TECH-SAVVY TERRORISM:

THE EVOLUTION OF VIOLENT EXTREMISM IN A DIGITAL AGE

AUTHOR

Colin P Clarke
Director of Research,
The Soufan Group

CHACR

The Centre for Historical Analysis and Conflict Research is the British Army's think tank and tasked with enhancing the conceptual component of its fighting power. The views expressed in this *In Depth Briefing* are those of the author, and not of the CHACR, Royal Military Academy Sandhurst, Ministry of Defence or the British Army. The aim of the briefing is to provide a neutral platform for external researchers and experts to offer their views on critical issues.

IN 2023, it would be nearly impossible to imagine a terrorist or extremist group without a significant online presence. Terrorists' adoption and use of emerging technologies often mimic broader trends in society, and in some cases, occur much earlier, driven by the need to adapt and evolve. The internet poses some vulnerabilities to extremist groups, but also myriad opportunities. This research brief will examine how terrorists and violent extremists use the internet, how this has changed over time, what makes their use of the internet so effective and, finally, what can be done to counter it.

EVOLUTION OVER TIME

How terrorists and violent extremists operate virtually continues to evolve, especially as new technologies afford nefarious actors more opportunities to radicalise, recruit, and raise funds. The online extremist landscape has progressed exponentially since the days when the Zapatista National Liberation Army (EZLN), or "Zapatistas," used the internet in the 1990s to disseminate information. Around this same time, white supremacists were using static websites and message boards to spread propaganda. Without the risk of hyperbole, it is accurate to say that the internet today is not simply part of the spectrum of terrorist activity, but one of the most critical elements of how they operate. Operating online, terrorists can recruit, but also plan attacks, communicating with operatives and directing violence from afar. The internet has lowered the barrier to entry for anyone wishing to engage with other extremists online, making the threat of radicalisation more ubiquitous. A report by the UK Intelligence and Security Committee, released just last month, discussed the threat of "self-initiated terrorists" who "are now radicalised and can radicalise others, online from the seclusion of their bedrooms."

Over time, non-state actors have proven highly adaptive in the virtual space, able to rebound from counter-terrorism actions while staying several steps ahead of law enforcement authorities and intelligence agencies. In a world where extremists connect online, physical geography and proximity are less determinative, though it is crucial not to downplay the importance of real-world interactions, as radicalisation is rarely a result of solely online behaviours. A report by the RAND Corporation identified five primary categories of internet-enabled functions

carried out by terrorist and extremist groups, including: financing; networking and coordination; recruitment and radicalisation; inter- and intra-group knowledge transfer; and mobilisation to action. The internet has augmented recruitment and radicalisation through the creation and dissemination of propaganda, the ability to broadcast messages to global audiences in real-time, and direct, secure communication with potential recruits.

The online component of terrorism and violent extremism also provides a global platform to charismatic ideologues that craft and distribute propaganda, recruit new members, and radicalise would-be supporters, often encouraging acts of violence. Anwar al-Awlaki, the American-born jihadist and chief propagandist of al-Qaeda in the Arabian Peninsula, was particularly effective at instigating terrorist attacks. Before being killed by a U.S. drone strike in Yemen in 2011, al-Awlaki was perhaps the most significant propagator of jihadist ideology and his influence extended well beyond his death, with his sermons readily available online. According to research by Alexander Meleagrou-Hitchens, a lecturer in terrorism and radicalisation at the War Studies department at King's College London, al-Awlaki inspired or was linked to 66 of 212 total cases of individuals charged with jihadist-related offenses in the United States. Over an eight-year period between 2007 and 2015, Awlaki either influenced, or was in direct contact with, 63 of 259 individuals linked to terrorist plots or attacks. Al-Awlaki was wildly popular with UK jihadists as well, one of the few jihadists to bridge the divide between al-Qaeda and Islamic State supporters. Other jihadists followed in al-Awlaki's footsteps, leveraging online communications to further the objectives of groups like the Islamic State. Another tech-savvy jihadist, a hacker named Junaid Hussain (Abu Hussain al-Britani), was a British foreign fighter and Islamic State operative who actively recruited ISIS sympathisers and sought to instigate terrorist attacks against Western targets, including attacks in the United Kingdom. Removing al-Awlaki and Hussain from the battlefield was a necessary step to counter the recruitment of terrorist operatives and mitigate the resonance of their respective online activities.

"TERRORIST AND EXTREMIST GROUPS RELY ON THE INTERNET FOR THE DIFFUSION OF TRADECRAFT, TAKING ADVANTAGE OF 'DO-IT-YOURSELF' CHATROOMS TO IMPROVE TECHNICAL KNOW-HOW RELATED TO ARTIFICIAL INTELLIGENCE, 3-D PRINTING, AND UNMANNED AERIAL SYSTEMS, OR DRONES."

Beyond serving as a force multiplier for radicalisation, the internet will continue to be exploited by terrorists in myriad ways in the future. Terrorists and violent extremists continue to seek to exploit the internet to finance their activities and organisations. Cryptocurrencies have captured the attention of groups like the Islamic State and Hamas, while far-right extremists have also dabbled in myriad crowdsourcing platforms to raise money. The Islamic State's "virtual planner" model highlights the importance of the internet for networking and coordination within and among terrorist networks. This innovation – outsourcing terrorism to radicalised individuals via the internet – has been a "game changer" for ISIS-enabled attacks against the West. Enabled by end-to-end encryption, this approach revolutionised attack planning for jihadist organisations. The internet has also been a force multiplier for recruitment and radicalisation. Terrorist and extremist groups also rely on the internet for the diffusion of tradecraft, taking advantage of "do-it-yourself" chatrooms to improve technical know-how related to artificial intelligence, 3-D printing, and unmanned aerial systems, or drones. Moreover, there is a mobilisation to action or incitement aspect, wherein jihadists, far-right accelerationists, and others actively call for their followers to engage in real-world acts of violence and terrorism.

Terrorists continue to find new and innovative ways to leverage the internet because it remains an effective tool for radicalisation. Online echo chambers reinforce pernicious narratives, perpetuate violent conspiracy theories, and spread mis-, dis-, and malinformation, uninhibited by moderate positions. Online interactions reinforce an 'us versus them' in-group/out-group dynamic that rewards those who adopt the most extreme positions. Online forums serve as incubators of extremist rhetoric, while malicious algorithms prioritise extremist content, in some cases contributing to an accelerated radicalisation process. The proliferation of online manifestos, particularly among far-right attackers, is a new twist to an old tactic, supplanting the jihadis' martyrdom tapes, used to both inspire future attacks but also to sow fear and terror among civilian populations. These manifestos live forever online and are aimed not just at radicalising would-be supporters but also as an eternal repository to learn

and refine tradecraft, weapons maintenance, and other tactics, techniques, and procedures.

WHAT MAKES TERRORISTS' USE OF THE INTERNET EFFECTIVE?

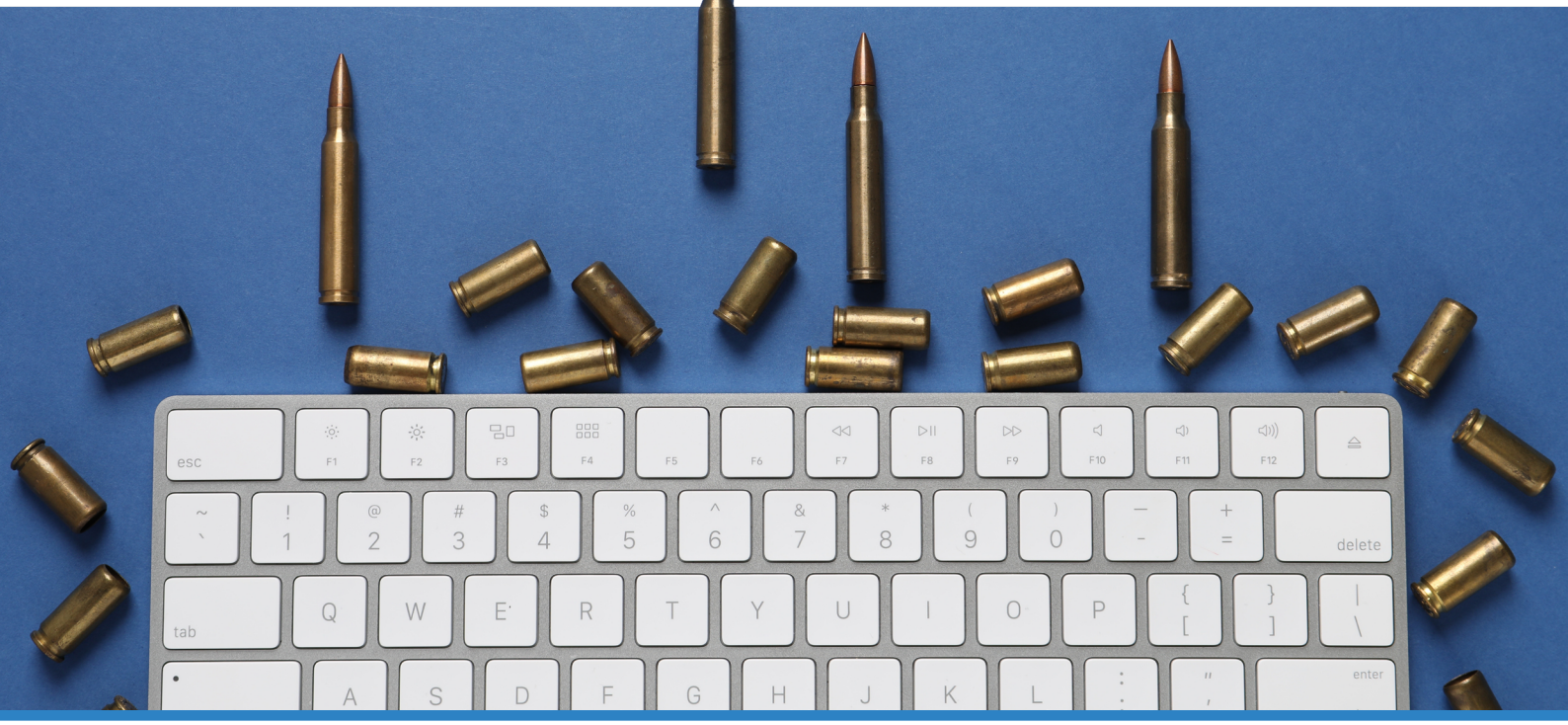
The internet is an effective incubator of radicalisation and violent extremism, producing echo chambers wherein virtual social networks serve as a shield for radicalised individuals, denying them an opportunity to encounter contrary descriptions of reality and, in turn, leading them to adopt more extreme views while eschewing positions that may be considered more moderate. There is also an aspect of deindividuation, wherein individuals may begin to align their behaviours with a group or organisation, and therefore offload responsibility for their actions. Moreover, algorithms like YouTube's content recommendation system push divisive and vitriolic content. Algorithmic radicalisation is not unique to YouTube and has been an issue for Facebook, TikTok, and other social media platforms. TikTok's recommendation algorithm has promoted QAnon conspiracy theories and content from a bevy of far-right extremist groups, including militias such as the Oath Keepers and Three Percenters.

"THE INTERNET IS ABLE TO BRING TOGETHER LIKE-MINDED INDIVIDUALS FROM ALL OVER THE WORLD IN ENCRYPTED FORUMS AND COMMUNICATION CHANNELS. ACCORDINGLY, THOSE WHO MAY HAVE BEEN UNAWARE OF ONE ANOTHER, OR RETICENT TO PURSUE OPPORTUNITIES IN THE REAL WORLD, ARE ABLE TO INTERACT, CONNECT, PLOT, PLAN, AND PROSELYTISE."

The internet is the great equaliser in terms of obviating the importance of geography. While face-to-face interactions are still incredibly valuable for radicalisation, the internet is able to bring together like-minded individuals from all over the world in encrypted forums and communication channels. Accordingly, those who may have been unaware of one another, or reticent to pursue opportunities in the real world, are able to interact, connect, plot, plan, and proselytise. With internet access and an abundance of extremist material, the cases of self-radicalisation have grown exponentially. Some scholars have suggested that this is one of the most important drivers of a shift to "post-organisational violent extremism and terrorism". The internet is also the key ingredient in the acceleration of radicalisation. As Molman and Ravndal have noted, individuals can move through multiple phases online, from the pre-radicalisation phase to "action triggering," which is the moment that created an impetus to commit acts of political violence or terrorism. Multiple factors influence this trajectory, as well as how long the process can take to reach fruition. According to a study by Michael Jensen of the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland, the average time span of radicalisation in the United States has shrunk from 18 months to seven months. In the United Kingdom, this challenge is compounded by the increasingly young age of individuals flagged for extremism, with many young men under the age of 24 now on the radar of the security services, particularly those inspired by extreme right-wing terrorism.

The internet has also functioned as a crossroads for violent extremists of different stripes to interact with one another, both directly and indirectly. The result has been severalfold. First, there has been a noticeable trend of far-right extremists emulating jihadists' tactics, techniques, and procedures. Second, there has been an erosion of neatly defined categories, giving way to what Bruce Hoffman has called ideological convergence, or what has become more commonly referred to as 'salad bar' terrorism, meaning that terrorists have viewed violent extremists ideologies as something akin to a buffet, deciding which aspects to adopt and which to jettison, regardless of precedent. As Daveed Gartenstein-Ross has astutely observed, "the lack of ability to disaggregate individuals who fit the salad bar extremism concept presents difficulties for analytic, prevention, and detection efforts".

Still, it should be noted that operating almost wholly online has obvious disadvantages. The



more dispersed and decentralised networks become, the more difficult it becomes to generate the critical mass needed for sustained terrorist attacks and operations. The absence of safe haven, sanctuary, or other control of territory is also important, imposing strict limitations on tacit knowledge transfer, rapport building, and in-person training. While The Base, Atomwaffen Division, and other far-right neo-Nazi groups remain a stubborn challenge, they have failed to develop into a threat on par with al-Qaeda or the Islamic State.

CHALLENGES COUNTERING EXTREMISM ONLINE

Disrupting terrorist and extremist networks online has proven challenging. Silicon Valley and social media companies have taken important actions with respect to content moderation, however begrudgingly. But de-platforming has been far from the silver bullet some had hoped for, as extremists migrated from mainstream tech platforms like Facebook and Twitter to more fringe sites, including 4chan, 8chan, Gab, and Telegram, to name just a few. Service providers regularly impose bans and restrictions following high-profile terrorist attacks, but extremists adapt easily, migrating to new platforms and harnessing new tools to continue operating online. Some tech companies have only engaged in more aggressive content moderation under duress, pressured by public backlash and media scrutiny. Yet even when extremists are purged en masse from sites like Twitter or Facebook, they can all too easily continue operating on fringe sites or alt-tech platforms like Gab, Parler, 4Chan, 8Chan, or Reddit.

Since terrorists are accustomed to operating in hostile environments, using emerging technologies in new and innovative ways is crucial to maintaining an advantage.

"SERVICE PROVIDERS REGULARLY IMPOSE BANS AND RESTRICTIONS FOLLOWING HIGH-PROFILE TERRORIST ATTACKS, BUT EXTREMISTS ADAPT EASILY, MIGRATING TO NEW PLATFORMS AND HARNESSING NEW TOOLS TO CONTINUE OPERATING ONLINE."

Competitive adaptation, the ability to stay several steps ahead of counter-terrorism and security forces, can be the difference between a group surviving and thriving or being destroyed. Violent extremists are also allocating more resources to operating in the online space, demonstrated by the Islamic State's recruitment of individuals with backgrounds and expertise in videography, production, and editing. The aesthetics and improved quality of terrorist propaganda are noticeable.

As terrorism expert Maura Conway has observed, much more needs to be done to improve the study of terrorists' online activity, particularly the radicalisation aspect. This includes paying more attention to the role of gender in violent online extremism, but also widening the aperture beyond jihadists, looking at accelerationism, the broader far-right, and the panoply of ideologies currently motivating violence and extremism. As Tech Against Terrorism has convincingly argued, there is also a need for more research on the second and third-order effects of deplatforming terrorists and terrorist content.

CONCLUSION

Tailored counternarratives and strategic communications campaigns aimed at preventing and countering violent extremism have been inconsistent at best, and amateurish at worst, leading many to be pessimistic about future efforts in this space. With the advent of the Metaverse and other emerging technologies and platforms, it will be crucial to enlist the private sector in countering terrorism and extremism online, working to forge effective public-private partnerships that can operationalise well-intended but vague and under-resourced policy prescriptions like enacting a whole-of-society approach. Terrorists and violent extremists will continue to exploit the internet to their advantage in novel ways. The Metaverse could provide violent non-state actors of various backgrounds with the ability to "forge and maintain virtual ideological and social communities and powerful, difficult-to-disrupt ways of expanding their ranks and spheres of influence".

While much of the discussion around policy recommendations places the onus on tech companies to take action, there are tangible implications of terrorist and extremist use of the internet for allied militaries. As evidenced by the influence of individuals like Anwar al-Awlaki and Junaid Hussain, tech-savvy terrorists can have a major impact on destabilising societies. Al-Awlaki's sermons and calls for jihad led directly to numerous acts of terrorism on Western soil, including an attack on a U.S. Army base in Texas. When it comes to terrorists that can either instigate or directly plan terrorist attacks, only the military and intelligence services are equipped with the tools to deal with these threats.