sciendo

Terrorism in the age of new technologies

Florian Hartleb

School of International Relations
Modul University Vienna
Am Kahlenberg 1
Vienna 1190, Austria
Florian.Hartleb@modul.ac.at

Abstract: This article examines how the phenomenon of terrorism is being reshaped by rapid advances in digital technology. It aims to provide a comprehensive analytical framework for understanding the impact of encrypted communication, online radicalization, the gamification of violence and emerging cyberterrorist threats. By exploring both the evolving tactics of extremist actors and the new vulnerabilities within modern societies, the study seeks to clarify how technological change is transforming the form and function of contemporary terrorism and to identify key areas for further research and policy response.

Keywords: *artificial intelligence, gamification, lone actors, new technologies, teenager terrorism, terrorism, TikTok radicalization*

1. Introduction

In the rapidly evolving digital age, technology has transformed nearly every aspect of human life (Harari, 2024)—from how we communicate to how we wage war. While these advancements offer numerous benefits, they also present significant challenges, particularly in the realm of terrorism. Modern terrorist organizations are leveraging new technologies to recruit, organize, fund and execute their missions more effectively than ever before (Ackerman, 2024). In this context, we can also observe the rise of autocracies (Applebaum, 2024), also in terms of barometers such as Freedom House and the Bertelsmann Transformation Index (Levitsky and Ziblatt, 2018). Also, multiple polymorphous crises like armed conflicts, a financial recession,

https://doi.org/10.2478/bjes-2025-0040 *TalTech Journal of European Studies*, 15(3(43))
Tallinn University of Technology (ISSN 2674-4619)

pandemics, climate change, the yet unknown consequences of AI and social polarization influence and design new manifestations of extremism (Bremmer, 2022).

This article adopts a qualitative, exploratory design that integrates secondary literature, selected empirical materials and elements of strategic foresight. The aim is not to produce a statistical model of terrorism, but to synthesize and interpret emerging technological trends that reshape extremist activity.

1.1 Data sources

The analysis relies on three main categories of sources. First, it draws from *scholarly and policy literature*, including peer-reviewed studies and reports on terrorism, cyberterrorism, online radicalisation and artificial intelligence published between 2017 and 2024 (e.g., Awan and Lewis, 2023; Whiting *et al.*, 2022; Weimann *et al.*, 2024). Second, *open-source empirical material*, covering publicly accessible documents and digital traces of extremist activity, including court records and case studies such as the 2019 Christchurch attack, the 2019 Halle attack and the foiled 2024 Vienna "Taylor Swift" plot. Third, *global datasets*, such as descriptive statistics and definitional frameworks from the Global Terrorism Database (University of Maryland, 2017) to contextualise historical trends.

The analysis followed four iterative steps: (1) *literature mapping*, or identification and thematic coding of key technological drivers of terrorism (e.g., algorithmic radicalisation, gamification and AI-enabled propaganda); (2) *comparative case study* involving qualitative examination of selected incidents to illustrate how these drivers manifest across ideological contexts (jihadist and far-right); (3) *strategic foresight*, that is, scenario-based reflection on possible future risks, drawing on methods of trend extrapolation and expert assessment commonly used in security studies and (4) *ethical and practical considerations* that involved using only publicly available information and no infiltration of closed extremist networks or private communication channels was attempted.

Terrorism remains a serious threat that disrupts global security and therefore presents an ongoing political challenge based on the concept outlined in *The three pillars of radicalization: needs, narratives, and networks* (Kruglanski *et al.*, 2019). Below is a concise academic explanation of each pillar, often used in radicalization research:

Needs. Radicalization often begins with unmet psychological, emotional or social needs—such as the search for belonging, identity, status or meaning. In the digital age, individuals facing marginalization, trauma or alienation may turn to online environments for validation. Extremist groups exploit these needs by offering a clear purpose, a sense of superiority and a moral mission.

Narratives. Extremist ideologies thrive through compelling narratives that simplify the world into binaries (good v. evil, us v. them) and legitimize violence. Online spaces allow these narratives to be disseminated rapidly through memes, videos, manifestos and influencers. The appeal lies not just in content, but in emotional resonance—stories of victimhood, heroism and vengeance that justify radical action.

Networks. Radicalization is rarely a solitary process. Networks—whether digital or offline—provide reinforcement, social bonding and access to radical peers and mentors. In the virtual sphere, these networks are often transnational, encrypted and emotionally charged. Social validation from these networks accelerates commitment, normalizes extremist beliefs and insulates individuals from counterarguments.

The pervasive nature of terrorist activities impacts communities across borders, influences political landscapes and raises critical questions about security, justice and freedom (Dietze and Verhoeven, 2022). Recent trends focus on virtual terrorist planning platforms, the gamification of activities and emerging online subcultures, each creating its own virtual ecosystem (Schlegel and Kowert, 2024).

Firstly, the topic fills a clear gap in the literature. While isolated studies on online radicalization (Awan and Lewis, 2023) or cyberterrorism (Whiting *et al.*, 2022) exist, few works synthesize these insights into a coherent, future-oriented analysis. The proposed article does just that—by employing strategic foresight, it not only assesses current trends (e.g., livestreamed attacks such as in Christchurch; Hartleb, 2000), meme-based propaganda, AI-facilitated radicalization (Weimann *et al.*, 2024) but also projects emerging risks such as drone-enabled violence or algorithmic extremism. This methodological framing provides value for both academics and practitioners seeking to anticipate and mitigate next-generation threats.

Secondly, the article offers interdisciplinary relevance. The article's examination of terrorism in the age of new technologies bridges security studies, political science, sociology, psychology, information technology and legal scholarship. By analyzing how digital tools facilitate radicalization,

communication and cyber operations, it speaks to computer scientists and cybersecurity experts concerned with network vulnerabilities and data protection. At the same time, its exploration of extremist narratives and online communities offers insights for sociologists and psychologists studying collective behavior and individual radicalization processes. For policymakers and legal scholars, the work highlights the need for regulatory frameworks and international cooperation to counter emerging threats. This convergence of technical, social and political perspectives underscores the article's value across multiple academic and professional fields. But there are some limitations: Research on tech-driven terrorism faces access barriers to extremist online content, encrypted communication and closed platforms (e.g., the dark web). Furthermore, data ethics and legal constraints limit observational studies. Scholars must adapt methods by developing new digital ethnographies, AI-informed pattern analysis or hybrid human-machine monitoring systems.

Without doubt, we currently find ourselves in the epicenter of a new, beginning wave of terrorism (Neumann, 2024, pp. 49–111). The previous four waves (Rapoport, 2004) have been almost seamlessly followed by a fifth (Simon, 2011). While Rapoport's typology begins the history of *modern* terrorism with the anarchistic wave of the late nineteenth and early twentieth centuries, the phenomenon of politically motivated terror is far older. Elements of what we would today call terrorism can already be found in the ancient world—in classical Greece, imperial China and republican Rome—where acts of targeted political violence were used to intimidate rulers and populations. A well-documented example is the Sicarii Zealots of the first century AD in Judea, who systematically assassinated individuals seen as collaborators with Roman rule. These ancient precedents underscore that while the *modern* era of terrorism is often dated to the nineteenth century, the practice of terror as a political tool has deep historical roots.

> *First wave: Anarchistic terrorism*. At the end of the nineteenth and the start of the twentieth century, anarchist terrorism spread across Russia and Europe, targeting monarchies and state leaders with dramatic acts of political violence. Revolutionary anarchists sought to dismantle existing power structures and inspire popular uprisings by assassinating heads of state, government officials and royalty. High-profile attacks, including the killings of monarchs and senior politicians, generated widespread fear and forced governments to tighten security and adopt new counterterrorism measures, shaping early modern approaches to political violence.

Second wave: Anti-colonial waves of violence. From the 1920s onward, anti-colonial waves of violence erupted in regions such as Indochina, Algeria and parts of South America, as nationalist movements fought to end foreign rule and gain independence. These struggles often involved guerrilla warfare, sabotage, and attacks on colonial authorities and infrastructure, reflecting both political and social grievances. The resulting conflicts hastened the decline of European colonial empires, reshaped international politics and laid the groundwork for the emergence of newly independent states in the mid-twentieth century.

Third wave: Left-wing extremist motivated terrorism. In the second half of the twentieth century, several European countries—including Italy, Germany and Spain—experienced waves of terrorism driven by left-wing extremist movements. Groups such as Italy's Red Brigades, Germany's Red Army Faction and various Marxist-inspired militants in Spain sought to challenge capitalist institutions and state authority through kidnappings, bombings and assassinations. Their campaigns, rooted in revolutionary ideology and opposition to Western political and economic systems, created significant political instability and forced governments to strengthen security and counterterrorism measures.

Fourth wave: Islamist terrorism. Since the 1979 revolution, Islamist terrorism has emerged as a violent force, reaching a particularly intense phase in the first two decades of the twenty-first century. Driven by extremist groups such as al-Qaeda and Daesh (also known as the "Islamic State"), it has shown few limits to the scale or brutality of its attacks, employing mass-casualty violence and global propaganda to advance radical ideological goals.

Fifth wave: Low-level-terrorism with new opportunities through the exploitation of virtual technologies in the USA and Europe, with different ideological inspiration or aspiration. Low-level terrorism in the USA and Europe is increasingly taking advantage of virtual technologies to create new opportunities for disruption and influence. Extremist actors—whether motivated by jihadist, far-right or other ideological currents—use encrypted messaging platforms, social media and the dark web to recruit supporters, spread propaganda and share tactics at minimal cost and with little physical risk. Online spaces enable decentralized "lone-actor" radicalization, allowing individuals to self-train through digital manuals, participate in virtual fundraising and even experiment with cyberattacks or digitally coordinated sabotage. This convergence

of varied ideological aspirations with accessible virtual tools lowers the barrier to entry for terrorism, making detection and prevention more challenging for security agencies across both regions.

Terrorism in Europe is nothing new also in terms of efforts to conceptualize it (Schmid, 2004). In the twentieth century, waves of terrorism descended on Europe again and again from the 1970s until the mid-1990s. Researchers at the University of Maryland have attempted to record and categorize global terrorist attacks since 1970. Most global databases indicate that terrorism has been on the increase worldwide ever since, however periodically not in Europe to the same extent. Methodically, terrorist attacks are included in the *Global Terrorism Database* (GTI) with one definitory precondition: A non-governmental organisation as the protagonist must intentionally exercise force against people or objects, or at least threaten to do so, to achieve political, religious or social goals (University of Maryland, 2017). But what is new is that terrorism in the age of new technologies gained totally new relevance. Who becomes a terrorist and why? (Hudson, 2018) Here, four factors play a key role:

1. *Evolving threat landscape*. Terrorism has moved beyond traditional physical attacks to include cyberattacks, digital propaganda and AI-driven disinformation in times of a growing world disorder and hybrid wars (Neumann, 2023). Terrorist actors now exploit encryption, anonymity and decentralized platforms—making detection and prevention increasingly difficult. The rise of new technologies has expanded both the means and motivations for radicalized violence.
2. *Low-tech meets high-tech*. Modern terrorism often combines simple tools (e.g., knives, vehicles) with sophisticated communication and planning infrastructures. Platforms like Telegram, cryptocurrencies, drones and livestreaming have become part of the modern terrorist toolkit—transforming small acts into globally visible events with psychological shockwaves.
3. *Global connectivity, local action*. Digital radicalization has created global extremist ecosystems, where lone actors draw ideological inspiration from attacks across continents. Cases such as Christchurch (2019) and Halle (2019) conducted via lone actors (Hartleb, 2020) illustrate how virtual spaces facilitate international imitation, making prevention a borderless challenge.
4. *AI and deepfakes as future weapons*. Emerging technologies such as artificial intelligence, deepfakes and autonomous systems (Weimann *et*

al., 2024) could be weaponized by terrorists to spread misinformation, discredit institutions or automate attacks. The potential for these tools to distort public perception and trust in democratic institutions is enormous.

2. Key dimensions of terrorism

The phenomenon of terrorism can no longer be understood solely through geopolitical, religious or ideological lenses; it must now be examined as a hybrid sociotechnical system, deeply intertwined with processes of globalization, digitalization and cultural disruption (Stockhammer, 2024). In this context, an intellectual approach requires moving beyond the reactive security paradigm and instead asking deeper questions about how technologies reshape violence, identity and power (see Table 1).

At the global level, terrorism in the digital age exhibits asymmetry not only in force, but in visibility, reach and narrative control. While liberal democracies face the challenge of protecting civil liberties, authoritarian regimes may exploit counterterrorism to justify censorship (Applebaum, 2024). Meanwhile, transnational actors use the global internet to flatten hierarchies, spread ideologies across borders and gamify terror for ideological and performative purposes. A global analytical approach must account for this multipolar and uneven terrain, where terrorism, disinformation and digital cultures intersect.

Intellectually, the field demands interdisciplinary synthesis. Political science, media theory, computational social science, philosophy and security studies must converge to understand phenomena such as memetic warfare, algorithmic radicalization and affective contagion. The study of digital terrorism cannot be separated from broader debates about truth, virtuality and democracy. Terror is a tool of politics as we have seen in many cases of separatist terrorists such in Northern Ireland; in the digital age, it is also a medium of narrative and a structure of perception (Fisher and Prucha, 2024).

Ultimately, an intellectual and global approach insists on critical imagination: the ability to theorize emergent forms of power and resistance before they fully materialize. This includes asking not only how terrorism is fought, but how it evolves, how it captures imagination and how it co-opts technologies designed for connection into tools of separation and fear. Such

a view is essential if democratic societies are to remain both resilient and self-reflective in the face of evolving threats.

Table 1. Key dimensions of terrorism in the age of new technologies. (Source: Author's elaboration.)

New dimension	Description	Challenge
AI-driven detection	Use of AI and predictive analytics to identify radical content and networks.	Privacy concerns and potential for false positives.
Platform governance	Big tech platforms now act as gatekeepers, moderating extremist content algorithmically.	Lack of transparency and risk of overreach or censorship.
Cyberterrorism	Cyberattacks on critical infrastructure are emerging as terrorism proxies.	Blurred legal definitions and jurisdictional gaps.
Digital resilience	Civic education, digital literacy and community engagement to counter online extremism.	Long-term impact hard to measure, underfunded.
Transnational lone actors	Lone actors influenced by global content across platforms, often without direct organizational ties.	Requires international intelligence cooperation and multilingual capabilities.

3. Data needs and analytical fields

To explain the scope of inquiry, the primary areas of analysis and associated data needs are detailed below.

- *Tactical innovation and weaponization of everyday tech. M*odern terrorism has evolved beyond traditional methods, with actors increasingly exploiting off-the-shelf technologies. ISIS, for example, deployed consumer drones to drop improvised explosive devices during urban warfare in Mosul. Meanwhile, right-wing extremists in the US and Europe have experimented with 3D-printed weapons to circumvent gun control laws (Hoffman and Ware, 2024). These cases show how technological accessibility lowers the threshold for operational readiness, especially for lone actors.
- *Platform migration and encrypted communication.* Encrypted messaging apps such as Telegram, Threema and Wickr have become the backbone of terrorist communication. After losing ground on open platforms like

Facebook and Twitter, groups such as ISIS shifted to Telegram, where they maintain propaganda channels and logistical coordination hubs. The challenge lies in balancing digital freedom with effective monitoring of these high-risk environments.

- *Radicalization through recommendation algorithms.* Online platforms do not just host extremist content—they sometimes help promote it. YouTube's recommendation algorithm has been criticized for funneling users from mainstream political content toward conspiracy theories and hate-based ideologies. Research has shown how simple search terms like "immigration crisis" can lead users into extremist rabbit holes, particularly on fringe platforms such as Bitchute or Odysee.
- *Terror financing via cryptocurrencies.* Cryptocurrencies have become a favored tool for terrorist financing. Hamas, for instance, publicly shared Bitcoin wallet addresses to solicit donations. Pro-ISIS networks have turned to privacy-focused cryptocurrencies like Monero, which are harder to trace than Bitcoin. The pseudo-anonymity of blockchain-based finance presents complex challenges for law enforcement and anti-terror finance regulations.
- *Gamification and visual propaganda.* The Christchurch shooter gamified his massacre, livestreaming it on Facebook and using memes and music familiar to online youth culture (Hartleb, 2020). This aesthetic of violence has since inspired others, including the Buffalo shooter in 2022, who cited prior attackers in his manifesto and streamed his own attack via Twitch. These incidents highlight how terrorism now blends ideological intent with performative spectacle, optimized for virality.
- *Cyberterrorism and information warfare.* Beyond physical violence, terrorism in the digital age includes cyberattacks and psychological operations. Pro-Russian hacking groups have launched disinformation campaigns across Europe, creating false flag narratives and sowing division on social media. In combination with fringe conspiracies, such as QAnon or anti-vaccine movements, these tactics aim to erode trust in democratic institutions—creating fertile ground for radicalization.
- *Drone-enabled terrorism.* The increasing availability of commercial unmanned aerial vehicles (UAVs) has created a new operational domain for terrorist actors. Consumer drones, which are inexpensive, easy to acquire and capable of carrying small payloads, have already been weaponized in conflict zones such as Iraq and Syria, where ISIS modified quadcopters to drop improvised explosive devices during the battle for

Mosul. Beyond direct attacks, drones can be used for reconnaissance, smuggling of weapons or explosives and live streaming of assaults to maximize psychological impact. The portability and anonymity of drone technology complicate detection and prevention, while counter-UAV measures—ranging from signal jamming to kinetic interception—raise legal and technical challenges in civilian airspace. As drone performance improves and autonomous navigation becomes more sophisticated, their potential as a tool of terrorism underscores the urgent need for integrated counter-drone strategies at national and international levels.

- *A new ecosystem of extremism*. Today's terrorism operates in a hybrid ecosystem: online and offline, centralized and decentralized, ideological and aesthetic. The boundaries between propaganda, radicalization, planning and execution have blurred. This complexity requires a new kind of response—integrating tech regulation, education, international law enforcement collaboration and ethical counter-narratives. Without such a multidimensional approach, terrorism in the age of new technology will continue to outpace reactive security frameworks.

4. The role of artificial intelligence

Terrorists increasingly exploit the entire digital value chain of terrorism. Starting from a first virtual contact with extreme positions and ideologies, over recruitment, propaganda and radicalization to the direct planning and organization of attacks—nearly everything is mandated online (Stockhammer, 2024). This phenomenon may be referenced as the *virtualization of terrorism* (Coester *et al*., 2023; Winter and Crawford, 2024). It implies that the immersion of terrorists into the sphere of cyberspace across the entire value chain (from the initial contact with extremist ideology to the planning and execution of attacks) is at the core of this terrorist manifestation. The internet and the dark net have meanwhile become a preferred space for terrorist activities. In many ways, artificial intelligence (AI) can be regarded as a game changer in that sphere, as it potentially enhances the terrorists' capabilities (Weimann *et al*., 2024). AI is in many aspects a double-edged sword (Harari, 2024). On the one hand, it is likely to enhance security measures by automating threat detection through advanced data analysis, pattern recognition and the monitoring of online spaces for radical content. AI tools can process vast amounts of data to identify potential threats in real time, making it easier for law enforcement to detect radicalization early

or trace suspicious communications on encrypted platforms. For example, AI algorithms can help flag extremist content on social media, analyze behavioral patterns indicative of radicalization and even simulate attack scenarios to improve response strategies (Harari, 2024).

On the other hand, terrorists themselves are beginning to exploit AI for their own purposes, such as creating deepfakes to disseminate propaganda, bypassing traditional surveillance with advanced encryption algorithms and potentially even using autonomous systems such as drones in attacks. The accessibility of AI-driven technologies like chatbots and language models such as ChatGPT could enable extremist groups to automate recruitment, spread misinformation or even direct terrorist attacks through virtual means, further complicating the threat landscape (Weimann *et al*., 2024).

The potential use of AI by terrorist groups has been identified as a disruption and emerged as a significant concern in the global terrorist threat landscape. As AI technologies become more accessible and sophisticated, terrorist organizations such as al-Qaeda, the IS and Hezbollah are increasingly exploring ways to leverage these tools for their nefarious purposes. The lowered barriers to entry in terms of cost, training and technical skills required have made AI more attainable for these groups, potentially amplifying their capabilities and reach. Terrorists are primarily exploiting AI in three key areas: propaganda and information operations, enhancing recruitment efforts and facilitating financing activities. In the realm of propaganda, AI is being used to generate, translate and disseminate content more efficiently. For instance, the IS has experimented with AI-generated news bulletins (Verma, 2024), while pro-al-Qaeda outlets have created propaganda images likely using AI tools. Far-right groups have also produced guides on using AI for creating extremist memes, demonstrating the technology's appeal across various ideological spectrums. The potential for AI to accelerate and enhance radicalization processes is particularly alarming. AI-powered chatbots can engage potential recruits in personalized interactions, potentially making the recruitment process more effective and harder to detect. Moreover, the immersive environments created by AI, such as those in the metaverse, could serve as powerful tools for terrorist training and indoctrination. Artificial intelligence may be misused to support operational and organizational planning of future attacks (Weimann *et al*., 2024). This could be mandated by quickly providing targeting and logistic information as well as something akin to terrorist project management.

Specific examples of terrorist use of AI have already been observed. The "Islamic State" has published guides on how to securely use generative AI tools, while various extremist groups are using AI for translating propaganda into multiple languages, significantly expanding their reach. These developments highlight the adaptability of terrorist organizations in embracing new technologies. While a comprehensive adoption of AI by terrorists is not guaranteed and depends on various factors, these groups' ability to adapt to and exploit new technologies should not be underestimated. Countering this emerging threat requires a collaborative effort between policymakers, law enforcement agencies, tech companies and civil society. Strategies need to be developed to monitor and contain AI-enhanced terrorist operations effectively. Interestingly, AI also presents opportunities for counter-terrorism efforts. There is potential to use AI for developing personalized counter-messaging to combat terrorist narratives and for enhancing intelligence gathering and analysis capabilities. As AI technology continues to evolve rapidly, the challenge of preventing its misuse by terrorist groups while harnessing its potential for counter-terrorism efforts remains a critical concern for global security. The dynamic nature of this threat necessitates ongoing research, policy development and international cooperation to stay ahead of terrorist innovations in the AI space (Weimann *et al*., 2024).

Not only on a motivational level but also in terms of capabilities, virtualization describes the capabilities and the ability to conduct (cyber) operations along the jihadist "value chain", ranging from providing propaganda platforms to preparing attacks. Capability and deeply rooted motivation go hand in hand, as extremists use the diverse opportunities offered by cyberspace for their activities in every conceivable way. Anonymity and clandestine operations favor organizations and lone actors who take advantage of sub-conventional, asymmetric tactics, and vice versa. If these jihadist followers manage to escape or bypass the countermeasures of counterterrorism investigators, they may create a virtual hub that allows them to quickly adapt and use it as a weapon. Fundamentally, the toxic combination of strong motivation and existing capabilities poses a constant threat to security. Unfortunately, the likelihood of establishing such a hub is considered relatively high.

5. Dynamic TikTok radicalization

TikTok has become a major platform where radicalization of adolescents takes place. Its customized content targeting youth suggests that extremists may be taking over and exploit this platform for their purposes. It already happens along the spectrum of extremisms. TikTok is used by far-right extremists to promote xenophobic attitudes, manifesting as racism and strong opposition to immigration. Religious intolerance is expressed through anti-Semitism and anti-Muslim prejudice, while gender-based discrimination is characterized by anti-feminist views and hostility towards LGBTQ rights and identities.

Islamist hate preachers and influencers are currently using the Middle East conflict and the war in Gaza in particular as a pretext and opportunity to convince young people of their extremist ideology. German constitutional protectors are alarmed: the instrumentalization of TikTok by Islamists in Germany has developed into a "fire accelerator" for youth radicalization (*Die Zeit*, 2024). TikTok is currently providing masses of propagandistically staged videos from Gaza. These include not only misinformation and propaganda, but also Salafist content, some of whom achieve enormous outreach. They deliberately spread victim and revenge narratives that are designed to incite young people. Another recurring aspect is the dichotomous division into *halal* or *haram*, a theologically dressed-up division of the world into "good" and "evil", which runs like a common thread through the messages of influencer preachers and is essentially designed to demand a Sharia-compliant life from young people in contrast to non-Muslim society, which can hardly be reconciled with the requirements and principles of the liberal constitutional state (Guhl and Comerford, 2021).

Moreover, the video-streaming app TikTok is increasingly deployed by political actors to reach younger voters. TikTok grants social media users the opportunity to create and share short videos of between 3 and 60 seconds with added music and audiovisual effects. In the past years, extremists of all ideological backgrounds have continued to exploit this platform as a space for propaganda to foster radicalization among adolescents. In early August 2024, the arrest of two teenagers, aged 18 and 19, in Austria, who had pledged allegiance to the Islamic State (IS) and likely plotted a terror attack at a Taylor Swift concert in Vienna, has underscored a growing concern: the recruitment of young individuals into Islamist and far-right terrorist groups through social media, especially TikTok (Hartleb and Stockhammer, 2024).

Intelligence experts highlight TikTok's role as a major recruiting platform for young lone attackers and virtual terror cells, owing to its extensive reach and algorithmic influence. Telegram, on the other hand, is often used for planning and coordinating attacks. Such a shift in recruitment strategies poses significant challenges for law enforcement. Monitoring online interactions and identifying virtual meeting places is far more complex than tracking face-to-face meetings between recruiters and recruits.

6. Emergence of teenage terrorism

In this context, teenager terrorism (Bloom and Horgan, 2019) is an alarming trend where young people, often influenced by online propaganda, radical ideologies or feelings of disenfranchisement, become involved in acts of terrorism or extremist violence (Hartleb, 2025). This phenomenon has been increasingly visible in both jihadist extremism and far-right extremism, with teenagers being targeted for recruitment due to their vulnerability, access to social media and often unstable social environments. Social media platforms and encrypted messaging apps have become central in the radicalization of teenagers. Extremist groups such as ISIS and far-right organizations exploit these platforms to spread propaganda and recruit young followers (Ebner, 2017). Teenagers, spending large amounts of time online, are particularly vulnerable to such content. The anonymity of the internet allows easy dissemination of radical ideas, often without parental or institutional oversight. Adolescents can be drawn into echo chambers or gaming communities that mask extremist narratives behind popular culture references.

Adolescence is a period of identity formation, and young people who feel alienated or disconnected from their community may be drawn to extremist ideologies that offer a sense of purpose, belonging or adventure. This is especially true for youth facing social marginalization, economic hardships or discrimination (Bloom and Horgan, 2019). Many teenage recruits to jihadist or far-right movements report feeling disenfranchised by their environments or suffering from mental health issues, which extremists exploit by providing them with a cause or sense of empowerment. Social and economic factors such as poverty, lack of opportunities and exclusion from mainstream society can push teenagers towards radicalization. In communities where young people see few positive role models or pathways to

success, extremist groups may appear as attractive alternatives, promising status and meaning. This is particularly true among migrant communities or neighborhoods where cultural or religious tensions create a sense of being "outsiders", which groups like the IS have skillfully exploited by appealing to both global religious narratives and personal grievances.

In many cases, teenagers are influenced by peer networks, where friends or older figures introduce them to extremist ideologies. The concept of group solidarity, where friends radicalize together, has been seen in both jihadist cells and far-right youth groups. In some cases, radicalized teenagers attempt to recruit others within their peer groups, creating a cycle of extremism within schools or youth communities.

The various forms of teenager involvement in terrorism can be analyzed from the perspective of the interrelations outlined in (Ebner, 2017):

- Jihadist extremism:
  - The IS had success recruiting teenagers from Western countries to either join their ranks in the Middle East or carry out attacks in their home countries. Many of these recruits were drawn in through slick online propaganda videos, forums and personal messaging campaigns.
  - Notable examples include teenagers from France, Belgium and the UK, some of whom traveled to Syria and Iraq to join ISIS, while others carried out lone-wolf attacks in their own countries.
  - The case of Shamima Begum, a British teenager who left to join ISIS in 2015, is one of the most widely publicized instances of teenage involvement in jihadist extremism.

- Far-right extremism:
  - There has been a rise in teenage involvement in far-right extremism in Europe and the US, often linked to white supremacist or neo-Nazi ideologies. Far-right extremists target young people by framing their rhetoric in the context of anti-immigration, anti-government views and identity politics.
  - An example is the increasing presence of teenagers in online forums promoting ideologies like the "Great Replacement" theory, which claims that white populations are being replaced by non-white immigrants, leading to violence such as the Christchurch attack (though the perpetrator was not a teenager, his manifesto inspired many younger individuals).

The changing threat has been catalyzed by arguably the two most significant trends in terrorism over the past two decades: the emergence of people acting alone who have been inspired by the ideology of terrorists and the ease of online radicalization. Both trends encourage the increased involvement of young people in extremism: When radicalization occurs in the living room (as with Anders Behring Breivik as a role model, see Hartleb, 2020), barriers to entry are lowered, allowing even teenagers to take active part.

Teenagers across the ideological spectrum have engaged as online innovators and influencers, and violent offline activists.

> Independently of adults, children have succeeded in producing terrorist propaganda, influencing their peers and adults towards violence, and preparing to engage in terroristic violence both domestically and abroad. The current data suggest that terrorists in Europe may become younger. In terms of radicalization, we observe 13–17 years old adolescents that develop firm intentions to commit terrorist attacks. The emergence is deeply linked with the rise of virtual platforms which can be regarded a disruption. In the field of jihadism, we can observe the so called *TikTok-Jihad*. (Kaltenbrunner and Neuhold, 2025)

TikTok has become the fastest growing application in the world, largely thanks to its popularity among "kids and teenagers". The tools are used in both dimensions: to recruit and radicalize. In this case, the "gamification thesis of terrorism" has a certain legitimacy due to the impact of memes and symbols (Kaltenbrunner and Neuhold, 2025). Also with the right-wing terrorism, teenager terrorism plays an increasing role, in groups such as *Atomwaffen- or Feuerkriegsdivision* (the Estonian commander was 13 years old!; Hartleb, 2025) or in terms of lone actors. Children are not merely passive consumers of content created and shared by adult counterparts but ideologically driven in the light of radicalization processes and networks sui generis. In the case of youth vulnerabilities to radicalization, online social media has been argued as playing an important role. Research does indicate young extremists are more likely to engage with social media and other virtual platforms compared with adults who are charged for terrorism. And terrorists such as the abovementioned Breivik are regarded as heroes and role models.

For the Islamist spectrum, the recent jihadist Taylor Swift plot in Vienna in summer 2024 is significant concerning the young age of the already known network. The suspects are 19, 18, 17 and possibly 15 years old (Hartleb and

Stockhammer, 2024). This confirms the current trend across Europe that (attempted) terrorists are getting "younger" all the time, which is obviously due to increasing online radicalization and the heightened appeal of this age group. In this specific case, it seems to be confirmed that Salafist hate/influencer preachers not only specifically address young people via channels such as YouTube and TikTok but can also influence on their radicalization with their dichotomous messages. Terrorist organizations such as the IS convey clear ideological guidelines to young, radicalized people in closed networks (such as Telegram) and inspire a virtual community, which in turn is more likely to be willing to commit acts of terrorist violence, as the inhibition threshold for manifest violence is usually lower among those radicalized in this way (Hartleb, 2025).

In conclusion, the increasing participation of teenagers in terrorist activities is a multifaceted issue that requires a comprehensive and empathetic response. By understanding the pathways to radicalization and implementing targeted prevention and intervention strategies, society can work towards mitigating this alarming trend and safeguarding its youth (Görzig, 2024).

7. Conclusion

Terrorism in the age of new technologies is no longer defined solely by violence in physical space—it now thrives in the psychological, digital and symbolic domains. As the battlefield shifts from geography to information, the role of perception, emotion and symbolic power becomes central. Terrorism today is often designed to be viral rather than tactical, targeting attention economies as much as physical infrastructure. Livestreamed attacks, meme-based propaganda and aestheticized violence are crafted not only to intimidate but to recruit, polarize and erode public trust. Extremist actors exploit the tools of our interconnected world—social media, encrypted apps, AI and digital aesthetics—to radicalize, coordinate and perform acts of terror with unprecedented speed and reach. This transformation demands a paradigm shift in how we understand, anticipate and counter terrorism.

Rather than responding only with kinetic force or reactive policy, modern counterterrorism must embrace anticipatory, interdisciplinary and democratic approaches. Strategic foresight, digital literacy, civic resilience and ethical technology governance must become core elements of our defense architecture. Tech companies, educators, citizens and governments must be treated not as separate actors but as a shared ecosystem of responsibility.

Ultimately, the challenge lies not only in countering extremist violence, but in preserving the resilience, integrity and values of open societies under digital siege. The digital age has empowered new threats—but it also offers new tools for intelligence, prevention and global collaboration. The decisive question is whether democratic societies can learn fast enough—and act wisely enough—to defend freedom without surrendering its essence.

From an intellectual standpoint, the digital evolution of terrorism forces a re-examination of foundational concepts such as violence, radicalization and power. Violence is no longer always physical—it can be symbolic, algorithmic or aesthetic. Radicalization may occur without human recruiters, instead shaped by ambient culture, algorithmic exposure or peer validation in gamified spaces. And power, once held by states or hierarchical groups, is increasingly distributed across decentralized networks, viral content flows and emotionally charged micro-communities. To analyze this, scholars must move beyond static typologies and adopt flexible, transdisciplinary frameworks that account for hybrid threats, affective mobilization and socio-technical entanglements.

Practically, this reconceptualization must inform the design of countermeasures that are as agile and adaptive as the threats they seek to prevent. Governments must foster digital resilience not only through legislation and law enforcement, but by investing in civic infrastructure—media literacy education, public-interest tech design and community-based early warning systems. Collaboration between the public and private sectors is no longer optional; it is structural. Furthermore, the ethics of counterterrorism must remain central. In defending democracy from technologically mediated extremism, we must be vigilant not to erode the very rights, pluralism and trust that define democratic life. The digital age demands not only stronger defense, but smarter, more principled engagement with the evolving landscape of ideological violence.

In a nutshell, the future of terrorism will likely be marked by increased technological sophistication, ideological diversification and heightened geopolitical instability. Extremists are expected to continue exploiting societal divisions, technological advances and global conflicts to further their agendas, necessitating that governments and international organizations remain vigilant and adaptable in their counterterrorism efforts.

Future research must further explore how evolving technologies like generative AI, immersive environments and decentralized platforms may

enable new forms of radicalization and disruption. Understanding not only what terrorists do but how they frame, aestheticize and disseminate violence is essential for developing nuanced counter-narratives and strategic foresight. This requires collaboration not just between states, but across disciplines and sectors, creating a multi-nodal defense of democratic values.

As we move deeper into the twenty-first century, it is clear that counterterrorism cannot be confined to borders, institutions or traditional military paradigms. The fight against tech-enabled extremism will be won not solely in intelligence rooms or courtrooms, but in classrooms, codebases and content ecosystems. The path forward is one of intelligent vigilance, moral clarity and strategic imagination—tools as essential as any firewall or forensic toolkit.

Dr. phil **Florian Hartleb**, has been, since September 2025, an associate professor for international relations at Modul University Vienna. He has studied political science, law and psychology at Eastern Illinois University and the University of Passau. In 2004, he defended a dissertation on right- and left-wing populism at the University for Technology Chemnitz (summa cum laude; in German). He has been a lecturer at the University of Passau, the Catholic University of Eichstätt, the University for Police Saxony-Anhalt and official investigator for the City of Munich in the case of the Munich attacks on July 22, 2016. Hartleb's latest book publications include *Lone wolves. The new terrorism of right-wing actors* (Springer Nature, 2020). He has served as the guest editor for the *Special issue: Extremismen im Vergleich* of *Journal for Intelligence, Propaganda and Security Studies*, 1(2024); and published *Teenager Terroristen. Wie unsere Kinder radikalisiert werden—und wie wir sie schützen können* (Hoffmann & Campe, 2025).

References

Ackerman, G.A. (2024) 'The emerging terrorist technological landscape', in N. Stockhammer (ed) *Routledge handbook of transnational terrorism*. London and New York: Routledge, pp. 97–106. Available at: https://doi.org/10.4324/9781003326373-11

Applebaum, A. (2024) *Autocracy, Inc.: the dictators who want to run the world*. New York: Penguin Random House.

Awan, A.N. and Lewis, J.R. (eds) (2023) *Radicalisation: a global and comparative perspective*. London: Hurst & Company.

Bloom, M. and Horgan, J. (2019) *Small arms: children and terrorism*. Ithaca and London: Cornell University Press. Available at: https://doi.org/10.7591/cornell/9780801453885.001.0001

Bremmer, I. (2022) *The power of crisis: how three threats—and our response—will change the world*. New York: Simon & Schuster.

Coester, M., Daun, A., Hartleb, F., Kopke, C. and Leuschner, V. (eds) (2023) *Rechter Terrorismus: international—digital—analog*. Wiesbaden: Springer. Available at: https://doi.org/10.1007/978-3-658-40396-6

Dietze, C. and Verhoeven, C. (eds) (2022) *The Oxford handbook of the history of terrorism*. Oxford: Oxford University Press.

Die Zeit (2024) 'Verfassungsschutz warnt vor "Tiktokisierung des Islamismus"', 21 April. Available at: https://www.zeit.de/gesellschaft/zeitgeschehen/2024-04/tiktok-islamismus-salafisten-jugend-radikalisierung (Accessed: 5 October 2025).

Ebner, J. (2017) *The rage: the vicious circle of Islamist and far-right extremism*. London: I.B. Tauris & Co. Available at: https://doi.org/10.5040/9781350989184

Fisher, A. and Prucha, N. (2024) 'Online territories of terror: the multiplatform communication paradigm and the information ecology of the Web3 era', in N. Stockhammer (ed) *Routledge handbook of transnational terrorism*. London and New York: Routledge, pp. 107–123. Available at: https://doi.org/10.4324/9781003326373-12

Görzig, C. (2024) 'Generation Z and terrorism', in N. Stockhammer (ed) *Routledge handbook of transnational terrorism*. London and New York: Routledge, pp. 183–191. Available at: https://doi.org/10.4324/9781003326373-21

Guhl, J. and Comerford, M. (2021) *Understanding the Salafi online ecosystem: a digital snapshot*. London: Institute for Strategic Dialogue. Available at: https://www.isdglobal.org/wp-content/uploads/2021/11/Snapshot-study.pdf (Accessed: 5 October 2025).

Harari, Y.N. (2024) *Nexus: a brief history of information networks from the Stone Age to AI*. London: Penguin Random House.

Hartleb, F. (2020) *Lone wolves: the new terrorism of right-wing single actors*. Cham: Springer. Available at: https://doi.org/10.1007/978-3-030-36153-2

Hartleb, F. (2025) *Teenager Terroristen: wie unsere Kinder radikalisiert werden—und wie wir sie schützen können*. Hamburg: Hoffmann & Campe.

Hartleb, F. and Stockhammer, N. (2024) *'I would have planted the explosives in the crowd': an analysis of the foiled terrorist attack on the mass event 'Taylor Swift concert' in Vienna in August 2024*. Vienna: European Institute for Counter Terrorism and Conflict Prevention (EICTP). Available at: https://eictp.eu/wp-content/uploads/2024/09/FINAL_SWIFT_ViennaENG.pdf (Accessed: 5 October 2025).

Hoffman, B. and Ware, J. (2024) *God, guns, and sedition: far-right terrorism in America*. New York: Columbia University Press. Available at: https://doi.org/10.7312/hoff21122

Hudson, R.A. (2018) *Who becomes a terrorist and why? The psychology and sociology of terrorism*. New York: Skyhorse Publishing.

Kaltenbrunner, S. and Neuhold, C. (2025) *Allahs mächtige Influencer: wie Tik-Tok-Islamisten unsere Jugend radikalisieren*. Wien: edition a.

Kruglanski, A.W., Bélanger, J.J. and Gunaratna, R. (2019) *The three pillars of radicalization: needs, narratives, and networks*. Oxford: Oxford University Press. Available at: https://doi.org/10.1093/oso/9780190851125.001.0001

Levitsky, S. and Ziblatt, D. (2018) *How democracies die*. New York: Crown Publishers.

Neumann, P.R. (2023) *The new world disorder: how the West is destroying itself*. London: Skribe UK.

Neumann, P.R. (2024) *Die Rückkehr des Terrors: wie uns der Dschihadismus herausfordert*. Berlin: Rowohlt.

Rapoport, D.C. (2004) 'The four waves of modern terrorism', in A.K. Cronin and J.M. Ludes (eds) *Attacking terrorism: elements of a grand strategy*. Washington, DC: Georgetown University Press, pp. 46–73.

Schlegel, L. and Kowert, R. (2024) *Gaming and extremism: the radicalization of digital playgrounds*. New York: Routledge. Available at: https://doi.org/10.4324/9781003388371

Schmid, A.P. (2004) 'Frameworks for conceptualising terrorism', *Terrorism and Political Violence*, 16(2), pp. 197–221. Available at: https://doi.org/10.1080/09546550490483134

Simon, J.D. (2011) 'Technological and lone operator terrorism: prospects for a Fifth Wave of global terrorism', in J.E. Rosenfeld (ed) *Terrorism, identity, and legitimacy: the four waves theory and political violence*. London and New York: Routledge, pp. 44–65.

Stockhammer, N. (ed) (2024) *Routledge handbook of transnational terrorism*. London and New York: Routledge. https://doi.org/10.4324/9781003326373

University of Maryland (2017) *Global Terrorism Index 2017*. Institute for Economics & Peace. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf (Accessed: 5 October 2025).

Verma, P. (2024) 'These ISIS news anchors are AI fakes. Their propaganda is real', *The Washington Post*, 17 May. Available at: https://www.washingtonpost.com/technology/2024/05/17/ai-isis-propaganda (Accessed: 5 October 2025).

Weimann, G., Pack, A.T., Sulciner, R., Scheinin, J., Rapaport, G. and Diaz, D. (2024) 'Generating terror: the risks of generative AI exploitation', *CTC Sentinel*, 17(1), pp. 17–25. Available at: https://ctc.westpoint.edu/wp-content/uploads/2024/01/CTC-SENTINEL-012024.pdf (Accessed: 5 October 2025).

Whiting, A., MacDonald, S. and Jarvis, L. (2022) 'Cyberterrorism: understandings, debates, and representations', in C. Dietze and C. Verhoeven (eds) *The Oxford handbook of the history of terrorism*. Oxford: Oxford University Press, pp. 673–690.

Winter, C. and Crawford, B. (2024) 'The virtualization of terror: violent extremism on the internet today', in N. Stockhammer (ed) *Routledge handbook of transnational terrorism*. London and New York: Routledge, pp. 124–131. Available at: https://doi.org/10.4324/9781003326373-13