UDC:316.77:004.738.5

DOI: https://doi.org/10.22182/pnb.specijal2022.9

Review article

The Policy of National Security Year XIII Special Issue 2022. pp. 101-110

Tomáš Kouba*

Graduate Student of Security Studies, Institute of Political Studies, Faculty of Social Sciences, Charles University Prague

ONLINE RADICALIZATION: TWITTER PRIVATIZATION AS A THREAT TO THE MODERN SOCIETY

Abstract

Social media plays a key role in the contemporary world, having indefinite power to influence people by just a single post and click of a button, reaching millions of people in a few seconds. In April 2022, Elon Musk announced his step into the world-famous'wall of opinions' - Twitter- with words of creating a better, free-speech-based platform with no limitations. Since online radicalization became the easiest and most powerful recruiting tool for terrorist and extremist organizations, this raised concerns about whether this action is beneficial or not. The aim of the paper was to describe the principle of online radicalization and present it via evidence-based examples, as well as transpose the known aspects of Elon Musk's purchase of *Twitter*. A comparison study was made between these known examples of radicalization on the Internet, currently used preventive policy principles and possible future steps based on the announcements of Elon Musk himself. Results confirmed that online radicalization is the most effective method for extremists, and that the society and authorities should keep an eye on the development of the platform regarding the real threat of losing control over the content that can be harmful to *Twitter* users. Free speech is a strong argument for freeing the rules of sharing content, but the 'dark side' of this move has to be considered as well.

Keywords: online radicalization, *Twitter*, extremism, Elon Musk, the Internet, online violence, terrorism, social media

Email address: tomas.kouba@fsv.cuni.cz

INTRODUCTION

The new era of the Internet brought about multiple challenges for ordinary life and online security. In these terms, online radicalization became a new phenomenon in violent groups' recruiting techniques and the 'securitization' practice of the social media audience. Since there isan easy and broad access to different platforms where the action can be taken immediately, this approach became very popular with radical groups. This paper aims to describe and present the whole problem of online radicalization with a focus on the platform *Twitter*, which is currently very much discussed due to its privatization and declaration of changing it to the 'free speech' board for all users. This can be a huge threat to the online audience if the policy of *Twitter* changes in favour of relaxing the rules and lessening control over the content, which can bring a new wave of 'unmonitored' radicalization posts. Moreover, this claim can be considered the biggest threat to the young generation addicted to technology of worldwide access to everything just in a few seconds. The lack of critical thinking and strong dissemination of misinformation even multiplies the threat to real contours.

CONCEPTUALISATION OF RADICALIZATION

Radicalization can be defined in many ways. Its connotation became more relevant after the 9/11 attacks in New York City, when the War on Terror was declared. Many authors agree that radicalization contains an adoption of some type of extremist view that is not accepted by the majority of society. Since there is no exact definition, there is a common agreement on what aspects radicalization is made of. According to Hafez and Mullins (2015), it is usually a "(1) gradual "process" that entails socialization into an (2) extremist belief system that sets the stage for (3) violence even if it does not make it inevitable" (Haffez and Mullins 2015).

Radicalization does not inevitably lead to violent behaviour, but it is its natural and most of the time a real threat (Haffez and Mullins 2015). Different authors frame its definition as "the process by which individuals (or groups) change their beliefs, adopt an extremist viewpoint and advocate (or practise) violence to achieve their goals" (Porter and Kebbell 2011). It is always essential to highlight the distinction between the necessary conditions for religious or political violence – cognitive and behavioural radicalization dimensions. It is also important to mention that these dimensions do not always produce violence. As being intuitive,

cognitive radicalization contains overtaking the values, worldviews, attitudes and approaches, or political beliefs. These values are usually different from the 'common ones' of the mainstream society. It can be said that the cognitive dimension is the passive form of the extremist stream, where no particular act of violence is done. On the other hand, there is a behavioural dimension of radicalization that is about taking action or rather participating in a range of radical activities. This can be also divided into two groups – legal or illegal – where clandestine can finally flow into terrorism (Haffez and Mullins 2015).

As Haffez and Mullins mention in their work, it is not usual that inactive individuals would migrate from no action to violent extremism. This is usually done by a series of radicalization steps, when some sort of ideological mediation is accepted. This is also linked to several commitments to radical belief. On the other hand, cognitive radicalization is more widespread since it is not so easily recognizable. Also, its impact is not so visible as in the case of the behavioural one. The threat lies in the terms of further gradation of radicalization and a change from cognitive action to real behavioural radical acts (Haffez and Mullins 2015).

Finally, it is important to amplify that radicalization is something different from violent extremism or terrorism. It can be understood as a process of changing the narrative of an individual's thinking that can lead to the extremes, such as terrorism (this is not predominantly the inevitable final step of the process). At the same time, it is a process of accepting violence (cognitive radicalization) as a way to achieve political or social goals. The further step involves the action itself that can lead to moving out from the legal way of activism. A combination of passive cognitive and active behavioural radicalization usually leads to violence, but it is not inevitable (Haffez and Mullins2015).

ONLINE RADICALIZATION

The Internet is a unique tool that enables anyone to get access to anything just in a few seconds. On the other hand, this challenging environment also serves the radicalized individuals or terrorists as a recruitment place with unlimited access to humanresources. From the start of the 'online' century, the Internet and the prevention of radicalization on it became a priority for individual governments, which are now facing homegrown radicalization since this environment's invention. Online radicalization is considered to be the most significant innovation used as a radicalizing tool since the 9/11 attacks that affects and enables the extremist groups' recruitment. As technology continues evolving (and

the Internet as well), there is also a development in methods of using different online platforms for radicalization. These are being misused by those who see the potential in technology usage to incite terror. Moreover, the Internet's rapid development also makes individual governments' counteractions more difficult (Neumann 2013).

It is widely known that the Internet is also used by extremist and terrorist groups. Some might try to imagine how it is being used by such groups, but it is not something difficult. The Internet was designed to be easy for users. Therefore, it is clear that radicalized individuals use the Internet like anybody else – they search for information, disseminate their ideas and promote causes, and mainly communicate with other related people (like-minded). The biggest advantage is that this can be done across great distances. The only difference from the usualusers of the Internet is the purpose of being online. These intentions can be understood in two ways: *communicative* and *instrumental*. While the communicative way just tries to get support and public attention, the instrumental way tends to facilitate acts of violence (Neumann 2013).

Firstly, the instrumental part can be invisible to an ordinary Internet user. It is being used for logistics – booking tickets, searching addresses, photos, and information. This can be hardly identified as suspicious behaviour. Furthermore, online platforms also serve as a useful sharing environment, where different training materials can be introduced to the audience, but experts do not see them as such. Since there were not many historical examples of extremists' cyberterrorism, the Internet environment seemed to be less effective in instrumental actions online than other forms at the start of the 2010s. Moreover, communication via emails or direct messages were often used to convict terrorist of incitement to any violent act (Neumann 2013). The situation within the society of understanding cyberterrorism changed through the years and at the end of the 2010s, there was an identified threat of using technologies for violent acts. For instance, the 2019 attack in Christchurch, New Zealand, on two Mosques was something new in terms of using the Internet for streaming the massacre that ended up in 50 deathsonline. This makes technology and terrorists (extremists) the most powerful allies with access to a global audience in a minute (Macdonald, Jarvis and Lavis 2019).

Secondly, there is a more powerful part – communicative radicalization. As long as the Internet is present, it is being used for radicalization (by violent extremists, and terrorists) for gaining support, getting public attention, and mainly recruiting new followers and sympathizers. In the past, there were static websites with no access to

the discussion that prevented the media from censorship and allowed the extremists to share unfiltered information. Since the Internet became more focused on security, the type of information shared changed dramatically regarding publishing basic information about ideologies etc. At the same time, such websites are banned in many countries. Another step was to set up forums for discussion – at the beginning, they were dependent on the world's largest Internet companies' providers. Afterwards, they were provided by independent individuals (funded by extremist groups – i.e., Al Ansar or White supremacists' Stormfront). Such forums became online platforms for communication, based on any possible topics with no danger of retribution (Neumann 2013).

The 21st century brought about multiple innovations that supported the extremists' 'onlinegoal' of spreading the ideology, propaganda or just information. This was about switching from text-based publishing to video-based ones. Moreover, the spread of user-based platforms and social networking presented a new level of communication across long distances, directly reaching the final addressees. This enabled extremists to 'step out from the shadow' of the Internet and publish and share the propaganda worldwide easily via YouTube, Facebook, Twitter, etc. This phenomenon of social networking was further deepened by smart devices and the shift of PC-based Internet to portable access that is being completely finalized nowadays (Neumann 2013). Furthermore, the instant need for development leads to improvement of applications' encryption that suits extremist groups. For instance, the application *Telegram* is wellknown for being used by the so-called Islamic State terrorist organization for sharing propaganda or direct messaging between individual members all around the world. Telegram's extraordinary features still attract terrorists mainly because of its secrecy benefits and also the provider's non-reliability in taking down violent-related channels (Tan 2017).

The Internet provides a great space for sharing ideas that are followingly being normalized and accepted by the audience. Social media platforms create echo chambers of like-minded people that help to confirm the promoted information. It is easier to convince someone to accept certain information within a group of like-minded people than in a group of many different-based individuals. Extremist groups often rely on social media platforms in the sense of exploiting the feeling of injustice among individuals and encouraging self-radicalization via shared ideological materials etc. The access to the global audience empowers such organizations in recruiting new members in different ways than in traditional in-person radicalization. For instance, this practice of attractingforeign fightersvia propaganda on social media is a

well-known method of al-Qaeda or ISIS (Hollewell and Longpré 2021).

According to Mølmen and Ravndal (2021), there are three phases of online radicalization of an individual. The first one is the *pre-radicalization phase*, identifying the impacts of pre-existing circumstances that led to the vulnerability of looking for or accepting different worldviews from the mainstream. Second is the *radicalization phase*, referring to an individual's process of becoming influenced by extremist content online. The last one is the *operational phase*, when an individual translates the new gained beliefs into action (Mølmen and Ravndal 2021).

The six important features indicate the process of radicalization or are at least favourable to supporting it – compensation, isolation, facilitation, echoing, acceleration, and action triggering. Compensation refers to an individual's dissatisfaction with the offline world and the need for further online presence. It is mainly connected to the pre-radicalization phase. Easily accessible content of different worldviews provides the vulnerable individual with the feeling of easy inclusion into such a group of followers. The vulnerability and different opinions opennessare often indicated by some sort of personal crisis or mental health issues. This is also connected to *isolation* when individuals excluded from particular societal groups are prone to online socialization via social media where social absorption is easier. It is often connected with mistrust in society itself, as well aswith the political order. Facilitation intensifies and facilitates access to extremist-related information that runs further radicalisation. Consequently, echoing refers to constant interaction with like-minded people that normalizes the extremist view as common sense and advocates the need for action. Social mediagre not designed to oppose but rather to bring individuals with similar opinions together. That makes radicalization process the biggest threat, given that it refers to referral objects, because they are not facing opposite ideas but confirming the extreme ones, amplified in the echo chamber. Acceleration presents online radicalization as a more advantageous and faster process (in the terms of the timeframe) than offline one, due to instant access to ideas or groups. Finally, action triggering refers to an impulse to commit an act of violence or the acceptance of participating in the radical framework (Mølmen and Ravndal 2021).

TWITTER AS A PLATFORM OF RADICALIZATION

Social media plays a key role in using the Internet. There were 3.6 billion users of social media in 2020 and it is estimated that the number of users will increase to 4.4 billion by 2025 (Statista Research Department 2022). One of the best-known platforms is *Twitter*, with about 330 million active users per month. More than 50 % of users use this platform for following the news and about 30 % of all users are there in order toeasilyshare the content with everyone on the site (Jay 2022). This platform was heavily medialized in late April 2022 when Elon Musk, the world's richest man, announced the acquisition of *Twitter*. This brought about several concerns from world security experts regardingthe change in *Twitter*'s policy when being privatized (Bove 2022). This platform is known for its simplicity in sharing ideas and was widely used by terrorist organizations (i.e., ISIS) for recruitment and sharing their propaganda.In 2016, *Twitter* reported that about 360 000 terrorist accounts were taken down during the previous year (Tan 2017).

Twitter technology and its uniqueness are based on immediate access to information from anyone connected online. The reactions that allow users to 'like', 'reply'or 're-tweet' help spreading the original message to a wider audience of followers of those who somehow reacted. Accounts recognized as belonging to terrorists were followed by single thousands of people, but they were connected to each other. When an individual account 'tweeted' some sort of information, the other independently re-tweeted and spread the reachable audience by his followers. That move multiplied the effect of the initiation tweet and attracted people not connected to the radical network. These radical organization accounts must be also precisely moderated in order to prevent them from being banned because of sharing disinformation or propaganda (Chatfield, Reddick and Brajawidagda 2015).

Furthermore, *Twitter* presents advantages for extremist groups in a certain level of anonymity because of the difficulty of achieving the source of tweets and their creators. The analysis of the Islamic extremist violent groups proved *Twitter* to be an arena showing a 'clash' with authorities in public. This is caused by the fact that many governments use this platform as the main communication channel with the wider public. This move supports the mobilization of followers and helps recruit new sympathizers that share a worldview that differs from the mainstream one. Moreover, the proliferation of accounts of individuals linked to ISIS raised questions and concerns about 'loneactor' attacks (Alava, Frau-Meigs and Hassan 2017).

The rise in the number of accounts related to violent groups led to a radical change in *Twitter* policy against such behaviour. Between 2015 and 2018, the social network banned 1.2 billion terrorist accounts (Reisinger 2018). Moreover, not just terrorist accounts were banned but accounts attributed with hate speech as well, such as the account of the former U.S. President Donald J. Trump after the incitement to hatred during the Capital Riot in Washington D.C. on January 6th, 2021 (Subramanian 2021). The concerns of the global security community focus on the announcement of Elon Musk that he is going to let all the banned users join the platform again in order to create a place of free speech. It is not known what will come and what control over the content will be imposed by the new owner, but the real threat of a wave of radicalization is being questioned (Stokel-Walker2022). According to Figliuzzi (2022), "the lines between free speech, dangerous speech, and unlawful speech are blurring at the speed of a keystroke". This claim is linked to the U.S. mass shooting cases, where evidence proved radicalization of individuals through online social networks and sharing of acts of violence. Relaxing the rules in order to post everything is rightly referred to as an initiation for expressing hatred and (as theory claims) creating echo chambers linked to the radicalization of individuals (Figliuzzi 2022).

CONCLUSION

Online radicalization is evidently currently most used and efficient (timeframe) method of recruiting new sympathizers. Moreover, the Internet allowed extremist violent groups to advocate their acts and get access to a wider audience. The innovation of technology and the development of social media empowered propaganda sharing, and some very well-known cases of illegal organizations (al-Qaeda or ISIS) got publicity through these platforms. The process of online radicalization differs from the face-to-face traditional method but also affects the broader scope of recipients of propaganda that making it easier to find new members. Since the rise of violent groups' online activity, multiple policy changes within the social network companies were made. Questions about Twitter security were raised recently because of the announcement of its privatization by Elon Musk, who publicly stated the will to allow anyone to share anything (according to law), with the goal of creating a free speech platform. The threat is hidden in the recognition of law offences in the continuous propaganda that is used by violent groups on Twitter. Further development will bring about challenges in thefightagainst the spread of disinformation and subsequent radicalization. On the one hand, *Twitter* can possibly become a platform for free speech but at the same time, it can also become the most suitable place for incitement of hatred and violence.

REFERENCES

- Allan, Jay. 2022. "Number of Twitter Users 2022/2023: Demographics, Breakdowns & Predictions." *Finances Online*. https://financesonline.com/number-of-twitter-users/.
- Alava, Séraphin, Frau-Meigs, Divina, and Hassan, Ghayda. 2017. *Youth and violent extremism on social media: mapping the research*. UNESCO Publishing.
- Bove, Tristan.2022. "All the ways that Twitter may change now that Elon Musk is in charge." *FORTUNE*.https://fortune.com/2022/04/25/elon-musk-twitter-six-big-changes/.
- Chatfield, Akemi T., Reddick, Christopher G., and Brajawidagda, Uuf. 2015. "Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided twitter networks." *Proceedings of the 16th Annual International Conference on Digital Government Research*: 239–249. doi: 10.1145/2757401.2757408.
- Figliuzzi, Frank.2022. "Elon Musk's ,free speech' collides with the reality of online radicalization." *MSNBC*.https://www.msnbc.com/opinion/msnbc-opinion/how-buffalo-shooting-proves-elon-musk-wrong-person-lead-twitter-n1295517.
- Hafez, Mohammed, and Mullins, Creighton. 2015. "The radicalization puzzle: A theoretical synthesis of empirical approaches to homegrown extremism." *Studies in Conflict & Terrorism* 38(11):958–975. doi:10.1080/1057610x.2015.1051375.
- Hollewell, Georgia. F., and Longpré, Nicholas. 2021. "Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet." *International Journal of Offender Therapy and Comparative Criminology* 66 (8): 1–18. doi:10.1177/0306624x211028771.
- Macdonald, Stuart, Jarvis, Lee, andLavis, Simon M. 2019. "Cyberterrorism Today? Findings From a Follow-on Survey of Researchers." *Studies in Conflict & Terrorism* 45 (8):1–26. doi:1 0.1080/1057610x.2019.16964.
- Mølmen, Guri N., and Ravndal, Jacob A. 2021. "Mechanisms of online radicalisation: how the internet affects the radicalisation of extreme-right lone actor terrorists." *Behavioral Sciences of*

- Terrorism and Political Aggression: 1–25. doi:10.1080/194344 72.2021.1993302
- Neumann, Peter R. 2013. "Options and Strategies for Countering Online Radicalization in the United States." *Studies in Conflict & Terrorism* 36(6): 431–459. doi:10.1080/1057610x.2013.78456
- Porter, LouiseE., and Kebbell, Mark R. 2011. "Radicalization in Australia: Examining Australia's Convicted Terrorists." *Psychiatry, Psychology and Law,* 18(2): 212–231. doi:10.1080/13218719.2010.48295
- Reisinger, Don. 2018. "Twitter Has Suspended 1.2 Million Terrorist Accounts Since 2015." FORTUNE. https://fortune.com/2018/04/05/twitter-terrorist-account-suspensions/.
- Statista Research Department. 2022. "Number of global social network users 2017-2025." *Statista*. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
- Stokel-Walker, Chris. 2022. "Right-Wing Trolls Are Trying to Break Back Into Twitter." *Wired*. https://www.wired.com/story/elonmusk-twitter-trolls/.
- Subramanian, Courtney. 2021. "A minute-by-minute timeline of Trump's day as the Capitol siege unfolded on Jan. 6." *USA Today*. https://eu.usatoday.com/story/news/politics/2021/02/11/trump-impeachment-trial-timeline-trump-actions-during-capitol-riot/6720727002/.
- Tan, Rebecca. 2017. "Terrorists' love for Telegram, explained." *Vox.* https://www.vox.com/world/2017/6/30/15886506/terrorism-isistelegram-social-media-russia-pavel-durov-twitter.*

^{*} Manuscript was received on September 8, 2022 and the paper was accepted for publishing on September 26, 2022.