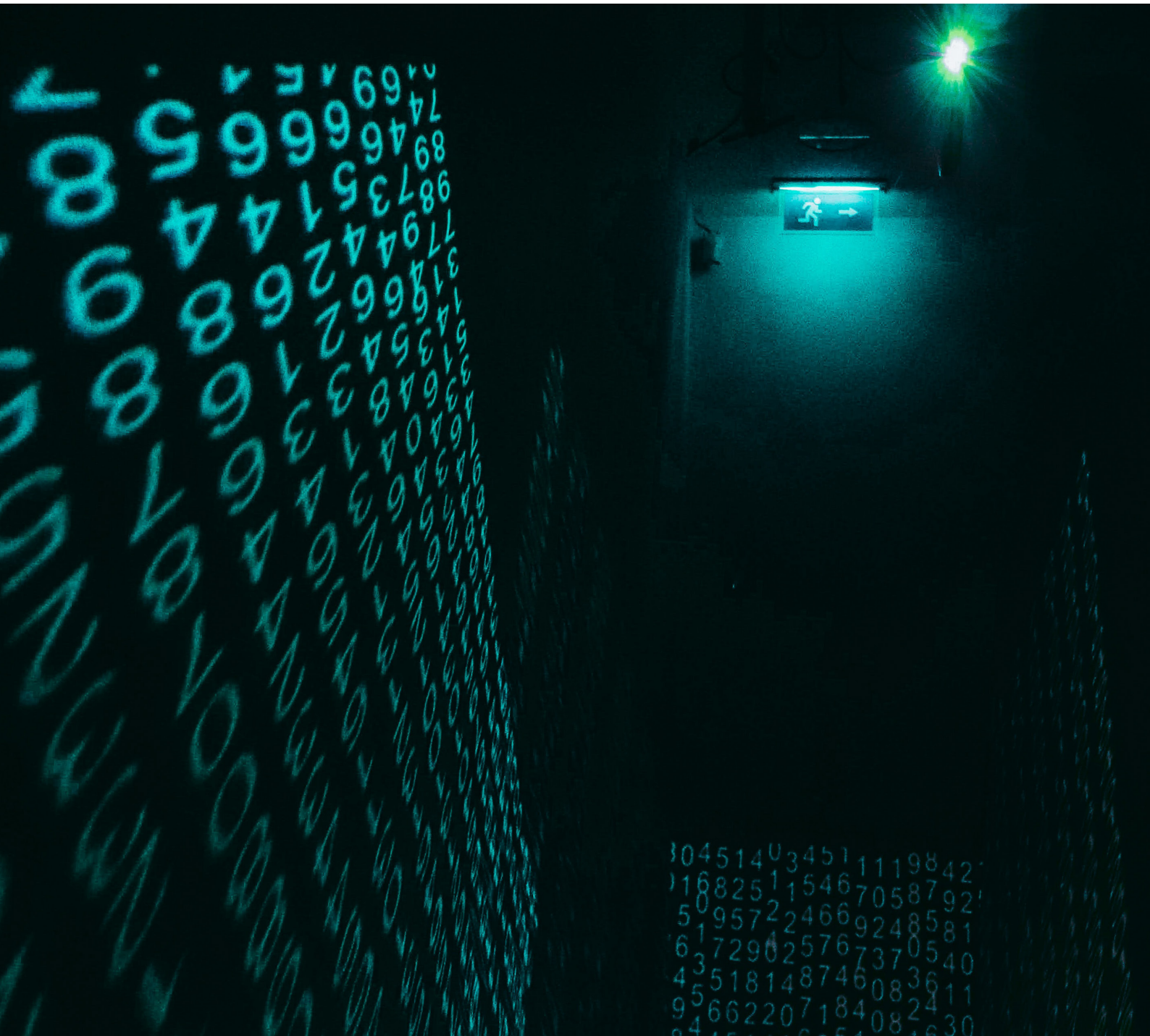
SISEKAITSEAKADEEMIA
Estonian Academy of Security Sciences
Co-funded by the European Union
Republic of Estonia Ministry of the Interior
INTERNAL SECURITY INSTITUTE

OKSANA BELOVA-DALTON

THE IMPACT OF NEW MEDIA AND THE INTERNET ON TERRORISM



THE IMPACT OF NEW MEDIA AND THE INTERNET ON TERRORISM

OKSANA BELOVA-DALTON

SISEKAITSEAKADEEMIA
Estonian Academy of Security Sciences

Front cover image: Pexels

Layout: Jan Garshnek
Editor: Kerli Linnat

ISBN 978-9985-67-407-9 (pdf)

www.sisekaitse.ee/kirjastus

CONTENTS

INTRODUCTION

By 2001, in Tim O'Reilly's (2005) terms, the "dot-com" Internet, or Web 1.0, had declined, largely due to its one-directional nature. Around 2003, the turning point occurred for the Internet, as Web 2.0 was born with its essentially interactive nature. Success stories of Web 2.0 are, among others, Wikipedia, in which users can both create and edit the content; BitTorrent, in which every client is also a server; eBay as collective commerce of all its users, etc. Other breakthroughs of Web 2.0 include the rise of social media, blogosphere, and chatting platforms. (O'Reilly, 2005)

The Web 2.0 revolution resulted in the emergence of new media, a nebulous concept that includes

> *virtual networks through which so-called many-to-many communication occurs; the specific platforms that facilitate such interactions, including blogs, Web forums, social networking websites, applications that allow the sharing of user-generated content, and so on; the Web-enabled devices that allow users to tap into these networks; and new media's interactive, collaborative nature (Amble, 2012, p. 340).*

This is the way in which new media is understood in this analysis, considering that various new platforms, with the concept of platform being the hallmark of Web 2.0, keep emerging and adapting to the needs of various users, including terrorists. For instance, closed Telegram or Discord groups; encrypted messaging services (Telegram, Signal, Tox, or dark web); crowdfunding platforms that can be used for terrorism financing, etc.

Internet is understood here as "including all communication, activity or content which takes place or is held on the world wide web (www) and cloud structures. This includes new online developments such as social media and networks." (Von Behr, *et al*, 2013, p. 2) However, the emphasis here is rather on what Sageman (2008, pp. 116) called "active Internet", including email, forums, and chat rooms, as opposed to "passive Internet" – the distinction being largely parallel to the one between Web 2.0 and Web 1.0. Another term to be used in this analysis is social media, being defined as

> *web-based applications and interactive platforms that facilitate the creation, discussion, modification, and exchange of user-generated content. Social networks, online platforms such as Facebook and Instagram where people interact and share content, are one type of social media. Other applications that fall under this category include blogs, business networks such as LinkedIn, social gaming, and virtual worlds, microblogs like Twitter, photo sharing such as Flickr, online product reviews, social bookmarking, YouTube videos, and digital forums. (Holbrook, 2022, p. 349)*

The above definitions of new media, active Internet, and social media overlap and are difficult to distinguish when used by various authors; hence, in this essay, all of them will be used to denote the interactive and cooperative nature characterising Web 2.0.

The rise of Web 2.0 occurred almost simultaneously with Al Qaeda's transformation from an organisation to a system with several nodes in different places. On the one hand, it was due to Al Qaeda's traditional jihadist websites being hacked and disrupted by security forces after 9/11 attacks (Awan & al-Lami, 2009, p. 57). On the other hand, in O'Reilly's (2005) terms, this can be called "Cooperate, Don't Control" principle, as Web 2.0 applications consist of a network of cooperating data services. Tapping into the virtual revolution, Al Qaeda started to effectively operate in the new media environment (Amble, 2012, p. 339). Decentralization of operations went so far as to encourage "Do It Yourself" terrorism, or leaderless resistance (Veilleux-Lepage, 2016, p. 39). New media also played a crucial role in the revolutionary breakthrough of terrorist propaganda by ISIS, which primarily used Twitter to disseminate their information and thus gained a wide audience (loc. cit., p. 41). By 2019, the Internet got filled by the extreme far-right propaganda to the extent that the far-right were said to have taken over the Web (Thompson, 2019). Hence, this essay will mainly focus on jihadi and far-right terrorism.

Jihadi groups already proliferated on the Internet when the online realm attracted the attention of security agencies and scholars (loc. cit., 37). However, since then, various counterterrorism measures have been undertaken to tackle terrorist content online, for instance, the Christchurch Call in 2019, European Parliament Regulation ((EU) 2021/784) on addressing the dissemination of terrorist content online in 2021, and EU's Digital Services Act in 2022. These are just a few examples of various measures of preventing abuse of the new media environment by violent extremists, terrorists, and their sympathisers for mobilisation, recruitment, and communication.

The aim of this essay is to critically analyse the impact of new media on terrorism. Hence, this essay will firstly focus on the characteristics of new media that make them a powerful tool in the hands of terrorists as well as how new media profoundly transformed the ways in which terrorists operate; secondly, the essay will then look at how various state and international actors are tackling terrorist activity in the new media environment and how new media also transformed the terrain of counterterrorism; thirdly, the essay will weigh whether the rapidly growing landscape of new media and its use by terrorists actually translate into the increase in the number of actual attacks. Terrorism is understood here along Bruce Hoffman's (2006, p. 40) lines as "deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change." This essay will focus primarily on the EU (and sometimes wider on the West), but also, where possible, on other countries and regions.

NEW MEDIA: CHARACTERISTICS AND THEIR EXPLOITATION FOR TERRORIST PURPOSES

New media allowed information consumers to simultaneously act as information communicators, yielding a vast number of information transmitters online. One consequence of this was the creation of virtual networks of like-minded people, preferring to receive information from the same sources. These virtual networks brought together persons with converging (extreme) worldviews from different geographical locations[1], providing them with strong virtual cohesion. Selective consumption of information by devotees of specific (extreme) ideologies increased this virtual cohesion, resulting in **crowdsourcing**[2]. Terrorist groups exploited the growing sense of group membership in their virtual networks to channel their propaganda and facilitate training (Amble, 2012, p. 340). ISIS resolved to crowdsource terrorism, or outsource the conduct of attacks to their followers either to attract them to Syria in 2014 or encourage them to perpetrate attacks in their locations (Yang Hui, 2017, p. 337). Virtual networks are very often considered as facilitating radicalisation[3] and terrorism:

> *Individuals carrying out attacks alone have been associated mainly with jihadist terrorism and right-wing terrorism and violent extremism. This does not necessarily mean that these individuals act in complete isolation. Online community building often plays a key role, as it connects peers virtually on a global scale. This drives radicalisation and provides access to terrorist propaganda, instructional material and opportunities for procurement of weapons and explosives precursors. (Europol TE-SAT 2022, p. 4)*

Moreover, it is argued that immersion into extremist forums can foster mortality salience and thus increase support for terrorist tactics as well as create a sense of moral outrage which can trigger violent behaviour (Powers & Armstrong, 2014, p 235). Notably, in terms of Indonesia, crowdsourced terrorism was not a salient factor in recruitment to ISIS (as offline social networks were more prevalent in this); rather, it contributed to the perpetuation of ISIS propaganda online (Yang Hui, 2017, p. 350). In addition, online training does not directly translate into a successful attack offline – "the actual possession

1 Hence, new media can be truly global in its scope and accessibility.

2 The term was coined in 2006 to mean the invitation of large numbers of anonymous people to contribute with their ideas, innovations, and solutions (Yang Hui, 2017, p. 339).

3 Radicalisation is understood here as "socialization into extremism that manifests itself in terrorism" (Coolsaet, 2022, p. 191).

of arms is only half the story; one must also know how to use them. It is easy to shoot, but appreciably more difficult to hit anything." (Most, 1884)

Another feature of new media is narrowcasting or niche marketing or "generation of targeted communication and filtered content based on preference, network, background, and choice history that aims digital matter at specific portions of an online community" (Holbrook, 2022, p. 352). Based on this principle, "suggestions" are made, e.g., by YouTube, to users based on their consumption habits, and it has been suggested that this feature holds visible and recommends extremist videos. (ibid.) This can also be referred to as algorithmic amplification. Within Web 2.0 world, algorithmic data management allows to reach out to the entire web, or "to the long tail and not just the head" (O'Reilly, 2005), including various fringe groups. According to Valentini and colleagues (2020, p. 5), the user's metadata and tags allow algorithmic mechanism to create an immersive user-tailored environment and a personalized virtual experience to keep the user at the platform. Social media depend on these algorithmic systems, which have been blamed for being the polarizing tools that expose users to pro-attitudinal content and allow them to contact with the like-minded virtual networks. This way, new media can create homogeneous virtual **echo chambers**. (loc. cit., p. 6)

Echo chambers created online by the use of filtering and recommendation technology are regarded by many policymakers and academics as creating an effect of an epistemic bubble, where communities are deprived of feedback and this amplifies the group's viewpoints. This allegedly leads to polarization of opinions across communities, thus increasing extremism. (O'Hara & Stevens, 2015, p. 401) An echo chamber is "a social structure from which other relevant voices have been actively discredited" and that "brings its members to actively distrust outsiders", hence becoming something like a cult (Thi Nguyen, 2018). In terms of extremist groups, this leads to increasing radicalisation of their members. However, according to O'Hara & Stevens (2015, p. 417), "echo chambers do not always have malign effects; most people have routes out of the chamber; the best conditions for their existence do not generally obtain." Also, creation of echo chambers is rather conditioned by the user's choices rather than algorithmic interference (Valentini, *et al*, 2020, p. 6). Still, individual decisions are pre-determined by the highly pre-structured environment in which a person operates (Steglich, 2019). Nevertheless, Cassam (2022, p. 183) stresses that radicalisation is an expression of an individual's own agency and cannot just happen to a person, for instance, in an echo chamber.

Yet another important feature of new media is the rise of blogging. Notably, the blogging community is highly self-referential, with bloggers increasing their power and visibility through paying attention to other bloggers. This is amplified by the echo chamber effect. Blogosphere, or "wisdom of crowds", is hard to compete with, because in the world of Web 2.0 it is the audience who decides what is important. (O'Reilly, 2005) Breivik admitted that involvement with far-right blog "Gates of Vienna" contributed to the iterative process of his radicalisation, while neo-Nazi activist Wade Michael Page, suspected of perpetrating the Gurdwara attack in Wisconsin in 2012, was closely affiliated with the online portal of Hammerskin Nation, a U.S. skinhead movement. While seen as lone actors, these violent extremists are believed to be representing a broader constituency, while the latter are becoming increasingly virtual (Powers & Armstrong, 2014, p. 236).

Streaming is another prominent feature of new media capitalised on by terrorists. Skilful use of streaming by ISIS made a breakthrough for their propaganda:

> *al-Qaeda's grainy battlefield videos and tedious 2-hour-long monologues have been replaced by IS' high definition steadicam shots – with carefully scripted and edited nar-*

> *ration – and multilingual messaging aimed, in part, at radicalizing young Muslims, and at encouraging them to emigrate to the newly-founded caliphate. (Veilleux-Lepage, 2016, pp. 36–37)*

For example, there is evidence that young Muslims were radicalized by YouTube videos of the violent treatment of fellow Muslims in other parts of the world (Cassam, 2022, p. 185).

Streaming also allowed for making attacks even more dramatic and shocking, in line with Jenkins' (1975, p. 4) definition of terrorism as theatre. With new media, terrorist attacks can be livestreamed, maximising the impact of this violence and visibility and prominence through immediacy. Christchurch attacks in 2019 with the first-person gaming view and made with mimicking YouTube star moments were livestreamed on Facebook, with Tarrant's attack video and manifesto he shared on Twitter spreading almost uncontrollably online. Content going viral (that platforms seek) is another feature of new media that terrorists capitalise on – attackers use Internet as part of their actions to publish pictures and writings before the attack for these to be further amplified and circulated by social media, thus giving fame and status to the perpetrator. The latter hence receives attention, which is often translated into acknowledgement, recognition, and even authority to force political change (Hoffman, 2006, p. 197).

Overall, in 2019, far-right attacks in New Zealand, the U.S., Norway, and Germany were part of a global wave of violent incidents, with perpetrators from similar online transnational communities taking inspiration from each other. (Europol TE-SAT, 2020, p. 18) Tarrant was partly inspired by Breivik and actively used 8chan – an Internet forum where far-right extremists subsequently promoted the video of his attack and manifesto.

Tarrant's attack demonstrated the importance of gaming in the far-right extremism and terrorism. In fact, "gaming platforms and services are increasingly used by right-wing terrorists to channel terrorist propaganda targeting a younger generation of users." (Europol TE-SAT 2022, p. 5) Gaming as a metaverse provides a social space where users can communicate and build their communities, shape and share experiences. Some neo-Nazis have been found to create their own chatrooms and share content using online gaming servers (Holbrook, 2022, p. 360).

NEW MEDIA VS OFFLINE DIMENSION IN TERRORISM AND RADICALISATION

All of the above, however, is not to neglect the offline dimension of terrorist operational and tactical activities, like, for instance, trainings and personal communication. There is no guarantee that online commitments and skills will translate into such offline. One possibility is that online terrorist community members are sufficiently satisfied with their virtual discussions with the like-minded peers and experience with no necessity for physical engagement with terrorism (Ramsay, 2013, p. 186). It should be noted that,

> *fundamentally, IS recognizes that the majority of Western supporters will never engage in kinetic actions such as terrorist acts in their homelands, or fighting abroad. Instead, IS utilizes these supporters for the purpose of disseminating information and propaganda relating to their cause. Arguably, not requiring Western supporters to engage actively in physical violence allows IS to garner the participation of these supporters without asking them to cross moral boundaries they might not feel comfortable crossing. (Veilleux-Lepage, 2016, p. 44)*

Hence, online and offline dimensions need to be balanced in order to keep operations afloat. Nevertheless, "it has become something of a cliché to blame radicalisation on social media" (Cassam, 2022, p. 183), like, for instance, RAND report (von Behr, *et al*, 2013) which maintains that Internet which includes social media may facilitate radicalisation and act as an echo chamber for extremist ideologies. The START study found that social media shortens the time period between first documented interest in extremism and attempted participation in extremist action (START, 2018, cited in Holbrook, 2022, p. 357). Powers and Armstrong (2014, p. 236) argue that, for most government agencies and experts, "the growing importance of the Internet in radicalisation is the single most significant innovation to have affected homegrown radicalisation since the 11 September attacks in 2001."

However, the aforementioned RAND report does not conclude that Internet and social media allow radicalisation to occur without any physical contact – for instance, Anwar Al-Awlaki self-radicalised, while those whom he radicalised online either emailed or texted him (Cassam, 2022, p. 184). Moreover, "there is no easy offline versus online violent radicalisation dichotomy to be drawn. It may be a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviours are compartmentalized

across these two domains." (Gill, et al, 2017, p. 100 cited in Holbrook, 2022, p. 364) A parallel could be drawn with the research on global online school shooting communities, where material on these massacres and their perpetrators is shared, created, and circulated. Research has shown that, in various parts of the world, deep interest in school shootings experienced by virtual community members does not equal a desire to perpetrate a school shooting (Raitanen, 2021).

Interestingly, those "who had been most active on social media platforms were found to have lower success rate in terms of actual outcomes, whether in the form of formulating terrorist plots or travelling overseas to become combatants. Those who were most successful in their orchestration of terrorist plots, in turn, abstained from social media usage altogether" (START, 2018, cited in Holbrook, 2022, p. 357). Moreover, active use of social media by ISIS volunteers in Syria and Iraq either allowed for their detection or/and provided tangible battlefield evidence to prosecute them in courts. In addition, during COVID-19 pandemic, ISIS spokesperson Abu Hamza al-Qurashi urged ISIS supporters to spend less time on social media and make "more effort on high-impact attacks, jailbreaks and other operational activity" (Burke, 2021).

Also, it cannot be assumed by default that terrorist actors only get supportive feedback and cannot fall prey to negative comments online or even digital hate, dismantling their brand management. One extreme example could be the repulse felt by fellow Muslims over too hostile beheading videos spread by Zarqawi on jihadist and video-sharing websites that Ayman al-Zawahiri (2005) came to criticize in his letter to Zarqawi. It is also possible to prove terrorists wrong using effective counter-narratives on social media (Holbrook, 2022, p. 360).

Notably, social media and, more widely Web 2.0 technology with its participatory and horizontal nature may make it hard for leaders of terrorist organisations to keep their hierarchical position (Holbrook, 2022, p 359). The same applies to controlling, for instance, the proliferation and production of unattributed jihadist messages. However, to leverage the situation, Al-Qaeda quickly recognized the significance of decentralization of the group's operations and encouraged leaderless resistance or individual jihad strategy, including electronic jihad. Internet also allowed to produce Inspire magazine and target English-speaking readership with do-it-yourself approach to terrorism. Highly decentralized operations of ISIS online as well as offline allow the group stay afloat even if one of their branches fails online or offline. (Veilleux-Lepage, 2016, pp. 39–40)

NEW MEDIA AND ONLINE COUNTERTERRORISM MEASURES

Jihadist groups already proliferated in cyberspace when it drew the attention of security agencies and scholars (Veilleux-Lepage, 2016, p. 37). For instance, between 2009 and 2016, most of individuals charged in the U.S. for jihadist-related offences were connected to or inspired by Awlaki, a jihadist YouTube star (Cassam, 2022, p. 184). By 2019, it had become obvious that terrorists were seeking notoriety both online and offline, so Prime Minister of New Zealand Jacinda Ardern said she would deny the accused perpetrator of Christchurch attacks the fame he sought by refusing to even speak his name; his face was blurred out in photographs and the video feeds showing him escorted into the courtroom (Mahtani & Fifield, 2019). Consequently, Christchurch Call, in which more than 120 governments, online service providers, and civil society organisations are cooperating to eliminate terrorist and violent extremist content online was initiated (see Christchurch Call, n. d.).

In 2021, European Parliament issued Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. This regulation establishes a legal framework to remove terrorist content within one hour of receiving a removal order from an authorized national authority. The regulation needs to be implemented by all EU Member States with the aim to prevent terrorists from using Internet to propagate their ideology, terrorize, radicalise, and recruit people. (Kersa, 2023)

Furthermore, in 2022, EU's Digital Services Act (DSA) was adopted, aiming at preventing manipulative algorithmic systems from misusing online services by amplifying the spread of disinformation, and for other malicious purposes. The DSA primarily concerns online intermediaries and platforms, e.g., "online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms" (European Commission, n. d. (a)). Companies like Tech against Terrorism specialise in detecting terrorist content online. Tech Against Terrorism employs its flagship tool called Terrorist Content Analytics Platform (TCAP) to track terrorist content and alert smaller Internet platforms so that they can remove it. (see Tech Against Terrorism, n.d.) Moreover, authorities can demand "back door" or access to encrypted messages on case-by-case basis, for instance, if a private group on Telegram is known to be used by a terrorist group (Holbrook, 2022, p. 351).

Social media and networking platforms are also interested in tackling terroristic content since this threatens their reputation among users as well as stringent policies on behalf

of the governments. For instance, Google, Facebook, and Microsoft organised "Global Internet Forum to Counter Terrorism" (Holbrook, 2022, p. 359), while the EU has the EU Internet Forum which provides a collaborative environment for EU governments, Internet industry, and other partners and aims at tackling terroristic and extremist content, looking at the issues of algorithmic amplification, borderline content, etc. EUIF aims at reducing access to terrorist content as well as spread effective counternarratives online (European Commission, n. d.). EUIF has contributed to, for instance, the creation of Europol's EU Internet Referral Unit (which flags terrorist content and notifies online platforms of it), Civil Society Empowerment Programme (which urges SCOs to tackle terrorist and violent extremist content online and produce effective counter-narratives), EU Crisis Protocol (which allows EU Member States and Internet platforms to rapidly and in a coordinated manner tackle the viral spread of terrorist content online after an attack happens) which largely follows the model of Christchurch Call. Among 58 governments committed to Christchurch Call are four Islam-majority countries (Jordan, Indonesia, Tunisia, and Senegal), which is something that can be effective in tackling also ISIS's and other Islamist terrorist content online:

> *The pervasiveness of its [ISIS's] ideology and message means that defeating the group will require more of Western governments than a simple military response in Iraq, or even elsewhere in the Middle East: the message itself needs effective countering as well. Western countries need to use an integrated, coordinated, and synchronized approach, with support from allied countries in the Islamic world and Muslim civil society more generally, in order to accomplish such a goal. (Veilleux- Lepage, 20216, p. 46)*

However, social media companies (Facebook, Twitter, TikTok, YouTube, Snapchat, etc) are still commercial enterprises at their core with their major aim of making a profit. Profit is click-based – cost per click in Web 2.0 as opposed to page views in Web 1.0 (O'Reilly, 2005). Terrorism-related content gets more clicks, so social media companies are likely to play with their definitions of terrorism to keep their business profitable. Users, in turn, are producing more of borderline content (so-called "lawful but awful" content) which avoids algorithms and is resilient to deplatforming.

In addition, it is always possible for terrorists and extremists to migrate to platforms that cooperate less with governments and where it is possible to have encrypted communication in closed groups (e.g., Gab, Telegram, Discord, etc.) or online gaming servers. Moreover, for instance, after the EU Regulation on addressing the dissemination of terrorist content online entered into force on 7 June 2022, the European Commission has decided to initiate infringement proceedings against 22 Member States for failing to fully implement the obligations under the regulation. (Kersa, 2023) Yet another interesting circumstance is that, although Tarrant's manifesto was deplatformed, manifestos by many other prominent terrorists, (including, for instance, incel Elliot Rodger, the far-right Buffalo shooter, the Unabomber, etc) are still freely available online.

NEW MEDIA VS NUMBER OF TERRORIST ATTACKS OFFLINE

Yet another way to assess the impact of new media on terrorism is to see whether, with the growing scale and scope of new media, the number of actual terrorist attacks is also growing. An interesting case to observe would be Covid-19 pandemic which swept across the world for two years, 2020 and 2021, respectively. A UN report warned that ISIS threatened with a wave of violence "to end its marginalisation from the news", as the group received captive audience due to social isolation and people spending more time online (Burke, 2021). The report, however, warned against possible upsurge of Islamist terrorism in conflict zones and parts of the world where Islamist extremist groups are well-established rather than in "non-conflict zones" like Europe (ibid.). According to Basit (2020, p. 11), since the outbreak of the pandemic, the amount of Islamist extremist materials increased on social media platforms, with terrorist groups seeking to capitalise on social distancing measures, as people were confined to their homes and used social media to communicate with their families and friends as well as to consume the content produced there. In times of crisis, people need coping mechanisms, e.g., religion, to handle their anxiety and fears; so, it was possible for terrorist groups to appeal to people's fears, expectations, and hopes and this way lure vulnerable segments of populations to their extremist narratives (ibid.).

EU Counter-terrorism coordinator warned as of 14 May 2020 that, although since the beginning of the pandemic the number of terrorist attacks had not grown or even declined in some parts of the world, the situation was unlikely to endure due to rapid proliferation of extremist discourse online regarding the crisis. Another alarming factor was a diminished focus of governments and organisations on counterterrorism, likely to last for months and even years, in the light of pandemic (EU Counter-terrorism coordinator, p. 2). The far-right extremists were also intensively exploiting the pandemic to reach out to wide audiences, especially to anti-vaxxers, with the aim to "co-opt anti-vaxxers to unwittingly serve neo-Nazi ends" (Hay, 2021). It was also admitted that online far-right conspiracies could result in offline actions: "throughout the pandemic, we've seen how easily and quickly an online conspiracy can result in acts, sometimes violent, in the real world" (Mollie Saltskog, cited in Hay, 2021).

However, within the EU, the impact of the pandemic was mostly visible in the shaping of extremist narratives, making some persons, especially younger people and minors, more vulnerable to radicalisation and recruitment into terrorism and extremism (Europol TE-SAT, 2022, p. 3), while the number of actual attacks did not grow – in the West, the number of terrorist attacks fell by 68% in 2021, while most attacks were committed

in Afghanistan, Sahel region, Iraq, and Somalia (Institute for Economics & Peace, 2022, p. 4).

According to the Global Terrorism Index (Institute for Economics & Peace, 2023, p. 2), levels of terrorism remarkably fell between 2015 and 2019, and these improvements continued for the past three years. The primary factor behind terrorism is violent conflict, since 88% of attacks and 98% of terrorism deaths are occurring in countries involved in an armed conflict, including ten countries most affected by terrorism in 2022. The underlying drivers of terrorism are complex and systemic, including "poor water utilisation, lack of food, ethnic polarisation, strong population growth, external interventions, geopolitical competition, pastoral conflict, the growth of transnational Salafi-Islam ideology and **weak governments**. Most of the terrorist activity occurs along borders where **government control is weakest**." (ibid.) Hence, the impact of new media on the number of actual terrorist attacks can only be assessed in the context of these more complex systemic terrorism drivers. In Holbrook's (2022, p. 356) terms, in countries where social media usage is high, while the level of government control is relatively low, "social media usage has been identified in a wide range of terrorism-related activities". What new media can contribute to in the countries and regions most impacted by terrorism is the spread of Islamist propaganda as well as ethnic polarization by giving "those with shared identities and grievances /…/ new opportunities to form collectives around them." (ibid.).

In the West, the number of attacks continues to decline, with Islamist extremists perpetrating only two attacks in Europe, four attacks in the UK and eight attacks in the U.S. in 2022. The West is rather affected by the far-right terrorism, resulting in 14 deaths in 2022 (Institute for Economics & Peace, 2023, p. 3). Hence, if new media were a significant driver of terrorism in the West, the growing span of new media and its domination by the far-right propaganda would have led to the increase in terrorist attacks, especially during the pandemic, but this number has, conversely, decreased. It follows that a major factor of terrorism is government control, primarily offline, but not ignoring the online dimension, too, searching for and implementing effective approaches to technological challenges in cooperation with other governments, international organisations, and online providers.

CONCLUSION

New media has become an essential part of terrorists' operational repertoire. Advantages of new media for terrorists include the fact that it allows the groups to put across their own narratives and perspectives, avoiding possible distortion of their ideas and acts by mainstream media (Holbrook, 2022, p. 348). New media facilitated crucial paradigmatic shifts for Al-Qaeda and ISIS, including decentralization of operations online as well as offline, leading to the sanctioning of leaderless resistance or individual jihad and, among other things, electronic jihad for those not wishing to come to the battlefield. The outreach terrorists can achieve via new media is global, while the opportunity to create high-quality propaganda is unprecedented. Communication technologies provided to terrorists by new media are unparallel – for instance, a livestreamed mode of terrorism appeared, tailored to have popular features of gaming and social media platforms.

However, the online realm does not always directly translate into the offline realm – for instance, participating in an online extremist or terrorist community or even undertaking training does not mean that a person is a potential fighter or that they can use tactical weapons successfully. This means that offline communication and trainings as well as other operations are as crucial as ever.

Chiangi (2021) argued that the current wave of religious terrorism is especially potent and will not end within the lifespan predicted by David Rapoport due to the "the powerful impact of the internet and technology on terrorist operations." However, a strong stable state prevents the direct translation of the power given to terrorists by new media into a significant increase of committed attacks. For instance, during the pandemic, as most people spent huge amounts of time in isolation and online, there was no upsurge in terrorism in countries that are otherwise not on the list of countries most affected by terrorism.

New media also importantly transformed counterterrorism operations by making online surveillance more encompassing – legal frameworks appeared along with various security agencies and tech companies specialising in the removal of terrorist content online. Security services can demand a "back door" to closed Telegram groups, deplatform terrorist content, infiltrate closed online groups and bust them if these become a serious threat. Still, effectiveness of counterterrorism measures online remains uncertain, since click-based profiteering of social media platforms can lead to circumventing legal frameworks, while it is unclear whether there can ever be enough staff to monitor the endless amount of information on the Internet even with the help of algorithms. Nevertheless, it can be said that the strength of state control in the West encompasses all issues related to terrorism. Hence, it can be concluded that terrorism, which has been accompanying human societies for hundreds of years, will be where humans are, including online, as "technology and social media are inextricably woven into our experience" (Sam, 2019, p. 333); however, there are other more complex and systemic factors, including government control, behind the number of actual terrorist attacks offline.

BIBLIOGRAPHY

Amble, John Curtis, 2012. Combating Terrorism in the New Media Environment. In *Studies in Conflict & Terrorism*, 35(5), pp. 339–353.

Awan, Akil N., Al-Lami, Mina, 2009. Al-Qa'ida's Virtual Crisis. In *The RUSI Journal*, 154(1), pp. 56–64.

Basit, Abdul, 2020. The COVID-19 Pandemic: An Opportunity for Terrorist Groups? In *Counter Terrorist Trends and Analyses*, 12 (3), pp. 7–12.

Burke, Jason, 2021. Islamic extremists planning 'rash of attacks' after Covid curbs lifted, says UN. *The Guardian*, 5/02/2021. Available at https://www.theguardian.com/world/2021/feb/05/islamic-extremists-planning-rash-of-attacks-after-covid-curbs-lifted-says-un, accessed 22 April 2023.

Cassam, Quassim, 2022. *Extremism: A Philosophical Analysis*. London & New York: Routledge.

Chiangi, Michael Aondona, 2021. Critically Examining David Rapoport's Four Waves Theory of Modern Terrorism in the Light of Factual Historical Events. In *African Journal on Terrorism*, 11(1), pp. 11–29.

Christchurch Call, n. d. *Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online*. Available at https://www.christchurchcall.com/, accessed 19 April 2023.

Coolsaet, Rik, 2022. When Do Individuals Radicalize? In Diego Muro & Tim Wilson (eds) *Contemporary Terrorism Studies*. Oxford: OUP, pp. 178–200.

EU Counter-Terrorism Coordinator, 2020. *Terrorism in times of corona: The development of the terrorist threat as a result of the Covid-19 crisis*. Available at https://data.consilium.europa.eu/doc/document/ST-7838-2020-REV-1/en/pdf, accessed 24 April 2023.

European Commission, n.d. *European Union Internet Forum (EUIF)*. Available at https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en, accessed 19 April 2023.

European Commission, n. d. (a). *The Digital Services Act package*. Available at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, accessed 22 April 2023.

Europol, 2020. *European Union Terrorism Situation and Trend report 2020 (TE-SAT)*. Available at https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020, accessed 22 April 2023.

Europol, 2022. *European Union Terrorism Situation and Trend report 2022 (TE-SAT)*. Available at https://www.europol.europa.eu/publication-events/main-reports/

european-union-terrorism-situation-and-trend-report-2022-te-sat#downloads, accessed 22 April 2023.

Hay, Mark, 2021. The 'Terrorgram' Plot by Neo-Nazis to Seduce Anti-Vaxxers. *The Daily Beast*, Available at https://www.thedailybeast.com/anti-vaxxer-panic-about-the-pfizer-coronavirus-vaccine-meets-neo-nazi-fantasies-in-corona-chan, accessed 22 April 2023.

Hoffman, Bruce, 2006. *Inside Terrorism*. New York: Columbia University Press.

Holbrook, Donald, 2022. Social Media and Terrorism. In Diego Muro & Tim Wilson (eds), *Contemporary Terrorism Studies*. Oxford: OUP, pp. 345–367.

Institute for Economics & Peace, 2022. *Global Terrorism Index 2022*. Available at https://reliefweb.int/report/world/global-terrorism-index-2022, accessed 22 April 2023.

Institute for Economics & Peace, 2023. *Global Terrorism Index 2023*. Available at https://reliefweb.int/report/world/global-terrorism-index-2023, accessed 22 April 2023.

Jenkins, Brian, 1975. *International Terrorism: A New Mode of Conflict*. Los Angeles: Crescent Publications.

Kersa, Kristina, 2023. European Commission Opens 5 Infringement Procedures Against Estonia. *ERR*, 26/01/2023. Available at https://news.err.ee/1608864740/european-commission-opens-5-infringement-procedures-against-estonia#:~:text=The%20European%20Commission%20has%20opened,children%2C%20and%20restricting%20hate%20speech., accessed 20 April 2023.

Mahtani, Shibani, Fifield, Anna 2019. 'You will never hear me mention his name': New Zealand's Ardern vows to deny accused shooter notoriety. *The Washington Post*, 19/03/2019. Available at https://www.washingtonpost.com/world/asia_pacific/you-will-never-hear-me-mention-his-name-new-zealands-ardern-hopes-to-deny-shooter-notoriety/2019/03/19/b4d163b8-49b5-11e9-8cfc-2c5d0999c21e_story.html, accessed 22 April 2023.

Most, John, 1884. Advice for Terrorists. In *Freiheit*, 13. september. Source: Laqueur, Walter/Alexander, Yonah, (eds.) (1987): *The Terrorism Reader: A Historical Anthology*, revised edition. New York: New American Library Trade, pp. 100–108.

O'Hara, Kieron, Stevens, David, 2015. Echo Chambers and Online Radicalism: Assessing the Internet's Complicity in Violent Extremism. In *Policy & Internet*, 7(4), pp. 401–422.

O'Reilly, Tim, 2005. *What is Web 2.0*. Available at https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1, accessed 14 April 2023.

Powers, Shawn, Armstrong, Matt, 2014. Conceptualizing Radicalisation in a Market for Loyalties. In *Media, War & Conflict*, 7 (2), pp. 233–249.

Ramsay, Gilbert, 2013. *Jihadi Culture on the World Wide Web*. New York: Bloomsbury.

Raitanen, Jenni, 2021. *Deep Interest in School Shootings Online*. PhD Dissertation. Available https://trepo.tuni.fi/handle/10024/124428, accessed 22 April 2023.

Sageman, Marc, 2008. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia, PA: University of Pennsylvania Press.

Sam, Cecile H., 2019. Shaping Discourse Through Social Media: Using Foucauldian Discourse Analysis to Explore the Narratives That Influence Educational Policy. In *American Behavioral Scientist*, 63(3), pp. 333–350.

Steglich, Christian, 2019. *Why echo chambers form and network intervention fail: Selection outpaces influence in dynamic networks*. Available at https://arxiv.org/abs/1810.00211, accessed 21 April 2023.

Tech Against Terrorism, n.d. *Tech Against Terrorism is supporting the tech industry tackle terrorist exploitation of the internet, whilst respecting human rights*. Available at https://www.techagainstterrorism.org/, accessed 22 April 2023.

Thi Nguyen, C, 2018. Escape the Echo Chamber. In *Aeon Magazine*. Available at https://aeon.co/essays/why-its-as-hard-to-escape-an-echo-chamber-as-it-is-to-flee-a-cult, accessed 21 April 2023.

Thompson, Derek, 2019. Why the Internet Is So Polarized, Extreme, and Screamy. *The Atlantic*, 23/05/2019. Available at https://www.theatlantic.com/ideas/archive/2019/05/how-did-the-far-right-take-over-the-web/590047/, accessed 22 April 2023.

Valentini, Daniele, Anna Maria Lorusso & Achim Stephan, 2020. *Onlife* Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalisation. In *Frontiers in Psychology*, 2020; 11: 524.

Veilleux-Lepage, Yannick, 2016. Paradigmatic Shifts in Jihadism in Cyberspace: The Emerging Role of Unaffiliated Sympathizers in Islamic State's Social Media Strategy. In *Journal of Terrorism Research*, 7 (1), pp. 36–51.

Von Behr, Ines, Anais Reding, Charlie Edwards & Luke Gribbon, 2013. Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism. Santa Barbara, CA: RAND Corporation. Available at https://www.rand.org/pubs/research_reports/RR453.html, accessed 20 April 2023.

Yang Hui, Jennifer, 2017. Crowdsourcing Terrorism: Utopia, Martyrdom and Citizenship Reimagined. In *Journal of Asian Security and International Affairs*, 4(3), pp. 337–352.

Zawahiri, Ayman, 2005. *Letter to Abu Musab al-Zarqawi*. Available at https://ctc.westpoint.edu/harmony-program/zawahiris-letter-to-zarqawi-original-language-2/, accessed 19 April 2022.

THIS WORK ANALYSES THE IMPACT OF NEW MEDIA AND THE INTERNET ON BOTH TERRORISTS' OPERATIONAL REPERTOIRE AND COUNTERTERRORISM OPERATIONS.

The advantages of new media for terrorists include the fact that it allows the groups to put across their own narratives and perspectives, avoiding possible distortion of their ideas and acts by the mainstream media. New media facilitated crucial paradigmatic shifts for Al-Qaeda and ISIS, including decentralization of operations online as well as offline, leading to the sanctioning of leaderless resistance or individual jihad and, among other things, electronic jihad for those not wishing to come to the battlefield. New media also importantly transformed counterterrorism operations by making online surveillance more encompassing – legal frameworks appeared along with various security agencies and tech companies specialising in the removal of terrorist content online.

sisekaitse.ee