No. 314 / September 2018

Facts & Findings

Counter-terrorism and Internal Security

Online-Radicalisation: Myth or Reality?

Linda Schlegel

- The Internet is often an important factor, but not the only element which contributes to radicalisation.
- Online radicalisation is both part of the strategy employed by potentially violent extremists and also a by-product of the proliferation of social media among the adherents of these groups. Not always is official propaganda the main driver, but rather, discussions started among users often become accelerators of the processes of radicalisation.
- The new focus on the radicalisation of children on the Internet is a cause for concern and demands a comprehensive approach to combatting it.
- Both the supply and the demand for online propaganda must be curbed. This can only succeed if we view the phenomenon not solely through a security lens.

Table of contents

The proliferation of extremist, jihadist and violence-inciting websites, blogs and channels in social media has long since become a major theme in security policy. Extremists and terrorists use the new technological tools to communicate with each other, to organise themselves and to publicise their ideas. Whereas terrorists in the previous millennium were still dependent on journalists to report their acts and to draw attention to their group and their ideology, potentially violent groups today are in a position to publish their story and their intentions unfiltered on the web, and to communicate with each other swiftly and effectively across national borders. Ever since the case of Australian teenager Jake Bilardi[1], who travelled to the territories of the so-called Islamic State (IS) and in 2015, at the age of 19, committed a suicide attack in Ramadi (Iraq), however, it is not just online communication by extremists that is in focus, but also the phenomenon of online radicalisation. According to the current state of information, Bilardi converted to Islam without any direct influences from his immediate environment, radicalised himself exclusively via online media, and travelled to Syria with the help of online contacts. His case, and many other cases of Western recruits, raised the question of whether a process of radicalisation can take place exclusively online or if online propaganda is only one facilitating factor that promotes and perhaps accelerates radicalization, but is in itself not sufficient to explain the whole process. Unfortunately, there are still not enough systematic, empirical studies on this subject area and our knowledge is generally limited to known perpetrator profiles. Nevertheless, some general statements can be made regarding online radicalisation.

Are there cases of radicalisation that occur only online?

To be clear: cases of radicalisation which can be proven to have been induced exclusively by the consumption of online propaganda are few and far between. Jake Bilardi is an exception, when one considers the majority of known cases. Nevertheless, this does not prove that there are no cases of pure online radicalisation. Only very few of those who become radicalised go on to plan and commit an attack. Thus, our data is based on the exceptional exceptions, namely those whose radicalisation leads to violence and is discovered by the authorities. It is therefore completely conceivable that online radicalisation is much more effective than has been assumed to date. The step from cognitive radicalisation, that is, from an altered view of the world without apparent use of violence, to violence and the intent to commit an attack can but need not take place. How many cognitively radicalised adherents of "virtual jihad"[2] there are in the "virtual caliphate"[3] cannot be determined with certainty.

Our knowledge about online-radicalization is largely based on the profiles of arrested perpetrators and therefore possibly skewed.

But even if we assume that there are no examples of pure online radicalisation, the Internet and social media still play an increasingly important role. They and can both open doors into an ideology and intensify physical radicalisation contacts. For one thing, this is because technological progress is increasingly shaping the world that we all live in. We all constantly use smart phones, computers and social media. It is therefore not surprising that the spaces of radicalisation have moved from the back rooms of bookstores, onward to secretly exchanged DVDs and then to websites and messaging services such as Twitter and WhatsApp. A digitalised world produces digitalised terrorists. For another, the few empirical studies that exist on the topic show that the Internet offers more opportunities to come into contact with extremist content and, decisively, to communicate with others about this content[4]. Radicalisation is a social process and the Internet favours communication and interaction beyond physical boundaries.

Digital natives use online-communication differently than previous generations.

Two factors which facilitate online radicalisation should be highlighted in particular. Firstly, it must be noted that the younger generation, the so-called *digital natives*[5], accept online media much more naturally as a part of their lives and their social relationships than older generations do. This means that the importance of face-to-face communication is declining and online contacts are encountered with great trust. This is especially the case if the online contacts mirror the particular linguistic features of the *digital natives* and attract them with content specific to the target group. Under certain circumstances, online communication can completely replace offline communication and thus facilitate online radicalisation; especially when a direct personal contact is established via a message service.

Social media creates an echo chamber, which is hardly penetrated by outside content.

Secondly, the so-called *filter bubble* or echo chamber[6] should be mentioned. Social media accounts show their users only things which their friends share, content of pages that they have “liked” or have subscribed to and offer the possibility of blocking many items which the users do not like. This creates an echo chamber, in which political views and ideologies are reflected from all sides like the echo in a cave. It gives the impression that everyone has the same opinion. Filter bubbles affect all users, but they can promote radicalisation, if the filter bubble contains extremist attitudes and certain perspectives are repeatedly communicated as the truth and the point of view of the community. Digital natives in particular, can take on radical points of view as a result of the suggested consensus of their network, because in their experience social contacts often occur mainly online. Next, the question arises as to what extent these developments have been anticipated and driven by extremists.

Top-down or Bottom-up?

In discussions about online radicalisation, the question repeatedly arises as to whether it is part of a deliberate strategy controlled by the leaders of terrorist organisations or whether social media is used more intensely for the exchange of ideas in general and jihadist ideas are discussed there more or less by coincidence. The question of whether radicalisation occurs *top-down* or *bottom-up* was a controversy discussed by academics and experts in the field even before the focus turned to online media. The *Hoffman-Sageman debate* in the US is symptomatic of this. Hoffman[7] believes that organisations can gain new adherents by using targeted propaganda and specially trained recruiters. In contrast, Sageman[8] assumes that radicalisation can be a by-product of other group dynamics and that it takes place especially where small groups of friends mutually ideologise each other.

Online-radicalization works top-down as well as bottom-up.

In the realm of online propaganda we find a hybrid between the two opposing positions[9]. On the one hand, there are official websites and social media channels. One study found that it is very likely IS used so-called bots on Telegram in order to post content simultaneously on thousands of channels. Additionally, the channels are moderated or monitored to some extent and inactive or “suspicious” users are excluded, which leads to the conclusion that official agencies of the organisation are at work here.[10] IS also produces professional videos and magazines in various languages, in order to address a broad target group. It is thus very likely that “professional’ recruiters also exist within the group, whose task is to actively promote radicalisation and to develop personal contacts with users. But even on official propaganda channels, the organisations attach importance to the possibility of direct exchanges. *Dabiq*, the English-language online magazine of the so-called Islamic State, contains email addresses and the claim that “The Dabiq team would like to hear back from its readers“[11]. Even official online propaganda is thus not just top-down, but rather opens doors to direct, personal communication. This must be understood as a deliberate strategy. Social media makes it very easy communicate with other users anonymously and in a fast manner, so that it is less dangerous and less difficult than it used to be to establish direct contact with extremists.

However, “normal users” also facilitate the role of social media in processes of radicalisation. Official propaganda is shared and commented upon. Often new propaganda is produced or disseminated among non-propaganda content via the comment function. The ability to actively shape ideology on the web should certainly be evaluated as a most alarming possibility. The Internet enables all sympathisers to take part in the ideological direction of the organisation and the categorisation of external events to an unprecedented degree. A person who can actively help to shape content has a greater psychological investment in the ideology than a passive consumer does. Radicalisation can be the result of and is intensified by the social processes and opportunities for exchanges on the web. Sageman’s group of friends can also exist virtually.

New Challenges

Instant messenger services such as WhatsApp present a special mixture of face-to-face and online-radicalization.

A new challenge for security agencies and civil society organizations involved in prevention and de-radicalisation is the spread of *instant messenger* services such as Twitter, Telegram und WhatsApp[12]. Here it becomes especially clear how social media can blur the boundaries between the pure consumption of online propaganda and active recruitment. For example, the Würzburg assassin had contact with IS members via WhatsApp just before the attack and received fairly detailed instructions.[13] Services such as WhatsApp facilitate direct communication over great distances with no time delays and thus encourage attack tactics using so-called “*remote-controlled*” perpetrators.[14] On the one hand, they are individual perpetrators and fall into the category of *lone wolves*, because they do not benefit from any practical help for their attacks and they often do not belong to any terrorist organisation. On the other hand, they receive instructions from the outside and are thus no longer to be categorised as individual perpetrators. In this context, Weimann speaks of “lone wolves and their virtual packs”[15], an unprecedented type of perpetrator. With this new phenomenon, terrorism research not only reaches its limits with regard to the verbal differentiation of perpetrator profiles, but also does not yet have any effective countermeasure to combat such direct but virtual radicalisation and recruitment efforts.

Sometimes jihad is presented as a youth subculture and thereby appeals to a broader audience.

A second challenge is the increasingly intensifying *gamification* of propaganda material.[16] *Gamification* describes the introduction of traditional gaming elements such as competition, status, level and prizes in a non-gaming context. On the one hand, mention should be made of incentives that keep the users longer on extremist websites, such as prizes for certain amounts of comments and privileges via rising to a new “level”. On the other hand, there are now also classic games which have been developed for propaganda purposes, such as an Islamist variant of the well-known game *Grand Theft Auto*.[17] This is part of the strategy of Islamist protagonists which is described as the so-called Pop-Jihad[18] also known as *Jihadi Cool*[19], which presents itself as a youth subculture and uses elements of pop culture such as games, rap and films for its purposes. In many cases, jihadist websites are designed in a much more professional, interesting and well-constructed manner than those of other organisations and are thus experienced as appealing and cool.[20] Gamification increases the psychological appeal of extremist ideas and can offer an easy and insidious introduction to the scene. Here as well, there is no effective countermeasure as yet, beyond the deletion of video material, discussion forums and games.

The radicalization of children and teenagers needs increasing attention.

This also means a greater risk to children and adolescents. It is not only that they are generally more likely to be users of online games, but also that Islamist organisations employ a special strategy so as to introduce even the smallest children to the ideology. The content used is adapted to various age and target groups and reflects the everyday reality of life for the children. For example, the IS App, *Moalem Al-Hijaá* (Spelling Teacher), is designed like a classic word-finding game, but instead of the usual words like car and ball, the correct spelling of military weapons is shown.[21] Older children and adolescents on the other hand, are appealed to with their own IS stickers and *GIFs* (Graphics Interchange Format, short video sequences). This is a new and dangerous development, because social media can expose children to propaganda content in a familiar and seemingly safe environment. In this case, collaboration is essential between youth protection services, political decision-makers and social media companies.

Outlook and Recommendations

Even if we currently still lack extensive empirical evidence and exact figures regarding online radicalisation, the importance online media in many newer perpetrator profiles is indisputable, whether as *Foreign Fighters* or as *Homegrown Terrorists*. The fact that terrorist associations like IS invest so much time and money in complex online propaganda means that it must have a major strategic benefit for the organisations and that they can use it to achieve their objectives. That in itself should be reason enough to study this material more closely, and to look for preventive measures to counter online radicalisation.

Physical counter-measures and censorship are not enough to solve the problem.

Since its physical weakening and its loss of territory, IS has greatly reduced its production of propaganda. However, this applies only to the official channels; the ideology and readiness to use violence lives on in its sympathisers. Even if IS itself might not recover, other organisations will take its place, calling online for violence and terrorism and contributing to the radicalisation of young people. Physical attacks against militias can decimate the official channels for a while, but will not permanently solve the problem. A complete censorship would be difficult as well. The Internet is fast-moving, screenshots are created within seconds and users repeatedly find new ways to access propaganda content. A problem that is fomented both *top-down* and *bottom-up* cannot be combatted only *top-down*. Where appropriate, this means a reallocation of resources, because “official” terrorist organisations are addressed differently than individual users.

Interdisciplinary research into radicalization is needed and must be applied on multiple levels.

Online propaganda will not disappear completely nor will online radicalisation be prevented completely. Both of these will continue to concern us for years to come. It is therefore of utmost importance to do more research into this phenomenon and to find an interdisciplinary approach to explain it; especially at the interface of sociology, psychology and communication sciences. Only then can a workable solution be found. At present, we still understand too little about how radicalisation mechanisms operate in the virtual world and we are fighting symptoms instead of causes. Furthermore, it is important to offer the groups at risk alternative narratives especially and as well, rather than just so-called *counter-narratives*. The essential is not just a response, but the offering of positive enticements both online and offline. An interdisciplinary approach is needed to create this narrative, and thus exchanges between scientists from different disciplines, practising experts in the field of prevention and de-radicalisation, security agencies and politics should be encouraged must more intensely than heretofore.

Particular attention should be paid to the alarming development with regard to the radicalisation of children. It is necessary to find an approach that draws upon concepts of social protection for the young and is not solely based on security considerations. The appeal of Jihadi Cool to children and young people can be immense and must be countered as early as possible. Whereas the CONTEST strategy against terrorism in Great Britain gives schools and universities special significance in the identification of possible cases of radicalisation, there are few comparable approaches in Germany. In this regard, it would make sense to evaluate the strategies of other European countries so as, if possible, to design a German strategy to counter the radicalisation of children and young people.

As Professor Peter Neumann advised the American government back in 2012[22]: to decrease cases of online radicalisation, both the supply of and the demand for such content must be reduced. There must be discussion of how to make extremist content less accessible, of the role played by organisations like facebook, and of legal measures to regulate the Internet. However, we must also question why more and more young people deliberately search for such content and how we can prevent helpful means of communication such as WhatsApp from being turned into recruiting tools. This means that a holistic perspective which goes beyond the security aspect would be advisable in order to develop effective approaches to solutions together with stakeholders of civil society.

[1] A BBC journalist spoke with Bilardi before his attack: https://www.bbc.com/news/world-australia-31845428 (05.08.18). In addition, parts of his blog, in which he himself describes his radicalisation, are available again: https://quadrant.org.au/opinion/qed/2015/06/jake-bilardis-deleted-blog/ (05.08.18).

[2] Awan, A. (2010). The Virtual Jihad. https://ctc.usma.edu/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare/ (05.08.18).

[3] Winter, C. (2015). Documenting the Virtual Caliphate. http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf (05.08.18).

[4] Cf for example van Behr, I., Reding, A., Edwards, C. und Gribbon, L. (2013).Radicalisation in the Digital Era: The use of the Internet in 15 cases of terrorism and extremism. https://www.rand.org/content/dam/rand/pubs/ research_reports/RR400/RR453/RAND_RR453.pdf (05.08.18).

[5] Prensky, M. (2001). Digital Natives, Digital Immigrants. http://old.ektf.hu/~kbert/2014_15_01/erasmus/DigitalNativesPartIII.pdf (25.07.18).

[6] Winter, C. (2016). Special Report: An integrated approach to Islamic State recruitment. https://www.aspi.org.au/publications/an-integrated-approach-to-islamic-state-recruitment/SR88_IS-recruitment.pdf. (27.07.18).

[7] Hoffman, B. (2006). Inside Terrorism. Columbia University Press.

[8] Sageman, M. (2004). Understanding Terrorist Networks. University of Pennsylvania Press
Sageman, M. (2008). Leaderless Jihad. University of Pennsylvania Press.

[9] Baaken, T. und Schlegel, L. (2017). Fishermen or Swarm Dynamics? Should we Understand Jihadist Online-Radicalization as a Top-Down or Bottom-Up Process? http://journals.sfu.ca/jd/index.php/jd/article/view/127/105 (20.7.18).

[10] Bloom, M. Hicham, T. and Horgan, J. (2017). Navigating ISIS's Preferred Platform: Telegram. Terrorism and Political Violence. DOI: 10.1080/09546553.2017.1339695.

[11] Weimann, G. (2016). "Why do terrorists migrate to social media?", in Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (Herausgeber). Violent Extremism Online: New Perspectives on terrorism and the Internet. Routledge: London, S. 54.

[12] Kiefer, M. (2017). Young Jihadists in WhatsApp-Chat: What role does religion play? http://www.bpb.de/politik/extremismus/radikalisierungspraevention/259448/junge-dschihadisten-im-whatsapp-chat (04.08.18).

[13] Cf. Czygan, Z. (2016) "IS-Anweisungen an Würzburger-Attentäter: 'Mach es mit der Axt'" ["IS instructions to Würzburg perpetrator: 'Do it with the axe'"]. https://www.augsburger-allgemeine.de/bayern/IS-Anweisungen-an-Wuerzburg-Attentaeter-Mach-es-mit-der-Axt-id39088002.html (09.07.18).

[14] Cf. e.g. Mullins, S. (2017). Lone-actor vs. remote-controlled jihadi terrorism: Rethinking the threat to the West. https://warontherocks.com/2017/04/lone-actor-vs-remote-controlled-jihadi-terrorism-rethinking-the-threat-to-the-west/ (25.07.18).

[15] Weimann, G. (2016). "Why do terrorists migrate to social media?", in Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (Herausgeber). Violent Extremism Online: New Perspectives on terrorism and the Internet. Routledge: London.

[16] Brachman, J. und Levine, A. (2011). The World of Holy Warcraft. http://foreignpolicy.com/2011/04/13/the-world-of-holy-warcraft/ (25.07.18).

[17] Al-Rawi, A. (2016). Videogames, terrorism and ISIS jihad 3.0. https://www.tandfonline.com/doi/pdf/10.1080/09546553.2016.1207633 (24.6.18).

[18] Der Tagesspiegel (2015). Werbung mit dem "Pop-Dschihad". [Promotion with the "Pop-Jihad".] https://www.tagesspiegel.de/politik/islamistische-rekrutierung-im-internet-werbung-mit-dem-pop-dschihad/12707602.html (27.07.18).

[19] Cottee, S. (2015). The Challenge of Jihadi Cool. https://www.theatlantic.com/international/archive/2015/12/isis-jihadi-cool/421776/ (25.07.18).

[20] Zick, A. interviewed by von Billerbeck, L. (2015). Wie der IS Jugendliche im Internet ködiert. [How IS lures young people on the Internet.] http://www.deutschlandfunkkultur.de/vorbild-islamismus-wie-der-is-jugendliche-im-internet.1008.de.html?dram:article_ id=309064 (29.06.18).

[21] Jugendschutz.net (2018). 2017 BerichtL Islamiismus im Netz. [Report: Islamism on the web.] https://www.hass-im-netz.info/fileadmin/user_upload/hass_im_netz/documents/Bericht_2017_Islamismus_im_Internet.pdf (24.07.18).

[22] Neumann, P. (2012). Countering Online Radicalization in America. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20_Online%20Radicalization%20Report.pdf (28.07.18).

Imprint

The Author

Linda Schlegel is a consultant in counter-terrorism and conflict management at the Konrad-Adenauer-Stiftung. She has a Master in Counter-Terrorism from King's College London and focuses in particular on the topics of radicalisation and the social effects of terrorism.

Konrad-Adenauer-Stiftung e. V.
Linda Schlegel
Consultant in Counter-terrorism and Conflict Management
European and International Cooperation
T: +49 30 / 26 996-3398
linda.schlegel@kas.de

Postal address: Konrad-Adenauer-Stiftung, 10907 Berlin

Publisher: Konrad-Adenauer-Stiftung e. V. 2018, Sankt Augustin/Berlin
Design & Typesetting: yellow too Pasiek Horntrich GbR
The print edition of this publication was printed carbon neutral
by copy print Kopie & Druck GmbH, Berlin, on FSC certified paper.
Printed in Germany.
Printed with financial support from the German Federal Government.

ISBN 978-3-95721-468-3

Title page illustration note
© Sergey Nivens/Shutterstock.com