affects the radicalisation process (von Behr et al., 2013). The literature that does critically question the way in which the internet affects radicalisation, on the other hand, mainly draws on second-hand evidence such as media reports (von Behr et al., 2013).

This paper summarises work carried out by RAND Europe, drawing on evidence gathered directly from 15 extremist and terrorist cases to clarify the role the internet plays in radicalisation. We sought to examine with first-hand evidence five of the main questions posed in the literature:

- Does the internet enhance opportunities to become radicalised?
- Does the internet act as an 'echo chamber' for individual beliefs?
- Does the internet accelerate the process of radicalisation?
- Does the internet allow radicalisation to occur without physical contact?
- Does the internet increase opportunities for self-radicalisation?

This study contributes to the body of evidence on terrorism by providing insights into the above questions from primary research and drawing from several types of data associated with terrorist and extremist cases given its grounding in first-hand evidence (cf. the SAFIRE paper on the limitations to the literature, which explains that the literature on terrorism continues to be undermined by a lack of first hand evidence).

Challenges

Findings from this work are based on a small number of cases and we cannot claim that they are representative of the wider terrorist population: they do not necessarily reflect the way in which all violent extremists and terrorists use the internet during their radicalisation.

In addition, the report does not make claims about causality: the study did not generate sufficient evidence to test whether the pattern of internet usage had caused the phenomena that we were researching, or whether the internet use was merely associated with it.

For these reasons, the results should be considered as providing insight into the way in which the internet appears to interact with the process of violent radicalisation in these cases on the basis of first-hand evidence.

.

Method

RAND Europe followed a two-step approach to explore whether the main questions posed in the literature were supported by first-hand evidence.

First, the research team carried out a literature review to identify the key questions posed in the literature and to document the current understanding of the role played by the internet in radicalisation, as reported in the literature. Initial literature was identified through a systematic search using a combination of search terms, including: a) radicalisation, extremism and terrorism, b) internet and online and c) role, effect, and influence. The research team identified further literature by snowballing from the initial literature.

The research team then gathered first-hand (or primary) evidence to explore the questions identified in the literature. The team gathered evidence relating to five cases of extremists and ten cases of convicted terrorists in the UK, all of which were anonymised: The research team carried out interviews with terrorists convicted in the UK and a handful of individuals who

were part of the Channel programme, a UK government intervention aimed at individuals identified by the police as vulnerable to violent extremism;
The team conducted interviews with the police officers responsible for convicted terrorists and Channel participants; and The team investigated the individuals' use of the internet rom data recovered by the police directly from their computers.

The research team's access to this primary data was authorized by the Home Office and relevant constabularies.

In a third of cases, the research team triangulated the information that it collected by pursuing all three research steps. The objective of this process was to gather as much information as possible about each case, and to check that the information collected was consistent across sources. Often, interviews with the police officers served to clarify seemingly contradictory information gathered from the literature and through interviews with the convicted terrorists. In two thirds of the cases, however, the research team was only able to interview police officers and/or examine the convicted individuals' computer information, and was not able to gain access to convicted terrorists or extremists who are part of the Channel programme. This was mainly due to the time and resource constraints of the study.

RESULTS AND CONCLUSIONS

The evidence that we gathered suggested that the internet played a central role in the radicalisation process. The evidence enabled the research team to delve into this further, and to explore whether the five main questions that emerged from the literature in relation to the supposed role of the internet in radicalisation held true in their cases.

The evidence gathered by RAND Europe was consistent with the consensus emerging from the literature in relation to a couple of research questions.

First, the primary evidence obtained in this research supports the suggestion that the internet may enhance opportunities to become radicalised, as a result of being available to a large number of individuals, irrespective of gender or ethnicity, and enabling them to connect with like-minded individuals from across the world at any time. For all 15 individuals included in the study, the internet had been a key source of information, of communication and of propaganda for their extremist beliefs. This was not only evident in their access of, and engagement with, extremist forums, but also in their use of the Google search engine and BBC News coverage of operations in Afghanistan, amongst other accessed sites. One convicted terrorist explained: 'the internet is just another platform. One which allows those that would otherwise be scared of being seen with the wrong people to get engaged, and one which makes the whole process more invisible to the authorities'.

Second, our research supports the suggestion that the internet may act as an 'echo chamber' for extremist beliefs; in other words that the internet provides an opportunity to consult only information that confirms existing beliefs. Figure 1 shows the most frequently used search terms by one convicted terrorist in the study, as evidenced by the information on his computer registry. The search terms show that he was mainly using his profile on that computer to look for jihad-related material.

Other information recovered by the police and shared with RAND Europe similarly suggests that the convicted terrorists included in this study were not looking at information that may have challenged their extremist beliefs. The finding that terrorists' internet use had a narrow focus may however be due to the fact that the information recovered from their computers related to a late stage of their radicalisation. This finding may also be associated with the fact that they accessed information from various profiles or computers. Figure 2 shows the diversity of locations from which extremists and terrorists who formed the sample for this study accessed the internet. The police made clear that it is challenging to attribute information recovered from computers to individuals and to be confident that this information is representative of the individual's usage of the internet. Tech-savvy individuals can use separate computers from different locations, they can hold multiple user names, break into others' profiles, or erase information from the computers they use.

While our research supported the suggestion that the internet has expanded opportunities for radicalisation and that it provides a means through which it is possible to exclusively consult material that is consistent with one's beliefs, our findings challenged other suggestions emerging from the literature.

First, the evidence does not support the suggestion that the internet accelerates radicalisation because of its capacity to connect individuals from across the world at any time. Instead, the internet appears to facilitate radicalisation, which, in turn, may or may not accelerate it. For example, one interviewee explained that: 'before [the internet], I used VHS tapes and passed them round the group, which took time. The internet let me send [potential recruits] videos every day.' The same interviewee explained that before the internet, his group recruited new members by taking them for dinner, a time-consuming and costly activity. The internet removed this cost, thereby making it possible for recruiters to reach out to a wider group of individuals in a shorter space of time. While this example suggests that the speed of communication has increased with the internet, it does not provide insight into whether this

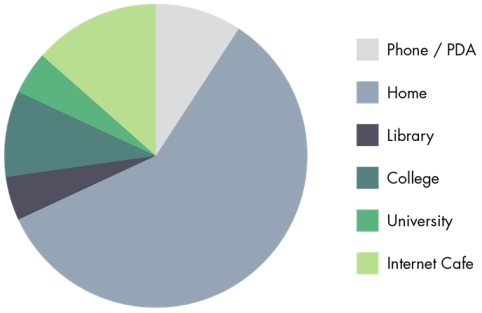
has in turn accelerated the radicalization of those individuals who are being recruited. To assess whether the internet has accelerated radicalisation, researchers would require evidence about the timeframe for individuals who radicalise while using the internet and to compare it with the timeframe for individuals who radicalise without using the internet.

Second, the evidence does not support the claim that the internet is replacing the need for individuals to meet in person during their radicalisation. Instead, the evidence suggests that the internet does not substitute, but rather complements in-person communication. In more than three quarters of the cases that RAND Europe researched, the individual had offline contact with family members or friends who shared their beliefs. Many of these individuals were already on the radar of the authorities, and many had travelled abroad to countries known to host training camps, such as Pakistan.

Figure 1 Word cloud depicting search terms recovered by the police from the computer registry of one terrorist case that RAND Europe examined

Legend: The relative size of the words indicates the frequency with which the term was used.
Source: von Behr et al. (2013)

Figure 2 Locations from which the 15 cases accessed material recovered by the police



Source: von Behr et al. (2013)

Third, the evidence does not support the suggestion that the internet has contributed to the development of a new phenomenon of self-radicalisation where individuals radicalise without ever interacting with others. Roshana Choudhry is the case that is most often cited to exemplify this concept of self-radicalisation. While there is no evidence to suggest that Roshana engaged with others during her radicalisation, interviewees directly involved in her case believe that there may be more to her story than is currently known. In addition, all of the cases that we reviewed during our research involved contact with other individuals, whether virtually or physically. This included cases that had been portrayed in the media as having self-radicalised.

Overall, the study demonstrates the importance of primary research with the population that is the subject of study. The detailed information to which the research team gained access suggested a contrasting picture to some of the claims put forward in the literature. This is particularly true with respect to the phenomenon of self-radicalisation, for which there does not appear to be more than anecdotal evidence.

The study also makes clear that the internet is a challenge for law enforcement: it facilitates and enhances the opportunities to become radicalised and to spread violent extremist beliefs. It also provides a mechanism through which to move towards violent extremist or terrorist acts in ways that are relatively easy to anonymise and difficult to detect.

Given this finding, European governments may wish to make the use of the internet in relation to radicalisation a focus for strategies, policies, and resource allocation. Currently, the internet is considered a key means through which to carry out counter-terrorism, but it is not always viewed as central to the radicalisation process (see for example the revised UK prevention strategy: Home Office, 2011).

REFERENCES

- Von Behr, I, A. Reding, C. Edwards, and L. Gribbon (2013) 'Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism', Cambridge, UK: RAND Europe.
- Home Office (2011) 'Prevent Strategy', available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf [accessed May 30 2013].