Chapter 12

Prevention of Radicalization on Social Media and the Internet

Sara Zeiger and Joseph Gyte

In the age of selfies, snaps, likes and shares, the internet and social media have transformed the way in which people communicate. In early 2019, global internet penetration reached 57%, or 4.4 billion users, and the overall number of mobile social media users reached 42%, or 3.2 billion people.[1] This means that people are able to share ideas, communicate and interact more rapidly than ever before, including with audiences on the other side of the world. Terrorist groups have certainly leveraged these new mechanisms and platforms for communicating amongst themselves and to potential recruits. For example, the Islamic State of Iraq and al-Sham (ISIS) has been known for producing sleek videos circulated on YouTube and Twitter, and has mastered new and emerging technologies and social media platforms, such as Telegram; all to promote its messages and recruit new members in cyberspace.

This chapter focuses on the prevention of radicalization on social media and the internet in this digital age. It first reviews the relevant methods and approaches that terrorists employ to spread their propaganda and recruit online. Subsequently, it looks at some of the more common and emerging prevention and preparedness strategies which address the online space. Besides reviewing the theoretical foundations to prevent radicalization on social media and the internet, this chapter will also draw upon specific examples, predominantly from three regions: Europe, Southeast Asia and East Africa, to illustrate what some countries are doing to tackle the problem of online radicalization.

Keywords**:** radicalization, violent extremism, prevention, online, internet, social media, propaganda, counter narratives.

Contemporary terrorist groups are the first generation whose members have grown up with access to the internet and social media. It should not be surprising, therefore, that these online platforms play a critical role in their approach to radicalizing and recruiting vulnerable individuals. In fact, social media and the internet have become increasingly useful facilitators of the promotion, incitement, intimidation, and radicalization of a much wider and previously unreachable audience.

Many terrorist organizations achieved great success through this approach. Online technologies, including social media, have many benefits - which are often leveraged by terrorist groups. They are able to reach audiences globally immediately, yet also tailor their messages to fit with different target audiences at the local level. They are able to develop rich content for the mass market, and still recruit individuals with privacy protections. Indeed, terrorist groups have proven to be innovative and adaptable, partially exploiting modern social communication systems and leveraging modern tools to achieve their aims.

Actors responsible for the prevention of online radicalization and recruitment face significant challenges. Most online platforms are owned and controlled by private companies, oftentimes under a different jurisdiction to that of the terrorists' location. Additionally, many terrorist groups have internally emphasized the importance of these social media platforms for recruitment and in order to develop high-quality, attractive propaganda, as well as effective marketing strategies for content dissemination. Furthermore, the sheer volume of terrorist propaganda published on an assortment of platforms has made it particularly challenging to contain their online presence.

Despite this, there are a number of potential legislative and policy measures to address this challenge, including: blocking online content and access; filtering and removing content; empowering online communities to counter the narratives of violent extremism and terrorism; the promoting positive and alternative messages; as well as building digital resilience and media literacy.

In this regard, through the use of in-depth desk research, this chapter will first outline some of the methods used by terrorist groups for radicalization on social media and the internet. Subsequently, it will address prevention strategies that are being – and possibly could be – implemented by the private and public sectors.

Terrorists' Methods for Radicalization on Social Media and the Internet

Due to the evolving nature and the vast variety of online platforms, as well as the breadth of exploitative techniques used, this section takes a broad approach when examining terrorists' methods, focusing on major platforms available at the time of writing, but noting the likelihood of other platforms being used. The methods presented should not be seen to be the only approaches employed, but rather a limited sample to provide a basic framework for understanding. In this regard, this section addresses how terrorist organizations have used social media and the internet to: adjust their structures and aims; enhance the quality of their propaganda materials; disseminate their messages to wider audiences; and recruit through more secure messaging platforms and leveraging new technologies. Select case studies will be utilized throughout for practical clarification of how terrorists are interacting with, radicalizing, and recruiting, vulnerable individuals online.

Structures, Dynamics and Aims of Terrorist Organizations

Terrorist organizations are dynamic systems that adapt and evolve over time.[2] Traditionally, terrorist organizations were thought to have a centralized, hierarchical structure in which the leaders at the top controlled the operations of the entire organization.[3] These traditional structures would often have a well-defined chain of command and control, with great specialization of functions for individuals and branches. This enabled hierarchical terrorist organizations to effectively maintain consistency in their disseminated message through specific individuals, but also increased the risk of interruption if the individual and/or unit was compromised.[4]

In recent years, social media and the internet have accelerated the speed, increased the complexity, and reduced the cost of sharing information. This has, in turn, supported the process of many terrorist organizations to reorganize themselves into a network style structure and enhanced the capacity of each cell and individual to operate more independently, especially for the dissemination of the organization's messages. This reorganization has provided them with greater flexibility, responsiveness, resilience, and outreach.[5] As a result, wider terrorist networks can remain operational, even if one or more cells are severely damaged or dismantled.[6] For example, after 9/11, Al-Qaeda suffered from increased pressures, lost training camps in Afghanistan, and many of the pre-9/11 senior leadership had been killed or captured. Therefore, in order for Al-Qaeda to remain relevant, they had to shift their approach toward inspiring and guiding other violent extremist groups, even if only through loose connections. Abu Musab al-Suri was one of the principal instigators for this shift in structure and strategy, and the internet was exploited as a means to facilitate this shift. This change in approach resulted in significant global impacts, as witnessed by the formation of local affiliated groups which conducted terrorist attacks in Bali, London, and Madrid.[7]

Now, modern terrorist networks typically consist of widely distributed, smaller cells who communicate and coordinate their campaigns in an interweaving fashion.[8] Relationships are often temporary and vary in intensity, depending on the task at hand. This has facilitated groups to develop not only wider internal connections, but external relationships as well, which tend to be based on shared norms, values, and mutual respect, rather than formed through formal bureaucratic structures.[9]

These characteristics of a networked approach were exemplified by the Charlie Hebdo attack, in Paris, France, in January 2015. One of the terrorists involved, Amedy Coulibaly, released a video stating that the attacks were carried out in the name of ISIS. However, the poor quality of the video suggested that this attack was not directly tied to ISIS' central media hub, al-Hayat Media; rather this was likely a smaller cell coordinating independently.[10] It was also reported that the other two terrorists involved, the Kouachi brothers, received $20,000 from Al-Qaeda in the Arabian Peninsula (AQAP), which highlights the increasing role of ad hoc external coalitions, caused by the networks communicating autonomously.[11]

In addition, the information revolution has also helped terrorist groups to move away from that of a traditional war model and move towards a new mode of conflict at societal levels. While terrorist organizations have always put effort into conducting psychological operations, they now have the capacity to conduct information operations on a much grander scale. Understanding the importance of knowledge and soft power, networked terrorists leverage social media and the internet for brand management[12] and propaganda, with the aim to influence public opinion and attract new recruits. Previously, terrorist organizations relied on traditional media, such as television, radio, leaflets, print, and in-person conversations to conduct their psychological operations. However, the internet and social media now provide an opportunity for terrorist organizations to increase the volume and diversity of disseminated messages, including a localized approach by individual cells. Hence, while terrorist organizations have always recognized how conflicts revolve around knowledge and information, they now have greater control over the information available, and consequently place greater emphasis on information operations which "aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries."[13]

In this regard, whilst terrorist propaganda will often depict violent behaviour, such as beheadings, with the intention of coercion or to encourage that such violence be imitated by others,[14] some propaganda now also focuses on brand management, through the portrayal of a narrative that aims to attract individuals to their cause.[15] Such narratives can take two approaches (or a combination of both): that which focuses on the personal incentives for joining the group (pull factors) and that which emphasizes or exaggerates the negative social, political, and/or economic conditions of the target population (push factors), thereby contributing towards a fertile environment for recruitment.[16]

Moreover, the global reach of these online platforms has allowed terrorist networks to merge and spread across national boundaries, cultures, and languages. This has been manifesting itself through the increasing occurrence of global coalitions of previously separate terrorist organizations. Most noteworthy was the pledging of allegiance (*bayat),* to Abu Bakr al-Baghdadi, the leader of ISIS. In light of geographic and security restrictions, which prevented oaths of allegiances being given in person, social media provided an alternative approach.[17] In Southeast Asia, for example, several terrorist groups in the Philippines and Indonesia, including Maute, Abu Sayyaf, Katibat Ansar al Sharia, and Mujahidin Indonesian Timor, all pledged their allegiances via online videos. In response, acceptance of the pledges was also released through online video.[18]

These adaptations, interactions, and behaviours highlight how the internet and social media have enabled terrorist groups to communicate, coalesce, and operate as global networks, while simultaneously providing greater freedoms for individual members and cells to coordinate, reach, and recruit target populations. Centralized messages can independently be adapted to a narrative that resonates in a localized context, in order to address the push and pull factors of the local population. ISIS, for example, has established media units in multiple regions, which are capable of producing sophisticated and locally contextualized propaganda materials, in the language and culture of the target population.[19]

Videos, Images, and Magazines: Propaganda

In parallel to social media and the internet enabling terrorist organizations to operate globally and distribute controlled propaganda, the wide diversity and availability of digital equipment, such as high-definition (HD) cameras and editing software, has also empowered terrorist organizations to produce propaganda of a quality similar to that of Hollywood movie professionals and those of the best marketing firms.[20] In fact, high quality propaganda has become increasingly important for a terrorist organization's branding strategy. The use of attractive digital media and novel methods contributes to the amplification of their brand, and has become an approach taken by numerous terrorist groups other than ISIS. The logic behind it is clear: in the battle for hearts and minds, they need to stand out and inspire individuals so as to secure recruits in an increasingly competitive environment.[21]

When propaganda can attract viewers as well as present a strong narrative that addresses the push and pull factors of local communities, it is likely to impact the radicalization process of vulnerable individuals. For example, Al-Hayat Media has produced many HD videos in the native languages of Europe, such as French and English, which targeted potential recruits and sympathizers by depicting life within ISIS territory as spiritually fulfilling, while at the same time declaring the European states to be immoral and unlawful. The production and distribution of such well-designed videos addresses the feelings of dissatisfaction present among parts of the European (diaspora) youth and offers a positive alternative. Such videos have played a significant role in the radicalization process of many young European Muslims and converts to Islam.[22]

Another modern example of high-quality propaganda is that of the video game *Salil al-Sawarem* (The Clanging of Swords): a "first-person shooter" game that was modelled on the popular Grand Theft Auto franchise, and aimed to gain publicity for - and draw attention to - ISIS. Trailers for the game were released on multiple websites and platforms across the internet, most notably YouTube, which at the time of the game's release in 2014, had 3.5 billion views a month on its gaming channels alone.[23] The use of cinematic productions and social media, and building on the engaging appeal of a videogame demonstrated the terrorists' tactic of exploiting popular culture as a means of enhancing the virality of their propaganda, as well showcasing their approach to reach the target audience—in this case game-loving youth.[24]

In this way, these types of sophisticated communications can easily go viral. The modern appearance assists with translating the terrorists' violence into a language that is understandable for the average young viewer, thereby increasing the psychological impact on the target audience.[25]

In addition to games, videos, and images, several terrorist groups also publish online magazines, and these publications appear to play an important role in online radicalization.[26] The accessibility and popularity of sleek online magazines has reportedly contributed towards the successful enlargement of several terrorist organizations, including ISIS, through their magazines *Dabiq* and *Rumiyah*, Al-Qaeda via *Inspire*, and Al-Shabaab through *Gaidi Mtaani*.[27]

Digital magazines provide their readers with a wide array of narratives in a single, well-presented package. Through the use of collective stories, individual stories, and event stories, terrorist magazines attempt to construct a wider narrative that resonates with their readers. In this regard, magazines can combine a multitude of various approaches. The inclusion of images that show fighters in militarized clothing has been shown to attract individuals to violence.[28] Additionally, emphasis on masculinity and bravery has been found to appeal to individuals who desire excitement and are attracted to thrill seeking.[29] The inclusion of other styles, such as the use of religious quotes, the presentation of members as heroic, their deaths as a sacrifice, and the portrayal of a common enemy, all have their own meanings, appeal to diverse readers, and lead towards a philosophical discussion and common ground.[30]

A secondary use of digital magazines is that the purpose cannot just be to inspire readers, but also to supply them with technical instructions on how to carry out violent acts as lone actors, or provide them with advice on joining the terrorist group.[31] The Boston Marathon bombing in 2013 was one such case. The brothers Tamerlan and Dzhokhar Tsarnaev, had read Al-Qaeda's *Inspire* magazine online, among other online propaganda, and claimed to have learnt how to make the bomb from an article in the magazine's first issue, titled *How to Make a Bomb in Your Mother's Kitchen.*[32]

The ability of terrorist organizations to produce inspiring, high quality propaganda that can be shared on social media and the internet has been of critical importance for their brand management and their approach to radicalization. In fact, social networking sites, such as Facebook, Twitter and YouTube, have become the modern-day tools that help to disseminate even the oldest of messages in a modern and relatable format.[33]

Social Networking Sites: Offering an Open Invitation to Everyone

The rise of social networking sites has enabled individuals and terrorist organizations alike to share information with large audiences instantaneously, irrespective of their geographic distance. Terrorists and their followers too are now able to share materials which can travel outside of their own social circles and reach populations that were previously inaccessible.[34]

The first terrorist to fully exploit this potential to an English-speaking audience was Anwar al-Awlaki, a US-born prominent Imam in AQAP dubbed the "bin Laden of the Internet."[35] He realized that despite the quality in which it was produced, online propaganda was not reaching as wide an audience as possible. In response, he pioneered the use of social networking sites to enlarge its scope, creating his own blog, Facebook page, and YouTube channel where he frequently shared his increasingly sophisticated videos and the online magazine *Inspire*.[36] Since then, terrorist organizations have specifically sought out Information Technology (IT) experts and skilled online marketers to lead their online propaganda campaigns,[37] which are now spread primarily via social networking sites.[38]

Most major social networking sites have instituted highly publicized and broad responses in an attempt to curtail the violent extremist content published on their platforms in recent years.[39] Unfortunately though, these platforms continue to be used by ideologues and recruiters, who remain adept at sharing propaganda and attracting followers.[40] In fact, an analysis of 1,000 pro-ISIS Facebook profiles from across 96 countries in 2018 found that the group's Facebook networks are still growing globally, despite efforts to take down new accounts as they emerge and are identified.[41]

These sites, which have become instrumental for the sharing of high-quality propaganda materials, have also become instruments for personal storytelling and for providing platforms for terrorists to share their experiences. Moreover, through the avoidance of posts that contain images and videos that could be censored by the host platforms, many of these stories remain online. These intriguing and personal narratives promote viral imitation, and have become a central feature in the recruitment process, particularly as a means to inspire those in pursuit of a new identity.[42]

An example of one such case is that of Siti Khadijah alias Ummu Sabrina, an Indonesian woman who managed Facebook pages for Kabar Dunia Islam (KDI), a media wing of ISIS based in Indonesia. She became well-known after posting her experience of traveling to Syria with her husband and their four children, which she published on Facebook, in June 2014. Following this, she regularly posted about her life in Syria, promoting the terrorist group's positive narrative of a monthly stipend, free schooling and healthcare, and how well her family had been treated. In response, her Facebook page was inundated with questions from Indonesians wanting to know how they too could travel to Syria. One Indonesian, for example, who went by the Facebook name Shabran Yaa Nafsi, was inspired by Siti Khadijah's story and travelled with his family in 2015 to Syria, where he was later killed.[43]

A similar example from a different geographical location was that of Aqsa Mahmood, a Scottish woman who travelled to the conflict zone in Syria and Iraq in 2013, when she was 19 years old. British authorities suspected that her use of social media, including Twitter and Tumblr, had contributed towards the radicalization and recruitment of a number of British teenagers. Similar to Siti Khadijah, Mahmood used social media to promote positive images of life under ISIS, and would frequently post propaganda publications, poems, religious verses, quotes by prominent extremists, and advice on how to travel to Syria.[44] These messages reached a wide audience, and encouraged other Westerners to travel to Syria and join Mahmood in her new life.

In addition to personal narratives, social networking sites have been used to control the narratives surrounding an event. During the Westgate terrorist attack in Kenya in 2013, Al-Shabaab made extensive use of Twitter for this purpose. An analysis of 556 tweets posted by Al-Shabaab throughout the attack found that the aim of these tweets was to control the narrative and retain the audience while they were trending online.[45] This approach, which has also been used by other terrorist groups, is known as "Hijacking a Twitter Storm": the posting of propaganda with a trending hashtag in order to take advantage of the huge traffic to greatly increase visibility.[46]

These examples, among others, all point in a similar direction; radicalization and recruitment through social networking sites are especially well-supported by personal narratives, stories, and first-hand reports, which are popularized and become viral. This in turn, then causes a chain reaction of imitations, particularly among those seeking to find their own identity.[47]

As well as using mainstream social media, such as those mentioned already, it should also be noted that terrorist groups use a wide range of various other social networking sites, including Flickr, Vimeo, Instagram, and SoundCloud, as well as their own blogs and websites, and file upload sites, such as Justpaste.it.[48] Having a larger volume of content online not only assures visibility, but simultaneously grabs the attention of the mass media (news outlets), thereby propagating the exposure to the propaganda further. This style of increasing conspicuousness helps terrorist organizations to seem more powerful than they actually may be, a phenomenon referred to as "force multiplication,"[49] which can have significant results. By increasing their communications, even a small group can create an exaggerated representation of the group's size, strength, and support in the community.[50] This, in turn, can then also directly affect reality: simply projecting the appearance of possessing many followers has been shown to increase the number of real followers.[51]

Furthermore, social networking sites provide support for the promotion of lone actors' narratives as well. For example, on 15 March 2019, 51 people were killed during terrorist attacks on two mosques in Christchurch, New Zealand.[52] The day before the attacks, the perpetrator, a right-wing violent extremist, posted his manifesto on Twitter and although his account was suspended after the attack, the 74-page anti-immigrant manifesto went viral before suspension.[53] Additionally, the perpetrator live-streamed the attacks through Facebook Live, via a head-mounted camera. Again, while the attacker's Facebook account was later removed, he streamed the attack for 17 minutes,[54] providing more exposure to his manifesto and narrative. In fact, this was further exacerbated by the copying and sharing of the video. In the first 24 hours after the attack, Facebook removed 1.5 million copies of the video and continued to find 800 visually distinct videos related to the original in the following days.[55] This clearly demonstrates how these platforms have provided extended scope for terrorist propaganda to reach a far wider audience than previously possible.

In addition to the messages and materials, the online accounts of violent extremists and terrorists are also frequently identified and deleted. However, these accounts are often reinstated multiple times after being removed, under different names or locations, allowing them to remain relatively unaffected by the implemented counter measures. For example, while ISIS has a limited number of central actors who are primarily responsible for online propaganda, no single individual account serves as an irreplaceable connection.[56] Moreover, as previously mentioned, terrorist propaganda can remain on a platform for long periods of time.[57] Such was the case of Ahmad Qadan, based in Sweden, who, through his Facebook profile, promoted ISIS and posted invitations such as "Contact me to support your brothers at the front," which remained on his Facebook profile from May 2013 to June 2015, until it was removed from the platform.[58]

Qadan's status highlights another key aspect of social networking sites: direct connections. As well as the use of these platforms for spreading sophisticated propaganda to wide audiences, and presenting personal narratives, they are also valuable to terrorist organizations for identifying and connecting with specific individuals who may be susceptible to recruitment.[59] However, having more explicit conversations with a potential recruit or fellow terrorist on a social networking site can leave these individuals more open to police monitoring. Therefore, once a recruiter identifies a potential recruit, they will often recommend moving over to a more secure platform to continue communications.[60] In other words, social networking sites are primarily used for disseminating propaganda and for radicalization purposes, e.g. by planting the seeds of dissatisfaction or offering alternative identities, which may not have been considered otherwise. On the other hand, private messaging channels are more often utilized for individual recruitment and coordination.

Messaging, Broadcasting and Channels

As the previous section has shown, online platforms have the potential to significantly influence the radicalization and recruitment process.[61] Once a vulnerable individual who may be susceptible to recruitment is identified, the recruiter will often guide the person to a more secure means of communication: either a one-to-one messaging application or a forum/channel (such as 4chan, 8chan or 8kun) with like-minded individuals. Many recruiters now rely on unregulated and unpoliced mobile messaging applications such as WhatsApp, Telegram and Kik, in order to deepen the contact with a potential recruit.[62] This highlights the importance of different types of social media platforms and different online media tools in the recruitment process. While some platforms and tools are more effective at spreading violent extremist messages to a broader audience, others aid the recruiter in guiding an individual towards one-to-one and eventually face-to-face interactions.

Encryption technology has been used by some terrorist organizations for the last couple of decades, for example, Pretty Good Privacy (PGP) was first created in the mid-1990s and Al-Qaeda's *Inspire* magazine would share its public-key, so that anyone could send an encrypted message to the publishers of the magazine.[63] However, most forms of encryption were primarily only available for higher ranking terrorists in an organization and mainly used for the coordination of attacks.[64] Now, almost all terrorists and their recruiters make use of encryption technologies.[65] In fact, terrorists now have access to a much larger market of encrypted communication options. For example, Skype, the internet-based telephone system, and one of today's largest online communication tools, is encrypted, allowing terrorists to speak in real time without a major risk of anybody discovering the content of their conversations.[66] Encrypted emails, like those offered by bitmessage.ch, also provide sophisticated methods for secure communications. Often not only is the original message encrypted but it is also sent to hundreds of other randomly selected accounts, making it virtually impossible to decipher who is the intended recipient who possesses the encryption key.[67]

Telegram, a free messaging application which allows its users to instantly send text messages, voice messages, pictures, videos, and any file type, has become the application of choice for most modern terrorist organizations. This is because Telegram provides "secret chats" with end-to-end "military grade encryption," which is not stored anywhere else but on the user's phone, while not even being accessible by the platform provider. Additionally, the platform provides further security, such as passcode locking the application and self-destruct timers on messages after being read.[68]

In Indonesia, the use of Telegram and other encrypted messaging services has reportedly contributed to the reinforcement of group solidarity, as members have been able to increase the sharing of information in a secure way.[69] Bahrun Naim, who was one of ISIS' top Indonesian propaganda distributors, used Telegram extensively. For example, in June 2015, Naim contacted a former friend, alias Ibad, via Facebook and connected him to his Telegram. They subsequently began to communicate about Ibad traveling to Syria via the encrypted service.[70]

Although encryption offers terrorists security of content, it does not necessarily keep them anonymous. The so called "dark internet" service providers and anonymous operating systems can often be used in unison with these encryption communications in order to further ensure anonymity.[71] The popular and often free means for achieving anonymity is "Virtual Private Networks" (VPN). These VPNs conceal a user's IP address and can make it appear in one or multiple countries, preventing, or at least slowing down, the security agencies' abilities to trace the source. The Onion Routing (TOR), originally created for the US Navy, is one such anonymous browser which utilizes such techniques.[72] These easy and often free forms of encryption and online anonymity have greatly impacted the recruitment process by allowing terrorists not only to send messages and files instantaneously, but to remain hidden and secure whilst doing so.

Leveraging Artificial Intelligence and Emerging Online Technologies

Finally, it is worth mentioning that terrorist groups are beginning to explore the use of Artificial Intelligence (AI) in their online radicalization and recruitment strategies. In the example from Indonesia above, Bahrun Naim also established a bot (an online "robot" application or program that autonomously completes tasks by interacting with systems and users) for communicating with potential recruits.[73] The bot would greet users with an automated message in Bahasa Indonesian and subsequently share propaganda messages and videos, such as interviews with militants, as well as guides for the fabrication of homemade explosives.[74] Al-Shabaab's news agency, Shahada, also used a bot on Telegram. The bot would send users a link to the most recent channel, which allows Shahada to remain in constant connection with its followers, even after an iteration of their channel had been suspended.[75] There is also speculation that more sophisticated language tools could be leveraged by terrorist groups to generate new content. For example, in a 2019 study, researchers speculated that open source AI tools, such as GPT-2,[76] could be used by malicious actors, including terrorist groups, to post auto-generated commentary on current events, overwhelm conversations on social media channels, or re-direct conversations online to match with their ideological views.[77] The report did not find evidence that GPT-2 was being used by terrorist groups, but it also found that existing auto-detection technology was not always able to distinguish human-generated extremist content from GPT-2-generated extremist content. This means that if terrorist groups begin to leverage open-source AI tools, it will take a human, not a machine, to accurately detect auto-generated terrorist content based on new technology.

Changes in internet structure and emerging technologies are also starting to be used by terrorist groups to circumvent detection, and this is complicating abilities to detect and take down terrorist content online. For example, the increasing use of decentralized web (DWeb) models, instead of centralized servers, mean that content can be stored across multiple users and multiple servers where hosting - and therefore takedown - cannot be controlled by a single source.[78] A switch to using DWeb services by a terrorist group like ISIS would essentially mean their propaganda would be almost impossible to eliminate from the internet. As another example, the alt-right's expanding use of social networks such as Gab has raised some alarm bells with counterterrorism researchers.[79] In this case, Gab's browser extension Dissenter allows for contentious debate and commentary on news articles that is not visible to anyone that does not have that extension installed, thus meaning automatic content detection is not usable on this platform. As new online technologies emerge, terrorists' use of these technologies is always a potential danger for further radicalization and recruitment strategies.

In summary, the internet and social media have been leveraged by terrorist organizations, which has also been correlated with a restructuring of organizations into local network cells that report globally but respond locally. Subsequently, terrorist groups have increased the sophistication of their propaganda materials and used social networking sites for dissemination. These platforms are also used to share personal and relatable messages that feed into their wider narrative. Essentially, social media and the internet have given terrorist organizations the means to effectively manage their brand both at a global and a local level. In addition, once a vulnerable individual is identified, encrypted messaging services can be used for the provision of specific information on how to carry out attacks or join the terrorist organization.

These methods of exploitation of social media and the internet pose considerable challenges for government authorities to prevent and counter online radicalization, either due to the sheer volume of online materials shared, the attractiveness of the narrative, or through high-end encryption software which makes it difficult to track. Moreover, new and emerging online technologies, such as AI and DWeb, if appropriately leveraged by terrorist groups, have the potential to further complicate potential prevention efforts aimed at reducing radicalization and recruitment through online channels.

Prevention Strategies for Radicalization on Social Media and the Internet

Noting the elaborate techniques used by terrorist groups that were outlined in the previous section, this chapter will now turn to possible solutions for preventing and countering radicalization on social media and the internet. Drawing on a strategy proposed by Stevens and Neumann, this chapter will examine three broad areas of how prevention of radicalization online might be possible: preventing the spread of terrorist content online (deterring producers); empowering online communities to counter the narratives of violent extremism and terrorism online and promote positive and alternative messages; and building digital resilience and media literacy (reducing the appeal).[80]

Preventing the Spread of Terrorist Content Online

The first strategy for preventing radicalization on social media and the internet involves preventing and prohibiting the spread of terrorist content and propaganda in the online space using digital mechanisms and tools. This includes: legislative and policy measures; blocking content and access to social media platforms; and filtering and removal of terrorist content from platforms. These mechanisms are intertwined, as the legislation around digital prevention can only be adapted and changed as new technological tools emerge in the space of prevention.

It should be noted that preventing the spread of terrorist content online involves leveraging technology and platforms that are usually owned by the private sector, so public-private partnerships and cooperation are critical in this particular strategy. One example of this sort of partnership is Tech Against Terrorism, an initiative developed in support of the United Nations (UN) Security Council Resolution 2354 (2017) to tackle terrorist narratives online.[81] The project builds the capacity of smaller start-up companies and provides online tools for the private sector technology industry to prevent the spread of terrorist content on their platforms. The project involves multiple private sector companies, such as Facebook, and regularly works with the UN Security Council bodies.

Legislative Measures: The Challenge of Creating Smart Regulation

The first method for preventing the spread of terrorist content online is through the use of legislation and policies that set regulations for prosecuting individuals and organizations. Some legislation penalizes the content itself, making it illegal for individuals or companies to host content online. For example, although it does not directly address only terrorist content, the German *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act, "*NetzDG*") sets the penalties for spreading hate speech and fake news online for up to 5 million euros for individuals and 50 million euros for organizations.[82] Under the definition of hate speech and fake news, the list of potential "unlawful" material include advocating actions against the democratic constitutional state, public order, personal honour, and sexual self- determination.[83]

Other legislative measures focus more on the specifics of how the private sector should prevent terrorist content on their platforms. Since 2019, there has been increasing pressure on the private sector to step up its efforts. For example, with reference to a letter sent by the Chairman of the Homeland Security Subcommittee on Intelligence and Counterterrorism of the United States to members of the Global Internet Forum to Counter Terrorism (GIFCT) in

March 2019, Facebook, Twitter, Microsoft, and YouTube were requested to provide information on their annual budgets to curb extremism on their platforms.[84] When information was not provided as requested, US Rep. Thomson and US Rep. Rose remarked in a press release;

> "The fact that some of the largest corporations in the world are unable to tell us what they are specifically doing to stop terrorist and extremist content is not acceptable… broad platitudes and vague explanations of safety procedures aren't enough. We need a full accounting of what is being done."[85]

Similarly, the European Parliament passed legislation called "Tackling the dissemination of terrorist content online" as a result of a 17 April 2019 resolution.[86] The regulation aims to avoid the "misuse of hosting services for terrorist purposes and contributing to the public security in European societies."[87] The legislation focuses specifically on what can be done by "hosting services" - i.e. social media platforms - in content regulation and takedown. It should be noted that some of the more controversial parts of the plan, such as the requirement to take down terrorist content within one hour of posting, had been scaled back to give private sector companies more time to complete this task.[88]

There are many challenges related to legislation and policy methods for preventing the spread of terrorist content online. Since policymakers tend not to be experts in communication technology, there is sometimes a misunderstanding of how internet and social media companies work, and which new technologies are available. There seems to be a general understanding from governments of how the mainstream social media platforms and tech giants operate (e.g. Facebook, Instagram, WhatsApp, Twitter, Microsoft, YouTube, and Google), but there is much less known about services offered by smaller companies such as Telegram, Signal, Ask.fm, Tumblr, Line, Kik, Qzone, Sina Weibo, Reddit, and many others. As new technologies such as AI and DWeb emerge, policymakers also struggle to keep up with the latest information and challenges associated with those technologies, and therefore are limited in their responses. Even less is known about how to moderate or regulate these platforms for preventing terrorist content online. In this regard, ensuring that governments and the private sector are working together in partnership is even more critical for smaller platforms that are less well-known.

As an example of this challenge, arguments against the EU's Terrorist Content Regulation have expressed that the adoption of the legislation may lead technology and social media platforms to "adopt poorly understood tools" to address violent extremism and terrorism online, and that "lawmakers and the public have no meaningful information about how well the [tools] serve this goal, and at what cost to democratic values and individual human rights."[89] In other words, there is a lack of evidence that the proposed tools are actually effective at successfully preventing terrorist content from spreading, and the consequences of such aggressive takedown could lead to unintentional infringements of human rights (e.g. limiting freedom of speech), should those methods not be proven to be efficient or effective.

Blocking Content and Access: Balancing Safety and Freedom of Expression

One of the approaches to preventing terrorism online undertaken by a number of governments has been to block access to a terrorist group's internet and social media channels. This has ranged from blocking individual websites and social media pages to blocking entire social media platforms. For example, in the aftermath of the 2019 Easter attacks on churches, hotels, and popular tourist sites in Sri Lanka, the government temporarily blocked all access to Facebook, Facebook Messenger, Instagram, WhatsApp, YouTube, and Viber.[90] This temporarily restricted the communications channels in the face of the imminent threat of more attacks across the country, but it also restricted the ability of Sri Lankans, expats, and tourists to communicate about their safety. In a similar way, Indonesia also blocked the popular social media application Telegram in 2017, after growing concerns of the influence of ISIS in the region and the use of Telegram in particular for spreading its messages on private Telegram channels.[91]

While on one hand, blocking websites, social media pages and entire social media platforms slows down the spread of terrorist messages online, it also slows down normal communications channels for the rest of the population. That is, while temporarily blocking access to content may be effective for short-term crisis situations like the aftermath of the multi-pronged jihadist attacks in Sri Lanka, long-term blocking will end up forcing terrorist groups and the general population alike to seek alternative forms of communication. For example, in this way, if WhatsApp is blocked in one country, another application is likely to take its place that will have similar features, and the population - and the terrorists - will regain their ability to communicate. There have also been allegations that blocking access to social media content is an infringement of fundamental human rights, and that blocking content has been used to prevent the spread of ideas of political opposition groups. In this regard, governments may need to consider balancing their efforts to block websites with ensuring basic human rights under international law, and see to it that basic human rights are not violated by their actions.

Takedown and Filtering of Terrorist Content

A third way to prevent the spread of terrorist content online is through the takedown of individual posts or websites by technology companies themselves or by third parties. This can be done in several ways: requests from government entities to remove pieces of content; the self-regulation of technology companies to remove content; artificial intelligence such as "upload filters" and; through individual hackers and civil society-led content takedown.

In most of the known cases, government bodies ask private sector companies to remove content on their platforms if it is identified as terrorist content. This is done through careful cooperation between intelligence and law enforcement entities and those companies. For example, Europol's Internet Referral Unit (EU IRU) is tasked to support EU authorities in flagging terrorist and violent extremist content online and sharing it with relevant partners. As of December 2017, the EU IRU assessed over 40,000 pieces of content across 80 platforms in ten languages, and 86% of the content flagged by this unit was successfully removed.[92]

In addition to cooperating with governments, the main tech giants tend to have relatively elaborate policies to make it more difficult for their platforms to become havens for terrorist content. For example, Facebook's counterterrorism policy states that there is no place for terrorism on Facebook,[93] using an academic definition of terrorism that is predicated on behaviour - not ideology.[94] Filtering and content takedown can be increased by the average social media user reporting on potential terrorist content, and Facebook's policies have particular terms of use which requires users to abide by certain behaviours and rules - otherwise risking their profiles being suspended or blocked. Once a particular item or post is flagged by a user, there is a dedicated team of experts (content moderators) reviewing the content to decide if it should remain online or offline. Twitter's policy around terrorism is similar in that its users "may not threaten or promote terrorism or violent extremism."[95] Twitter users can report Tweets that violate this policy, indicating that it is "abusive or harmful" and "threatening violence or physical harm."[96] YouTube has also developed a "Trusted Flagger" program which consists of individuals, government agencies, and NGOs working in various locations across the world that actively monitor content on YouTube, and flag content that violates their Community Guidelines.[97] The purpose of this program is to ensure that there are relevant local experts that understand the contextual and linguistic nuances of content being uploaded online.

The content flagged by the "Trusted Flagger" program receives higher priority for review by content moderators.

Another way for social media platforms to remove terrorist content from their platforms is through the use of AI. For example, image matching systems categorize previously removed terrorist content, and block the upload of new images or videos that are the same. The GIFCT has developed a "Hash Database": a shared list of the "hashes" or unique digital fingerprints of terrorist imagery and recruitment videos.[98] Members of the GIFCT are able to share new content with each other so that it can be removed before it spreads online. However, it should be noted that there are certain limitations to this database - notably that the "hashes" have to be exact matches to the original file data. In this way, images or videos that are manipulated slightly by users will not match the "hash" and therefore would not be recognized by the AI systems. In the meantime, social media companies are working with more sophisticated AI tools internally to become better and smarter at recognizing terrorist content automatically on their platforms.

In an April 2019 resolution taken by the EU, it was suggested that it become mandatory for companies to use "upload filters" - technological mechanisms that prevent content from being uploaded to social media sites if suspected of being terrorist content. The pressure to implement "upload filters" was exacerbated after the Christchurch attack in March 2019 - where the perpetrator live-streamed the attack on Facebook. Facebook subsequently reported that it removed 1.5 million videos circulated afterwards.[99] However, it should be noted that the effectiveness of "upload filters" and AI mechanisms is still unknown, and more research is needed in this field to ensure the technology and content detection are evolving as the terrorist threat evolves. As such, at the same time that social media companies continue to improve their AI systems, regulatory bodies should also factor in new technologies - and their limitations - in automatic content detection to their new policies.

Individuals also have the ability to directly combat terrorist propaganda online. As an example, a group of hackers linked to the "Anonymous Collective" also "declared war" on ISIS' online accounts and propaganda through #OpISIS, a hacking campaign that aimed to report, interfere and disrupt suspected ISIS accounts.[100] The campaign initially exposed 70 ISIS-linked websites and 26,000 Twitter accounts being used for recruitment, communications, and intelligence-gathering, which were later investigated and taken down by authorities.

There are several challenges with content takedown on social media platforms. First of all, content takedown requires a certain level of knowledge of the material (e.g. terrorist content) by those moderators charged with removing it. In some circumstances, human content moderators are faced with difficulties discriminating between legal and illegal content, and often face a "grey area" making it hard to decide whether something should or should not be considered in violation of company policies. For example, would a historical photo of Germany with Nazi flag in the background be considered neo-Nazi propaganda? The determination of how this might be a violation of company policy may depend on the context, comments and placement of the photo on the platform by the user. Appropriate staff training and expertise is needed to ensure appropriate content takedown - which of course requires resources. While these resources may be more readily available for larger companies, smaller platforms struggle to keep up with the knowledge and resources required for preventing terrorist content on their platforms.

Moreover, even the larger companies struggle to employ experts that have nuanced language and cultural expertise. For example, Facebook came under fire by the media over its inability to take down hate speech on Rohingya in Myanmar in April 2018.[101] Reuters was able to find over 1,000 examples of posts, comments and images attacking Rohingya communities on Facebook, which resulted in Facebook reacting by ramping up operations and more closely monitoring content in Myanmar.[102] Facebook was originally not equipped to handle the hate speech online due to a lack of experts with Burmese language and cultural skills, the use of slang and obscure language used to identify target groups, and the sheer volume of hate speech against the Rohingya community, something not anticipated by Facebook at the time.

In the same vein, as removing and filtering terrorist content slows down the flow of terrorist propaganda, it does not stop it entirely. One critic explained the challenge using the "Whack-A-Mole" metaphor - alluding to the "amusement park classic where one takes a mallet to a seemingly unending set of furry rodents that pop up at random from holes in a big board."[103] When content is taken down from one website, a replacement (or several) is made on a different channel. The online environment is constantly changing, and those charged with content takedown and filtering are met with an unending and exponentially growing supply of the same material appearing across different platforms.

Countering the Narratives of Violent Extremism and Terrorism Online

A second strategy for preventing radicalization on social media and the internet is related to countering (directly or indirectly) the narratives of violent extremism and terrorism in the online/digital space. The terminology of "counter-narratives" has been hotly debated in the CVE community, and while a robust debate of the definition of a counter-narrative is outside the scope of this chapter, it is important to take a commonly accepted definition of a "counter-narrative" as an attempt "to challenge extremist and violent extremist messages, whether directly or indirectly through a range of online and offline means."[104]

There are several points related to this strategy worth mentioning. First of all, the strategy of countering narratives in the online space should always take into consideration the target audience through the local context. If a counter-narrative does not address the grievances or needs of those joining terrorist groups, or counter the attractions of terrorist propaganda, then the counter-narrative surely will not be effective. This can be accomplished partially through empowering communities, both online and offline, with the appropriate knowledge, skills and tools to contest and counter the messages of violent extremism and terrorism in their networks. In this sense, some organizations have provided capacity-building to "local voices" as part of their broader communications campaign against terrorism. An example of this approach is the Kenya-based YADEN's #insolidarity campaign. The initiative provides capacity-building, tools, and platforms for youth to develop their own messages and share their stories about how terrorism has influenced their lives.[105]

Second, it is recommended that the design and structure of a counter-narrative focus on the development of a counter-narrative that is tailored to a specific target audience. Hedayah has developed a "How-To Guide" as well as several capacity-building modules that provide guidance for organizations looking to enhance their counter-narratives and campaigns.[106] The nine steps outlined in Hedayah's framework take a marketing perspective that is needs-based, whereby the context and target audience are carefully defined in the beginning of the process. This process is consistent with the integrated marketing communications (IMC) approach whereby significant research on the target audience is conducted at the outset, and strategic messages simultaneously target decision-makers and peripheral observers to achieve the maximum impact.[107] As one youth-worker from Kenya noted, terrorists use this same strategy in their communications techniques: "propaganda is seen as 'rebel cool' because it shows defiance and rebellion against governments."[108] On the other hand, their organization's peaceful protests were sometimes viewed by the community with scepticism, noting that their organization received complaints when police did not show up or aggressively confront protesters "because it is 'cool' to be seen as rebellious."[109] In this example, the actions taken by the youth organization were rejected by their target audience because it was not adapted to their perceptions of being "cool."

Once the target audience is identified, one of the most critical steps is to determine which messenger would be most effective at influencing that target audience. In this case, the counter-narrative needs to critically integrate a messenger that the target audience is most likely to listen to. For example, in Pakistan, the pop star Haroon created a cartoon series called *Burka Avenger,* based on a teacher at a girls' school fighting evil with books, pens, and martial arts. As a messenger, Haroon's celebrity status drew in an audience for *Burka Avenger* to deliver messages of peace, tolerance, acceptance, cooperation, gender-equality, and other critical values. Although the message was not necessarily designed to counter terrorism, the messenger for these positive messages was effective at reaching a broader and more relevant audience.

Finally, the content of a counter-narrative needs to both be attractive, but also provide the right information that prevents individuals from being allured by the terrorist group. This can be done in several ways: deconstructing terrorists' arguments (pointing out where they got the facts wrong); undermining the credibility of the group; and providing alternative narratives that emphasize non-violent actions. It is also crucial that counter-narratives are complemented by positive actions; mere words and pictures are not enough to persuade most dissatisfied people if unaccompanied by credible and matching deeds.

Deconstructing Terrorist Arguments

The first way of preventing terrorism online through counter-narratives is by directly engaging with and deconstructing the arguments of terrorist groups. Despite the direct engagement with terrorists or potential terrorists, the target audience for this type of strategy is actually not the individuals or group themselves - but the broader "theatre" of those that might be watching, listening, and following publicly-available forums. A specific example of this sort of deconstructive "theatre" can be seen through the public debate on Twitter between journalists, scholars, and religious leaders and the American Al-Shabaab terrorist Omar Hammami.[110] Some narratives aimed at Hammami attempted to persuade him to turn himself in, and exploited the schism between Hammami and Al-Shabaab's leadership as an entry point. For example, after an attempt on Hammami's life by Al-Shabaab, J.M. Berger tweeted, "Looks like you were within a quarter inch of dying… Perhaps it's time to come in now."[111] Others deconstructed his ideological and religious claims, using the Qur'an and Sunnah to contradict the justifications Hammami was making about jihad and his struggle against the West. While Berger was also hoping to personally persuade Hammami to surrender, it also had the effect of delivering a message to those followers closely watching Hammami's accounts.

De-legitimizing Terrorist Groups and Actions

A second counter-narrative method is to de-legitimize the message of terrorist groups by exploiting inaccurate information disseminated by terrorist groups, or leveraging humour and sarcasm to discredit a particular message or the organization as a whole. It is hypothesized that leveraging the voices of former terrorists ("formers" or "defectors") can assist in discrediting the group, and indeed some counter-narratives have exploited this idea.[112] Formers can draw attention to the hypocrisies of a group, such as highlighting corruption or injustice, or speaking to a reality that is inconsistent with what is promised by propaganda videos and recruiters. For example, Abu Abdallah, a former ISIS soldier, explained the oppression, punishments, and killings that took place under the rule of ISIS in Syria in an Arabic-language video "Inside ad-Dawlah."[113] Areeb Majeed, a suspected ISIS member from India, explained how he had been asked to conduct "menial tasks like cleaning toilets or providing water to those on the battlefield, instead of being pushed into the warzone" partially due to racial discrimination because "Indians were considered physically weak."[114]

Humour and sarcasm can also be used to discredit terrorist groups. One example is the case of Japan "winning the internet" through a technique Huey calls "political jamming," or "a subversive, satirical activity that draws on humour to reinforce ideological messages."[115] After the 20 January 2015 release of an ISIS YouTube video of two Japanese hostages, Kenji Goto Jogo and Haruna Yukawa, the Japanese public responded with screenshots of the video, photoshopped to ridicule ISIS. The hashtags #ISISCrappyCollageGrandPrix and #ISISPhotoshopGrandPrix encouraged more memes and photoshopped images to circulate.[116] The message from Japan to ISIS was clear: the Japanese were not intimidated by ISIS.

Positive Messages and Alternatives to Terrorism

Finally, instead of countering - or reacting to - the messages of terrorist groups, preventing terrorism online can focus on promoting positive and alternative messages to terrorism. These messages can address both structural or personal grievances such as building positive identities and enhancing social cohesion. There are several examples of alternative narratives worth mentioning here. In the Indonesian context, the Nahdlatul Ulama (NU), one of the largest Muslim organizations in the world, has been conducting a campaign focused on highlighting *Islam Nusantara*, or Indonesian Islam, the tenants of which are outlined in a 90-minute film, "The Divine Grace of Islam Nusantara."[117] The principles of Islam Nusantara emphasize the religious and cultural identity components of Islam in Indonesia that are uniquely Southeast Asian, and run contrary, in some cases, to more Salafist interpretations of Islam that are perceived by some to be "foreign." In March 2019, the NU announced that they recommend eliminating the use of the Arabic word *kafir* (infidels) to describe non-Muslims, and instead advocated for the use of the word *muwathinun* to emphasize that both Muslims and non-Muslims were equal in terms of citizenship in Indonesia.[118]

One important component of alternative messaging is to provide a non-violent action that still addresses grievances that communities might have which can be underlying drivers of radicalization. For example, in South Sudan, the *Anataban* (meaning "I am tired") campaign supports the "tired" people of South Sudan through music and art that promotes peaceful and non-violent movements. A video published in 2017, "*Soutna,*" meaning "Our Voice," states "we need peace desperately in order to achieve a bloodshed free 2017,"[119] encouraging users to use #Bloodshedfree2017 on their social media posts. The video shows young South Sudanese peacefully demonstrating in their communities and participating in actions such as voting and stating "we raise our voices to peace." The *Anataban* movement recognizes that violence and corruption are normalized in South Sudan and citizens are encouraged to take proactive steps towards peace while not tolerating violence in their communities.

Developing counter-narratives does not come without criticisms or challenges.[120] First, there is always the question around how these efforts can be measured and evaluated. There are very few studies that look at the impact and effectiveness of counter-narratives, although this body of literature is growing with efforts to find communications solutions that work in the space of terrorism prevention. Some studies have attempted to evaluate the effects of counter-narrative campaigns. For example, an initiative by students at Simon Fraser University in Vancouver, Canada, created the "Voices Against Extremism" project which included several components. The "Stories of Resilience" campaign featured students and average Canadians explaining "how extremism has affected their lives as well as their thoughts and opinions on community and Canadian identity."[121] It also included a YouTube video titled "An Evolution of Violent Extremism &Terrorism" to provide more information to students on the effects of violent extremism, and featured an art gallery event called "Art is H.E.R.E: Reshaping Identities." The project reached over 160,000 individuals on their online campaigns, and an additional 100 individuals (students) through their offline engagements. However, the evaluation of the campaign included largely superficial measurements; there is no evidence of impact on cognitive and behavioural changes.

Another study by McDowell-Smith, Speckhard and Yayla (2017) examined the effects of counter-narrative videos on the perceptions of college students in the US.[122] The study showed several video campaigns using defectors from ISIS to a group of college students and asked them to provide information on their perspectives regarding the effectiveness of the campaign. One critical limitation to this study was, of course, that the average US college student is not radicalized, and therefore the effectiveness of the campaigns can only be considered in terms of a wider "youth" population, but not with respect to the potential target population of youth that may be interested in joining ISIS.

Perhaps one of the best in-depth studies specifically on counter-narratives was conducted by the Institute for Strategic Dialogue on three counter-narrative campaigns: "Exit USA," "Average Mohammad," and "Harakat ut Taleem."[123] This study seems to be unique in that it starts to look at measures of engagement and impact, rather than simply measures of the scope or reach of the campaigns.[124] Using analytical tools such as assessing the sentiment of the comments or anecdotes of sustained engagement (both constructive and antagonistic), this study started to examine the potential impact of the campaigns on changing attitudes of the target audience. For example, the "Exit USA" campaign had the effect of soliciting a sustained engagement with a former white supremacist who was thinking of returning to the group, and managed to persuade him to participate in Exit USA's activities, thereby deterring him from re-engaging from the group.

Second, there are potential considerations for "blowback" if certain parts of the message or the messenger are not right, and there have been examples where campaigns against violent extremism have actually made the problem worse.[125] Campaigns countering the message of terrorist groups may provide a platform for terrorists to make their arguments in a more public way - drawing attention to their arguments rather than detracting from them. A frequently-cited example of the "blowback" effect of a communications campaign is that the media coverage on Iraq and Afghanistan, specifically the coverage of detention facilities in Guantanamo Bay and Abu Ghraib, reduced the support on the ground in these countries for the American actions there.[126]

The third challenge relates to some communications strategies that have attempted to flood the Internet with messages directly countering terrorists' messages in the hopes that this would overwhelm communications channels with the "right" messages. The US Department of State also took on this strategy through the Center for Strategic Counter-Terrorism Communications (CSCC), now relabelled Global Engagement Center, whereby their digital outreach team (DOT) "crashe[d] various online forums to troll ISIS sympathizers and regularly jumps onto pro-ISIS Twitter hashtags."[127] By "hijacking" the hashtags, CSCC's DOT intended to make available a larger quantity of counter-messages than the violent extremist content.

However, there is little evidence to suggest that this approach has been effective at reducing the appeal of terrorism or preventing radicalization online. This is because the trajectory from the development and distribution of a communications product to the consumption of its message to the potential impact on an individuals' behaviour is a complex process. Research suggests that most participants in foreign fighting and/or terrorist activities are not primarily recruited online, but rather by "real-world" connections to social networks.[128] As Archetti outlines, consumers of information engage in an active selection of the materials on which to focus, meaning consumers only "buy" into the information that catches their attention or appeals to them in some way.[129] In this sense, the mere availability of a message, or the number of times it appears to have been viewed, does not directly translate into interest, or impact on cognitive processes, let alone impact on behaviour. Obviously, availability alone is not correlated with behavioural change; all individuals that view a video by ISIS online do not necessarily become radicalized. Otherwise, there would be a very strange pool of "radicalized" counterterrorism experts and researchers that regularly view terrorist content in the hope to understand the content and messaging techniques used by various terrorist organizations.

At the same time, and what is easily illustrated by the spread of terrorist messages, is that few individuals can be responsible for an idea that goes "viral" and reaches a large audience. According to Malcom Gladwell's *Law of the Few*, 20% of participants are responsible for 80% of the work as long as that 20% includes the right mix of actors: connectors, or those that bring the network together; mavens, or those "experts" that provide new information to the group; and salesmen, or those that bring charisma and powerful negotiating skills to the participants.[130] Saifudeen argues that groups like ISIS and Al-Qaeda have adopted a communications model that applies this theory. ISIS "fanboys" are the connectors that spread the message easily to their networks, fighters are the mavens that offer information and experience from the battlefield, and leaders like Anwar al-Awlaki are the salesmen that give credibility and charisma to the ideas.[131]

Last, there seems to be a lack of emotional appeal for many of the counter-narratives that are devised and constructed online, especially those that are more direct and targeted towards terrorist content. For example, the Religious Rehabilitation Group (RRG) operating out of Singapore provides a point-by-point deconstruction of the ideologies leveraged by groups such as Al-Qaeda and ISIS in an attempt to discredit them. However, as Archetti puts it, "Narratives… are much more than rhetorical devices… they have deep roots: they are socially constructed."[132] Ferguson also argues that, "questions around why certain [violent extremist] VE narratives can be so powerful are rarely addressed in detail in contemporary grey CVE literature… VE narratives are successful… because they tap into, and seemingly confirm, existing beliefs of anxieties."[133] The narratives that terrorist groups offer are highly emotional, and therefore the counter-narratives need to reflect this same principle.

Building Digital Resilience and Media Literacy

In today's digital age, there is a massive challenge related to "fake news," "misinformation," and "disinformation," which are tactics employed by political actors and terrorist groups alike. A third and final strategy for the prevention of terrorism online is through building digital resilience and media literacy skills. This is premised on two assumptions. Firstly, that by building digital resilience and media literacy, the average citizen is able to peacefully overcome grievances that might lead to radicalization that are based incorrectly on misinformation or disinformation. Secondly, that a citizen that is able to evaluate both the content of the information provided and the credibility of the source more effectively, would less likely be persuaded by terrorist propaganda.

The terms "fake news," "misinformation," and "disinformation" are sometimes used interchangeably, so it is first of all important to define these terms for the purposes of preventing terrorism. "Fake news" can be defined as "fabricated information that mimics news media content in form, but not in organizational process or intent," whereas "misinformation" is "false or misleading information, and "disinformation" is "false information that is purposely spread to deceive people."[134] All of these types of content are leveraged by many different kinds of actors (including politicians and terrorist groups) - and are not always intended to do harm. However, these tools are also employed by terrorist organizations, and can have the effect of exacerbating structural or societal grievances or other push factors that may lead to radicalization or recruitment. Moreover, these tactics may emphasize underlying black-and-white thinking or encourage polarizing worldviews that lead to divisions in society. These tactics can also play upon pull factors that may make a terrorist group or ideology seem more attractive. Combined with divisive rhetoric used in hate speech and by terrorist groups that exacerbate "us" versus "them" thinking, tactics employing "fake news," "misinformation," and "disinformation" can be dangerous.

It is important, therefore, that skills and mechanisms for building digital and media literacy are enhanced as part of a comprehensive way of preventing terrorism online and in social media. This means that potentially vulnerable youth should be equipped with the appropriate skills to navigate the challenging communications environment they experience every day, including a large social media presence online. This environment is often filled with conflicting messages - and determining which of those messages are credible and which are false is a complex skill to be cultivated. This approach has been adopted in UNESCO's preventing violent extremism (PVE) efforts, noting the importance of responsible behaviour online and offline as part of an individual's responsibility as a "digital citizen."[135]

Even ISIS has caught on to the importance of digital and media literacy, but has distorted this concept to serve its own aims. For example, in an infographic titled *Rumors*, ISIS warns against the danger of rumours that "distort a person or a group of Muslims," or "demoralize the Muslims in times of hardship," or "dividing the Muslims and making problems between them," among others.[136] The infographic was accompanied with advice on how to fight rumours, and how these can be damaging to Muslims.

The formal education sector also plays a significant role in ensuring students are able to differentiate between various kinds of tactics that are used by terrorist groups to spread their messages. To aid the education sector, there are a number of resources available to teachers to better enhance their abilities to teach students about digital resilience. For example, UNESCO has a number of tools, including a framework and assessment tools, to monitor the progress of digital literacy skills worldwide, in support of Sustainable Development Goal #4 on Quality Education. The framework provides guidelines on a number of different digital competencies that include:

- information and data literacy (e.g. browsing, searching, and evaluating data online;
- communication and collaboration (e.g. interacting, sharing, and collaborating using digital technologies);
- digital content creation (e.g. developing digital content, copyrights, and licensing);
- safety (e.g. protecting devices, personal data, and well-being); and
- problem solving (e.g. identifying needs and digital/technical responses).[137]

It goes without saying that the digital literacy framework is broader than supporting terrorism prevention online, and is intended to be integrated into school systems globally.

Social media and technology companies have also dedicated quite a few resources to educating the public on digital and media literacy skills. For example, Google for Education also has a number of digital tools for teachers that provide educators with ways to bring hands-on learning to digital and media literacy. They have a suite of lesson plans, activities, and video tutorials dedicated to assisting teachers in cultivating digital skills in their students.[138] Facebook also has developed a Digital Literacy Library comprised of lesson plans designed to help youth develop digital skills, both inside and outside the classroom.[139]

While digital and media literacy of course have other possible effects in addition to preventing terrorism, digital resilience for the purpose of terrorism prevention should focus on verifying the credibility of the sources and methods of the content under question. The Tony Blair Institute for Global Change suggest the "RAVEN" method for determining the credibility of Internet sites in relation to identifying terrorist propaganda:[140]

- Reputation: The student examines the credibility of the website or author.
- Ability to see: The student questions if the person writing is in a position to be well-informed about the issue.
- Vested interest: The student questions if the author stands to gain anything by having a certain point of view.

- Expertise: The student questions if the author is qualified to know what s/he is talking about through training or background.
- Neutrality: The student questions if the content is neutral, and if not, why the author might be taking a particular point of view.

While there are other methods in existence, the critical point of digital literacy for students in this case is to ensure that students really understand the credibility of the source before it is trusted as fact or shared with others.

Another way that sources can be checked is through fact-checking websites. For example, Snopes.com is a tool that can check the content of a webpage to verify against other known sources to determine whether the content is likely factually-based. In some cases, Snopes.com has been able to identify hate speech online. For example, in May 2019, Snopes reported on how anti-Islamic hate speech, revealed by their fact-checking technology, was being spread on Facebook through a particular network.[141] As a result of the investigation, the network and forum for this hate speech was reportedly disabled.[142] The government of Indonesia has also undertaken a similar initiative through its TRUST Positif website.[143] Here, internet surfers can insert a URL and verify whether or not a given source is a trusted domain name. Smaller companies dedicated to fact-checking for social good are beginning to evolve on social media platforms, and these tools can be leveraged to avoid the spread of "fake news," "misinformation" and "disinformation," some of which is affiliated with terrorist groups.

Conclusion

This chapter highlighted that terrorist organizations are continuously adapting to the evolving technologies and are particularly adept at using social media and the internet for radicalization and recruitment purposes. However, this chapter also notes a number of potential approaches which could contribute towards terrorism prevention.

Firstly, a public-private cooperative and inclusive approach was found to be most important, contributing to the enhancement of all prevention efforts. As noted, there is a distinct lack of understanding within the public sector on how exactly most of these platforms operate and the types of responses these can feasibly take. This was found to be especially the case for smaller, lesser-known online platforms. Hence, it is important to coordinate and consult with all relevant providers when developing legislation and policies, as well as for practical responses. On this note, realistic legislation that sets regulations for prosecuting individuals and organizations, penalizes the content, and makes it illegal to host such content on a platform is also seen to be a valuable response; provided that private sector representatives are engaged during development, to ensure achievability.

Another approach is the blocking of access to content shared by terrorist groups. However, it should be noted that the blocking of entire platforms has unintentional effects on the general population and there is a significant risk of infringing upon universal human rights. Furthermore, online platforms tend to be resilient; when one platform is blocked, another will often surface in its place. Therefore, a potentially more effective approach, although often requiring more man-power and time, is takedowns of terrorist content. While this is primarily implemented as per the private organizations' own policies, it would also benefit from strong public-private cooperation and collaboration, whereby government agencies can inform platform providers of content to be removed. Additionally, this can be further enhanced by awareness raising and the encouragement of a whole-of-society approach, where every user understands the importance of her or his role in flagging and referring any online content that is in breach of such policies. Those who are responsible for the decision on whether a takedown is required also need further training, particularly in relation to localizing their knowledge and understanding. Having a clear comprehension of the local language and culture will greatly enhance their decision-making skills on whether specific content should be removed, thereby increasing the effectiveness of the response overall.

On the other side of the coin is "upload filters," which also could be seen to be a proactive and efficient means for prevention. However, the effectiveness of such an approach has yet to be proven and the technologies for doing so are not yet mature enough to definitively work independently of human review and action.

While these approaches may help to contain the spread of online terrorist propaganda, they will not necessarily stop the flow entirely. Therefore, there is also a need for additional approaches which can address the propaganda that leaks through. One such approach is that of counter-narratives. While the effectiveness of this approach is still disputed, developing a comprehensive counter narrative strategy which delegitimizes and deconstructs the terrorists' narrative and produces positive and alternative narratives, may assist with addressing the structural and personal grievances which leave individuals and groups vulnerable to radicalization. In this regard, there is a need to enhance the skills - and amplify the dissemination - of those who are appropriately positioned to produce counter narratives, such as former violent extremists and creative young activists, in a manner that is locally tailored, targeted and relevant.

However, there will still be cases where the terrorists' propaganda reaches the target audience, but the counter narratives do not. Therefore, there is also a need to build the resilience of individuals, especially in the form of digital resilience and media literacy. In this regard, global education sectors have a significant role to play and should adapt their curriculum to include approaches that would provide youth with the understanding and skills to question the credibility of sources more effectively, thereby decreasing the likelihood of being persuaded by terrorist propaganda. It is noted that some governments and private organizations have started to engage in this field. However, at the current stage, the further enhancement of these efforts could be a useful step for governments to take.

Finally, it should also be noted that while these approaches are preventative, they are also reactive in development, based upon previous experiences and the ongoing methods used by terrorist groups. It is of the utmost importance for governments and online platform providers to be forward-looking: assessing how the platforms may be exploited in the future and what possible forthcoming platforms may play a role in radicalization and recruitment. The effective identification of possible future threats will allow for more proactive prevention strategies and ensure positive outcomes.

Sara Zeiger is the Program Manager for the Department of Research and Analysis at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Sara Zeiger supports the Director in managing the Department's resources and programs, including the Counter-narrative Library, Hedayah's non-resident Fellowship Program and Hedayah's annual International CVE Research Conference. Sara was also the lead content developer for Hedayah's App, MASAR, that provides practical guidance on MM&E for CVE. She has also been a co-Director for a NATO Science for Peace and Security (SPS) grant on enhancing the role of women in international CVE efforts. In addition to her duties in the Department of Research and Analysis, she was also Hedayah's liaison with the Global Counterterrorism Forum (GCTF) to support the development and drafting of their framework document, the "Abu Dhabi Memorandum on Good Practices for Education and CVE" and the follow-up "Action Plan". Sara Zeiger is currently a Non-Resident Fellow in International Relations and Counter-Terrorism for TRENDS Research & Advisory. Prior to joining Hedayah, Sara worked as a Research Assistant at the Center for Middle Eastern Studies at Harvard University. She also served as a Head Teaching Fellow for the Harvard Extension School where she taught courses on anthropology in the Gulf, politics in the Middle East, and

Islam in the West. Sara Zeiger holds a Master's in International Relations and Religion (concentrations: Security Studies and Islam) from Boston University, and graduated as valedictorian with a B.A. in Psychology and Religion from Ohio Northern University.

Joseph Gyte is the Senior Program Associate within the Capacity Building Department at Hedayah, the International Center of Excellence for Countering Violent Extremism in Abu Dhabi. Joseph Gyte supports the curriculum development, implementation and evaluation of capacity building programs, and leads a program for psychologists and social workers to support families affected by violent extremism. Prior to joining Hedayah, Joseph Gyte worked as a Terrorism Prevention Program Consultant at the United Nations Office on Drugs and Crime (UNODC), Regional Office for Southeast Asia and the Pacific. In this position, he acted as focal point for the planning and implementation of capacity building activities related to Counter Terrorism in Indonesia, Myanmar and the Philippines. He also contributed technical inputs towards the development of a National Action Plan to Prevent Violent Extremism in a Southeast Asian country, and produced multiple training manuals, handbooks, publications and Op-Eds, on behalf of UNODC. Joseph Gyte has also worked in the Office of the EU Counter-Terrorism Coordinator in Brussels, where he was directly involved in the EU's development of policy responses to the evolving phenomena of foreign terrorist fighters and violent extremism. Joseph Gyte's educational background includes a Master's degree in Terrorism Studies from St. Andrews University and a Bachelor's degree in Psychology from Cardiff University.

Endnotes

[1] We Are Social, 'Digital in 2019,' We Are Social, 2019. Available at: https://wearesocial.com/global-digital-report-2019.

[2] Carley, Kathleen, Matthew Dombroski, Max Tsvetovat, Jeffrey Reminga, and Natasha Kamneva, 'Destabilizing Dynamic Covert Networks'; in: The 8th International Command and Control Research and Technology Symposium, 2003. Available at: http://www.dodccrp.org/events/8th_ICCRTS/pdf/021.pdf.

[3] Perliger, Arie, 'Terrorist Networks' Productivity and Durability: A Comparative Multi-Level Analysis,' *Perspectives on Terrorism,* 8(4), 2014, pp. 36-52.

[4] Red Alert, 'Implement Hierarchy Reconstructing Methods,' Eötvös Loránd University et al., 2019. Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c3b41079&appId=PPGMS.

[5] Zanini, Michele and Sean J.A. Edwards, 'The Networking of Terror in the Information Age'; in: Arquilla, John and David Ronfeldt (eds.), Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND, 2001, ch. 2. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

[6] Xu, Jie, Daning Hu, and Hsinchun Chen, 'The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad,' *Journal of Homeland Security and Emergency Management,* 6(1), 2009, pp. 1-33.

[7] Cruickshank, Paul and Mohannad Hage Ali, 'Abu Musab Al Suri: Architect of the New Al Qaeda,' *Studies in Conflict & Terrorism,* 30, 2007, pp. 1-14.

[8] Arquilla, John and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime and Militancy.* RAND, 2001. Available at: http://www.rand.org/pubs/monograph_reports/MR1382.html.

[9] Nohria, Nitin and Robert G. Eccles, *Networks and Organizations: Structure, Form and Action.* Boston: Harvard Business School Press, 1992.

[10] Withnall, Adam, 'Were Paris Attacks the First Case of al-Qaeda and ISIS Working Together? Six Questions Raised in Aftermath of France Shootings,' *The Independent,* 2015. Available at: http://www.independent.co.uk/news/world/europe/were-paris-attacks-the-first-case-of-al-qaeda-and-isis-working-together-six-questions-raised-in-9975349.html.

[11] Levitt, Matthew, 'How do ISIS Terrorists Finance Their Attacks?' The Hill, 2015. Available at: http://thehill.com/blogs/pundits-blog/homeland-security/260597-how-do-isis-terrorists-finance-their-attacks.

[12] For the purpose of this chapter, "Brand Management" is used to refer to the techniques employed by terrorist groups to maintain and increase the perceived value, importance and reputation of the group.

[13] Arquilla and Ronfeldt 2001.

[14] Koch, Ariel, 'Jihadi Beheading Videos and their Non-Jihadi Echoes,' *Perspectives on Terrorism*, 12(3), 2018, pp. 24-34.

[15] Macnair, Logan, and Richard Frank, 'Voices Against Extremism: A Case Study of a Community Based CVE Counter-Narrative Campaign,' *Journal for Deradicalization*, 10, 2017, pp. 147-174.

[16] Hedayah, *Introduction to Countering Violent Extremism.* Abu Dhabi: Hedayah, 2019.

[17] Atwan, Abdel Bari, *Islamic State: The Digital Caliphate*. Berkeley, California: University of California Press, 2015.

[18] Weis, Caleb, 'Philippines-based Jihadist Groups Pledge Allegiance to the Islamic State,' FDD's *Long War Journal*, 2016. Available at:

https://www.longwarjournal.org/archives/2016/02/philippines-based-jihadist-groups-pledge-allegiance-to-the-islamic-state.php.

[19] Macnair, Logan, and Richard Frank, ‘Changes and Stabilities in the Language of Islamic State Magazines: A Sentiment Analysis,’ *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide,* 11(2), 2018, pp. 109- 120.

[20] Atwan 2015.

[21] Bulbeck, Emilia, ‘The Path to Persuasion: An Investigation into how al-Shabab Constructs their Brand in their Digital Magazine Gaidi Mtaani,’ Master’s Thesis, Uppsala University, 2017. Available at: http://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1148028&dswid=-8240.

[22] Macnair and Frank 2017.

[23] Al-Rawi, Ahmed, ‘Video Games, Terrorism, and ISIS’s Jihad 3.0,’ *Terrorism and Political Violence*, 30(4), 2018, pp. 740-760.

[24] Plebani, Andrea and Paolo Maggiolini, ‘The Centrality of the Enemy in al-Bahdadi’s Caliphate’; in: Maggioni, Monica and Paolo Magri, (eds.), *Twitter and Jihad: The Communication Strategy of ISIS*, ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.

[25] Ibid.

[26] Macdonald, Stuart, ‘Terrorist Narratives and Communicative Devices: Findings from a Study of Online Terrorist Magazines’; in: Zeiger, Sara (ed.), *Expanding Research on Countering Violent Extremism*. Abu Dhabi/Perth: Hedayah/Edith Cowan University, 2016, pp. 127-141.

[27] Madrazo, Andrea, ‘*Recruiting Followers for the Caliphate: A Narrative Analysis of Four Jihadist Magazines*,’ Master’s Thesis, University of Central Florida, 2018. Available at: https://stars.library.ucf.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=6786&context=etd.

[28] Hamm, Mark, ‘Apocalyptic Violence: The Seduction of Terrorist Subcultures,’ *Theoretical Criminology*, 8(3), 2004, pp. 323-339.

[29] Cottee, Simon and Keith J. Hayward, ‘Terrorist (E)motives: The Existential Attractions of Terrorism,’ *Studies in Conflict & Terrorism,* 34(12), 2011, pp. 963-986.

[30] Sunde, Hans Myhre, ‘Stories, Style and Radicalization: A Cultural and Narrative Criminological Study of Jihadi Propaganda Magazines,’ Master’s Thesis, University of Oslo, 2017. Available at: https://www.duo.uio.no/bitstream/handle/10852/57541/Masteroppgave_HMSUNDE.pdf?sequence=1&isAllowed=y.

[31] Conway, Maura, Jodie Parker, and Sean Looney, ‘Online Jihadi Instructional Content: The Role of Magazines’; in: Conway, Maura et al. (eds.), *Terrorists’ Use of the Internet: Assessment and Response*. NATO Science for Peace and Security Series – E: Human and Societal Dynamics (136). Amsterdam: IOS Press, 2017, pp. 182-193.

[32] Gunaratna, Rohan, and Cleo Haynal, ‘Current and Emerging Threats of Homegrown Terrorism: The Case of the Boston Bombings,’ *Perspectives on Terrorism,* 7(3), 2013, pp. 44-63.

[33] Maggioni, Monica, ‘The Islamic State: Not That Surprising, If You Know Where to Look,’; in: Maggioni, Monica and Magri, Paolo (eds.) *Twitter and Jihad: The Communication Strategy of ISIS*. ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.

[34] Kernan, Erik R., ‘The Islamic State as a Unique Social Movement: Exploiting Social Media in an Era of Religious Revival,’ Honors Thesis, University of Vermont, 2017. Available at: https://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1227&context=hcoltheses.

[35] Madhani, Aamer, ‘Cleric al-Awlaki dubbed ‘bin Laden of the Internet’, *USA Today*, 2011. Available at: http://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm.
[36] Conway, Maura, ‘From al-Zarqawi to al-Awlaki: The Emergence and Development of an Online Radical Milieu,’ *Combatting Terrorism Exchange,* 2(4), 2012, pp. 12-22.
[37] Nissen, Thomas Elkjer, ‘Terror.com: IS’s Social Media Warfare in Syria and Iraq,’ *Contemporary Conflicts: Military Studies Journal*, 2(2), 2014, pp. 1-8.
[38] Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen, ‘Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization,’ *Studies in Conflict & Terrorism,* 2016. Available at: https://www.tandfonline.com/doi/abs/10.1080/1057610X.2016.1157402.
[39] These responses, which include monitoring and takedown, will be discussed in greater depth in the following section.
[40] Shajkovci, Ardian, ‘Engaging English Speaking Facebook Users in an Anti-ISIS Awareness Campaign,’ *Journal of Strategic Security*, 11(3), 2018, pp. 52-78.
[41] Waters, Gregory, and Robert Postings, ‘Spiders of the Caliphate: Mapping the Islamic State’s Global Support Network on Facebook,’ Counter Extremism Project (*CEP) Report,* 2018.
[42] Lombardi, Marco, ‘IS 2.0 and Beyond: The Caliphate’s Communication Project’; in: Maggioni, Monica and Paolo Magri (eds.), *Twitter and Jihad: The Communication Strategy of ISIS.* ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.
[43] Institute for Policy Analysis of Conflict (IPAC), ‘Online Activism and Social Media Usage Among Indonesian Extremists,’ *IPAC Report No. 24,* 2015. Available at: http://file.understandingconflict.org/file/2015/10/IPAC_24_Online_Activism_Social_Media.pdf.
[44] Counter Extremism Project (CEP), ‘Extremists: Aqsa Mahmood,’ CEP, 2016. Available at: https://www.counterextremism.com/extremists/aqsa-mahmood.
[45] Mair, David, ‘#Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack,’ *Studies in Conflict & Terrorism*, 40(1), 2017, pp. 24-43.
[46] Atwan 2015.
[47] Lombardi 2015.
[48] Conway, Maura, ‘Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research’; in: Anne Aly, Stuart Macdonald, Lee Jarvis and Thomas Chen (eds.), *Violent extremism online: New perspectives on terrorism and the Internet*. Abingdon: Routledge, 2016, pp. 123-148.
[49] Nissen 2014.
[50] Maggioni, Monica, ‘The Islamic State: Not That Surprising, If You Know Where to Look’; in: Maggioni, Monica and Paolo Magri (eds.), *Twitter and Jihad: The Communication Strategy of ISIS*. ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.
[51] Nissen 2014.
[52] Graham-McLay, Charlotte, ‘Death Toll in New Zealand Mosque Shootings Rise to 51,’ The *New York Times,* 2 May 2019. Available at: https://www.nytimes.com/2019/05/02/world/asia/new-zealand-attack-death-toll.html.
[53] Christofaro, Beatrice, Michelle Mark, and Ellen Cranley, ‘What We Know So Far About Brenton Tarrant, The Suspect in The New Zealand Mosque Shootings,’ *Business Insider,* 2019. Available at: https://www.businessinsider.com/new-zealand-mosque-shoote.rs-what-we-know-2019-3?r=US&IR=T.
[54] Associated Press,’Christchurch Mosque Shootings: Gunman Live Streamed 17 Minutes of Shooting Terror,’ *New Zealand Herald,* 15 March 2019. Available at:

https://www.nzherald.co.nz/nz/christchurch-mosque-shootings-gunman-livestreamed-17-minutes-of-shooting-terror/BLRK6K4XBTOIS7EQCZW24GFAPM/.
[55] Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.
[56] Waters and Postings 2018.
[57] Lombardi 2015.
[58] Associated Press, 'Swedish Isis fundraiser statuses were on Facebook for two years before deletion,' *The Local*, 25 March 2018. Available at: https://www.thelocal.se/20180325/swedish-isis-fundraiser-statuses-were-on-open-facebook-page-for-two-years-before-deletion.
[59] Waters and Postings 2018.
[60] Atwan 2015.
[61] Aly et al. 2016.2016.
[62] Stalinsky, Steven and R Sosnow, 'Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis, Reaches New Level with Increased Dependence on Apps, Software,' *The Middle East Media Research Institute, Inquiry and Analysis Series Report No. 1168,* 2015.
[63] Graham, Robert, 'How Terrorists Use Encryption,' *CTC Sentinel*, 9(6), 2016. Available at: https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf.
[64] Atwan 2015.
[65] Dunlap, Justine A., 'Intimate Terrorism and Technology; There's an App for That!' University of Massachusetts School of Law, 2014. Available at: https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1028&context=fac_pubs.
[66] Stalinsky Sosnow 2015.
[67] Weimann, Gabriel, 'Going Dark: Terrorism on the Dark Web,' *Studies in Conflict & Terrorism*, 39(3), 2015, pp. 1-24.
[68] Stalinsky, Steven and R. Sosnow, 'Germany-Based Encrypted Messaging App Telegram Emerges as Jihadis' Preferred Communications Platform,' Part V of MEMRI Series: Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis,September 2015-September 2016. *The Middle East Media Research Institute,* Inquiry and Analysis Series Report No. 1291, 2016.
[69] Institute for Policy Analysis of Conflict (IPAC) 2015.
[70] Ibid.
[71] Atwan 2015.
[72] Weimann 2015.
[73] Ahmed, Mubaraz and Fred Lloyd-George, 'A War of Keywords: How Extremists are Exploiting the Internet and what to do about it,' *The Tony Blair Institute for Global Change*, 2017. Available at: https://institute.global/sites/default/files/inline-files/IGC_War%20of%20Keywords_23.08.17_0.pdf.
[74] Stalinsky and Sosnow 2016.
[75] Middle East Media Research Institute (MEMRI), 'Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram,' *MEMRI*, 2017. Available at: https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.
[76] GPT-2 is an open-source unsupervised language model developed by Open AI that generates coherent paragraphs of text, performs reading comprehension, machine translation, question answering, and summarization without task-specific training.
[77] Newhouse, Alex, Jason Blazakis, and Kris McGuffie, 'The Industrialization of Terrorist Propaganda: Neural Language Models and the Threat of Fake Content Generation,' Monterey: Middlebury Institute for International Studies at Monterey, 2019. Available at: https://www.middlebury.edu/institute/sites/www.middlebury.edu.institute/files/2019-

11/The%20Industrialization%20of%20Terrorist%20Propaganda%20-%20CTEC.pdf?fv=TzdJnlDw.

[78] Bodo, Lorand, 'Decentralised Terrorism: The Next Big Step for the So-Called Islamic State (IS)?' *Vox-Pol Blog* (online), 2018. Available at: https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.

[79] Zannettou, Savvas, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivvianos, Gianluca Stringhini, and Jeremy Blackburn, 'What is Gab? A Bastion of Free Speech or an Alt-Right Echo Chamber?' *Computer Science, Cornell University,* March 2018. Available at: https://arxiv.org/abs/1802.05287.

[80] Stevens, Tim, and Peter Neumann, 'Countering Online Radicalisation: A Strategy for Action,' London: International Centre for the Study of Radicalisation (ICSR), 2009. Available at: https://icsr.info/2009/03/16/countering-online-radicalisation-a-strategy-for-action/.

[81] Tech Against Terrorism, 'Project Background (Online),' Tech Against Terrorism, 2017. Available at: https://www.techagainstterrorism.org/project-background/.

[82] Splittgerber, Andreas and Friederike Detmering, 'Germany's new hate speech act in force: what social network providers need to do now,' *Technology Law Dispatch*, 2017. Available at: https://www.technologylawdispatch.com/2017/10/social-mobile-analytics-cloud-smac/germanys-new-hate-speech-act-in-force-what-social-network-providers-need-to-do-now/?utm_content=bufferd5f9a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#page=1.

[83] Ibid.

[84] US Department of Homeland Security, 'Rep. Max Rose Calls for Counterterrorism Budgets from Social Media Companies,' Committee on Homeland Security, 2019. Available at: https://homeland.house.gov/news/correspondence/rep-max-rose-calls-for-counterterrorism-budgets-from-social-media-companies.

[85] US Department of Homeland Security, 'Thomson, Rose: Social Media Companies Must be Transparent about Efforts to Counter Terrorism,' Committee on Homeland Security, 2019. Available at: https://homeland.house.gov/news/press-releases/thompson-rose-social-media-companies-must-be-transparent-about-efforts-to-counter-terrorism.

[86] European Parliament, 'Tackling the dissemination of terrorist content online' (Provisional Edition), European Parliament, 2019. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf?redirect.

[87] Ibid, p. 3.

[88] Lecher, Colin, 'Aggressive New Terrorist Content Regulation Passes EU Vote,' *The Verge,* 17 April 2019. Available at: https://www.theverge.com/2019/4/17/18412278/eu-terrorist-content-law-parliament-takedown.

[89] *Open Letter to the European Parliament,* 8 February 2019. Available at: https://cdt.org/files/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf.

[90] Liptak, Andrew, 'Sri Lanka restricts access to social media sites following terror attack,' *The Verge*, 21 April 2019. Available at: https://www.theverge.com/2019/4/21/18510006/sri-lanka-restricts-access-social-media-sites-facebook-youtube-instagram-whatsapp-terror-attack.

[91] Kapoor, Kanupriya, 'Indonesia Blocks Telegram Messaging Service over Security Concerns,' Reuters, 14 July 2017. Available at: https://www.reuters.com/article/us-indonesia-security-apps-idUSKBN19Z1Q2.

[92] EUROPOL, 'EU Internet Referral Unit - EU IRU,' EUROPOL, 2019. Available at: https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru?page=0,1.

[93] Bickert, Monika., and Brian Fishman, B., 'Hard Questions: How We Counter Terrorism,', Facebook Newsroom, 15 June 2017. Available at: https://about.fb.com/news/2017/06/how-we-counter-terrorism/.
[94] Cruickshank, Paul, 'A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook,' *CTC Sentinel*, 10(8), September 2017. Available at: https://ctc.usma.edu/a-view-from-the-ct-foxhole-an-interview-with-brian-fishman-counterterrorism-policy-manager-facebook/.
[95] Twitter Help Center, 'Terrorism and Violent Extremism Policy,' Twitter Help Centre, 2019.
[96] Ibid.
[97] YouTube Help, 'YouTube Trusted Flagger Program,' YouTube Help, 2019. Available at: https://support.google.com/youtube/answer/7554338?hl=en.
[98] Global Internet Forum to Counter Terrorism (GIFCT), 'Hash Sharing Consortium (Joint Tech Innovation),' GIFCT, 2019.Available at: https://gifct.org/joint-tech-innovation/.
[99] Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.
[100] Paganini, Pierluigi, 'Anonymous Affiliate GhostSec has Supported US Law Enforcement and Intelligence Agencies in Thwarting ISIS Terror Plots in New York and Tunisia,' *Security Affairs,* 2018. Available at: https://securityaffairs.co/wordpress/38860/cyber-crime/ghostsec-thwarts-isis-terror-plots.html.
[101] Steckler, Steve, 'Why Facebook is Losing the War on Hate Speech in Myanmar,' *Reuters,* 2018. Available at: https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.
[102] Ibid.
[103] Peritz, Aki, 'What Whac-A Mole Can Teach Us About How to Fight Terrorism,' *Foreign Policy,* 12 August 2015. Available at: https://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight-terrorism/.
[104] Briggs, Rachel and Sebastian Feve, 'Review of Programs to Counter Narratives of Violent Extremism,' London: Institute for Strategic Dialogue, 2013, p. 6.
See also: Schmid, Alex P., 'Al-Qaeda's 'Single Narrative' and Attempts to Develop Counter-Narratives: The State of Knowledge,' *The International Centre for Counter-Terrorism - The Hague (ICCT),* 2014, p. 1. Available at: https://www.researchgate.net/publication/285546585_Al_Qaeda's_Single_Narrative_and_Attempts_to_Develop_Counter-Narratives.
[105] Zeiger, Sara, 'Undermining Violent Extremist Narratives in East Africa: A How-To Guide,' Abu Dhabi: Hedayah, 2018. Available at: https://www.hedayahcenter.org/resources/reports_and_publications/undermining-violent-extremist-narratives-in-east-africa-a-how-to-guide-2/.
[106] Zeiger, Sara, 'Undermining Violent Extremist Narratives in South East Asia: A How-To Guide,' Abu Dhabi: Hedayah, 2016. Available at: https://hedayah-wp-offload.s3.eu-central-1.amazonaws.com/hedayah/wp-content/uploads/2019/11/17120110/File-3182016115528.pdf ; Elsayed, Lilah, Talal Faris, and Sara Zeiger, 'Undermining Violent Extremist Narratives in the Middle East and North Africa: A How-To Guide,' *Abu Dhabi: Hedayah,* 2017. Available at: https://www.resolvenet.org/index.php/research/publications/undermining-violent-extremist-narratives-middle-east-and-north-africa-how ; Zeiger 2018.
[107] Key, Thomas Martin and Andrew J. Czaplewski, 'Upstream Social Marketing Strategy: An Integrated Marketing Communications Approach,' *Business Horizons,* 60(3), 2017, pp. 325-333.
[108] Zeiger 2018.
[109] Ibid.

[110] Berger, J.M., 'Omar and Me,' *Foreign Policy,* 13 September 2013. Available at: https://foreignpolicy.com/2013/09/17/omar-and-me/.
[111] Ibid.
[112] McDowell-Smith, Allison, Anne Speckhard, and Ahmet S. Yayla, 'Beating ISIS in the Digital Space: Focus Testing ISIS Defector Counter-Narrative Videos with American College Students,' *Journal for Deradicalization,* 10, 2017. Available at: https://journals.sfu.ca/jd/index.php/jd/article/view/83.
[113] International Center for the Study of Violent Extremism (ICSVE), 'Inside ad-Dawlah,' ICSVE, 2017. Available at: https://m.youtube.com/watch?time_continue=17&v=fKw6j-Z9u64.
[114] Associated Press, 'I Cleaned Toilets while in ISIS,' Kalyan Youth Areeb Majeed Tells NIA,' *Times of India,* 30 November 2014. Available at: https://timesofindia.indiatimes.com/india/I-cleaned-toilets-while-in-ISIS-Kalyan-youth-Areeb-Majeed-tells-NIA/articleshow/45328623.cms.
[115] Huey, Laura, 'This is not your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming,' *Journal of Terrorism Research,* 6, 2015.
[116] Ibid.
[117] International Institute of Qur'anic Studies, 'The Divine Grace of Islam Nusantara – Trailer,' International Institute of Qur'anic Studies, 2015; Available at: https://m.youtube.com/watch?time_continue=11&v=aLEi5ED_-Xw.
[118] Associated Press, 'NU Calls for End to word 'Infidels' to describe non-Muslims,' *The Jakarta Post,* 1 March 2019. Available at: https://www.thejakartapost.com/news/2019/03/01/nu-calls-for-end-to-word-infidels-to-describe-non-muslims.html.
[119] Anataban South Sudan, 'Soutna by #Anataban South Sudan Music 2017,' Anataban South Sudan, 2017. Available at: https://m.youtube.com/watch?v=196d9E0Xl_4.
[120] Meleagrou-Hitchens, Alexander and Lorenzo Vidino, 'The Challenges and Limitations of Online Counter-Narratives,' Peace Research Institute Frankfurt [Blog], 2018. Available at: https://blog.prif.org/2018/06/04/the-challenges-and-limitations-of-online-counter-narratives/.
[121] Macnair and Frank 2017.
[122] McDowell-Smith, Speckhard and Yayla 2017.
[123] Silverman, Tanya, Christopher Stewart, Zahed Amanullah, and Jonathan Birdwell, *The Impact of Counter-Narratives*. London: Institute for Strategic Dialogue, 2016; Available at: https://www.isdglobal.org/isd-publications/the-impact-of-counter-narratives/.
[124] Ibid.
[125] Bell, Paul, 'ISIS and Violent Extremism: Is the West's Counter-Narrative Making the Problem Worse?' *Influence Online,* 25 June 2015. Available at: https://influenceonline.co.uk/2015/06/25/isis-violent-extremism-wests-counter-narrative-making-problem-worse/. Ferguson, Kate, 'Countering Violent Extremism through Media and Communication Strategies: A Review of the Evidence,' *Partnership for Conflict, Crime & Security Research*, (PaCCS), 2016. Available at: http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf.
[126] Schmid 2014.
[127] Cottee and Hayward 2011.
[128] Bjelopera, Jerome, 'American Jihadist Terrorism: Combating a Complex Threat,' Washington, DC: Congressional Research Service Report for the U.S. Congress, 2013. Available at: https://fas.org/sgp/crs/terror/R41416.pdf ; Huey 2015
[129] Archetti, Cristina, 'Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age,' *Perspectives on Terrorism,* 9(6), 2015. Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/401.

[130] Gladwell, Malcolm, *The Tipping Point: How Little Things can make a Big Difference*. Boston: Little, Brown, 2000.
[131] Saifudeen, Omer Ali, 'Getting out of the Armchair: Potential Tipping Points for Online Radicalisation'; in: Khader, Majeed (ed.), *Combating Violent Extremism and Radicalization in the Digital Era.* IGI Global, 2016, pp. 129-148.
[132] Archetti 2015.
[133] Ferguson 2016.
[134] Lazer, David M.J., et al., 'The Science of Fake News,' *Science*, 359 6380), 2018, pp. 1094-1096. Available at: https://scholar.harvard.edu/files/mbaum/files/science_of_fake_news.pdf.
[135] United Nations Educational, Scientific and Cultural Organization (UNESCO), '*A Teacher's Guide to Preventing Violent Extremism,'* Paris: UNESCO, 2016. Available at: https://en.unesco.org/sites/default/files/lala_0.pdf.
[136] Paganini, Pierluigi, 'The Role of Technology in Modern Terrorism,' INFOSEC, 2018. Available at: https://resources.infosecinstitute.com/topic/the-role-of-technology-in-modern-terrorism/#gref.
[137] Law, Nancy, David Woo, Jimmy de la Torre, and Gary Wong, 'A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2,' Paris: UNESCO and Centre for Information Technology in Education, 2018. Available at: http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf.
[138] Google, 'Digital Tools to Engage Students in Learning,' Google for Education, 2017. Available at: https://edu.google.com/products/chromebooks/digital-tools/?modal_active=none.
[139] Facebook, 'Digital Literacy Library,' Facebook, 2018.
Available at: https://www.facebook.com/safety/educators.
Available at: https://www.facebook.com/safety/educators
[140] Ahmed and George 2017.
[141] Kasprak, Alex, 'Disgusting Hate: How Radical Evangelicals Spread Anti-Islamic Vitriol on Facebook,' *Snopes*, 15 May 2019. Available at: https://www.snopes.com/news/2019/05/15/radical-evangelical-facebook/.
[142] Ibid.
[143] Ministry of Communication and Information Technology, Government of Indonesia 2010.

Bibliography

Ahmed, Mubaraz and Fred Lloyd-George, 'A War of Keywords: How Extremists are Exploiting the Internet and what to do about it,' The Tony Blair Institute for Global Change, 2017. Available at: https://institute.global/sites/default/files/inline-files/IGC_War%20of%20Keywords_23.08.17_0.pdf.

Al-Rawi, Ahmed, 'Video Games, Terrorism, and ISIS's Jihad 3.0,' *Terrorism and Political Violence*, 30(4), 2018, pp. 740-760.

Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen, 'Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization,' *Studies in Conflict & Terrorism*, Taylor and Francis Online, 2016. Available at: https://www.tandfonline.com/doi/abs/10.1080/1057610X.2016.1157402.

Anataban South Sudan, 'Soutna by #Anataban South Sudan Music 2017,' Anataban South Sudan, 2017. Available at: https://m.youtube.com/watch?v=196d9E0Xl_4.

Archetti, Cristina, 'Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age,' Perspectives on Terrorism, 9(6), 2015. Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/401.

Arquilla, John and David Ronfeldt, Networks and Netwars: The Future of Terror, Crime and Militancy, RAND, 2001. Available at: http://www.rand.org/pubs/monograph_reports/MR1382.html.

Associated Press, 'Christchurch Mosque Shootings: Gunman Livestreamed 17 Minutes of Shooting Terror,' *New Zealand Herald*, 15 March 2019. Available at: https://www.nzherald.co.nz/nz/christchurch-mosque-shootings-gunman-livestreamed-17-minutes-of-shooting-terror/BLRK6K4XBTOIS7EQCZW24GFAPM/.

Associated Press, 'I Cleaned Toilets while in ISIS,' Kalyan Youth Areeb Majeed Tells NIA,' *Times of India*, 30 November, 2014. Available at: https://timesofindia.indiatimes.com/india/I-cleaned-toilets-while-in-ISIS-Kalyan-youth-Areeb-Majeed-tells-NIA/articleshow/45328623.cms.

Associated Press, 'NU Calls for End to word 'Infidels' to describe non-Muslims,' *The Jakarta Post*, 1 March 2019. Available at: https://www.thejakartapost.com/news/2019/03/01/nu-calls-for-end-to-word-infidels-to-describe-non-muslims.html.

Associated Press, 'Swedish Isis fundraiser statuses were on Facebook for two years before deletion,' *The Local*, 25 March 2018. Available at: https://www.thelocal.se/20180325/swedish-isis-fundraiser-statuses-were-on-open-facebook-page-for-two-years-before-deletion.

Atwan, Abdel Bari, Islamic State: The Digital Caliphate. California: University of California Press, 2015.

Bell, Paul, 'ISIS and Violent Extremism: Is the West's Counter-Narrative Making the Problem Worse?' Influence Online, 25 June 2015. Available at: https://influenceonline.co.uk/2015/06/25/isis-violent-extremism-wests-counter-narrative-making-problem-worse/.

Berger, J.M., 'Omar and Me,' *Foreign Policy*, 13 September 2013. Available at: https://foreignpolicy.com/2013/09/17/omar-and-me/.

Bickert, Monika, and Brian Fishman, 'Hard Questions: How We Counter Terrorism,' Facebook Newsroom, 15 June 2017. Available at: https://about.fb.com/news/2017/06/how-we-counter-terrorism/.

Bjelopera, Jerome, 'American Jihadist Terrorism: Combating a Complex Threat,' Washington, DC: Congressional Research Service Report for the U.S. Congress, 2013. Available at: https://fas.org/sgp/crs/terror/R41416.pdf

Bodo, Lorand, ‘Decentralised Terrorism: The Next Big Step for the So-Called Islamic State (IS)?’ Vox-Pol Blog (online), 2018. Available at: https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.

Briggs, Rachel and Sebastian Feve, ‘Review of Programs to Counter Narratives of Violent Extremism,’ London: Institute for Strategic Dialogue, 2013

Bulbeck, Emilia, ‘The Path to Persuasion: An Investigation into how al-Shabab Constructs their Brand in their Digital Magazine Gaidi Mtaani,’ Master’s Thesis, Uppsala University, 2017. Available at: http://uu.diva-portal.org/smash/record.jsf?pid=diva2%3A1148028&dswid=-8240.

Carley, Kathleen, Matthew Dombroski, Max Tsvetovat, Jeffrey Reminga, and Natasha Kamneva, ‘Destabilizing Dynamic Covert Networks’; in: The 8th International Command and Control Research and Technology Symposium, 2003. Available at: http://www.dodccrp.org/events/8th_ICCRTS/pdf/021.pdf.

Christofaro, Beatrice, Michelle Mark and Ellen Cranley, ‘What We Know So Far About Brenton Tarrant, The Suspect in The New Zealand Mosque Shootings,’ *Business Insider*, 2019. Available at: https://www.businessinsider.com/new-zealand-mosque-shoote.rs-what-we-know-2019-3?r=US&IR=T.

Conway, Maura, ‘From al-Zarqawi to al-Awlaki: The Emergence and Development of an Online Radical Milieu,’ *Combatting Terrorism Exchange*, 2(4), 2012, pp. 12-22.

Conway, Maura, ‘Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research’; in: Anne. Aly, Stuart Macdonald, Lee Jarvis and Thomas. Chen (eds.), *Violent extremism online: New perspectives on terrorism and the Internet*. Abingdon: Routledge, 2016, pp. 123-148.

Conway, Maura, Jodie Parker, and Sean Looney, ‘Online Jihadi Instructional Content: The Role of Magazines’; in: Conway, Maura. et al. (eds.), *Terrorists’ Use of the Internet: Assessment and Response. NATO Science for Peace and Security Series – E: Human and Societal Dynamics (136).* Amsterdam: IOS Press, 2017, pp. 182-193.

Cottee, Simon and Keith J. Hayward, ‘Terrorist (E)motives: The Existential Attractions of Terrorism,’ Studies in Conflict & Terrorism, 34(12), 2011, pp. 963-986.

Counter Extremism Project (CEP), ‘Extremists: Aqsa Mahmood,’ CEP, 2016. Available at: https://www.counterextremism.com/extremists/aqsa-mahmood.

Cruickshank, Paul, ‘A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook,’ *CTC Sentinel*, 10(8), September 2017. Available at: https://ctc.usma.edu/a-view-from-the-ct-foxhole-an-interview-with-brian-fishman-counterterrorism-policy-manager-facebook/.

Cruickshank, Paul and Mohannad Hage Ali, ‘Abu Musab Al Suri: Architect of the New Al Qaeda,’ *Studies in Conflict & Terrorism*, 30, 2007, pp. 1-14.

Dunlap, Justine A., ‘Intimate Terrorism and Technology; There’s an App for That!’ University of Massachusetts School of Law, 2014. Available at: https://scholarship.law.umassd.edu/cgi/viewcontent.cgi?article=1028&context=fac_pubs.

Elsayed, Lilah, Talal Faris, and Sara Zeiger, ‘Undermining Violent Extremist Narratives in the Middle East and North Africa: A How-To Guide,’ Abu Dhabi: Hedayah, 2017. Available at: https://www.resolvenet.org/index.php/research/publications/undermining-violent-extremist-narratives-middle-east-and-north-africa-how.

European Parliament, ‘Tackling the dissemination of terrorist content online’ (Provisional Edition), European Parliament, 2019. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf?redirect.

EUROPOL, ‘EU Internet Referral Unit - EU IRU,’ EUROPOL, 2019. Available at: https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru?page=0

Facebook, ‘Digital Literacy Library,’ Facebook, 2018. Available at:

https://www.facebook.com/safety/educators.

Facebook Newsroom, 17 March 2019. Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.

Ferguson, Kate, 'Countering Violent Extremism through Media and Communication Strategies: A Review of the Evidence,' Partnership for Conflict, Crime & Security Research, (PaCCS), 2016. Available at: http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf.

Gladwell, Malcolm, *The Tipping Point: How Little Things Can Make a Big Difference*. Boston: Little, Brown, 2000.

Global Internet Forum to Counter Terrorism (GIFCT), 'Hash Sharing Consortium (Joint Tech Innovation),' GIFCT, 2019. Available at: https://gifct.org/joint-tech-innovation/.

Google, 'Digital Tools to Engage Students in Learning,' Google for Education, 2017. Available at: https://edu.google.com/products/chromebooks/digital-tools/?modal_active=none.

Graham, Robert, 'How Terrorists Use Encryption,' *CTC Sentinel*, 9(6), 2016. Available at: https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf.

Graham-McLay, Charlotte, 'Death Toll in New Zealand Mosque Shootings Rise to 51,' *The New York Times,* 2 May 2019. Available at: https://www.nytimes.com/2019/05/02/world/asia/new-zealand-attack-death-toll.html.

Gunaratna, Rohan, and Cleo Haynal, 'Current and Emerging Threats of Homegrown Terrorism: The Case of the Boston Bombings,' *Perspectives on Terrorism*, 7(3), 2013, pp. 44-63.

Hamm, Mark, 'Apocalyptic Violence: The Seduction of Terrorist Subcultures,' *Theoretical Criminology*, 8(3), 2004, pp. 323-339.

Hedayah, 'Introduction to Countering Violent Extremism'. Abu Dhabi: Hedayah.

Hemmingsen, Ann-Sophie and Karin-Ingrid Castro, 'The Trouble with Counter-Narratives,*' Copenhagen: Danish Institute for International Studies,* 2019. Available at: https://pure.diis.dk/ws/files/784884/DIIS_RP_2017_1.pdf.

Huey, Laura, 'This is not your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming,' *Journal of Terrorism Research*, 6, 2015.

Institute for Policy Analysis of Conflict (IPAC), 'Online Activism and Social Media Usage Among Indonesian Extremists,' IPAC Report No. 24, 2015. Available at: http://file.understandingconflict.org/file/2015/10/IPAC_24_Online_Activism_Social_Media.pdf.

International Center for the Study of Violent Extremism (ICSVE), 'Inside ad-Dawlah,' ICSVE, 2017. Available at: https://m.youtube.com/watch?time_continue=17&v=fKw6j-Z9u64.

International Institute of Qur'anic Studies, 'The Divine Grace of Islam Nusantara – Trailer,' International Institute of Qur'anic Studies, 2015. Available at: https://m.youtube.com/watch?time_continue=11&v=aLEi5ED_-Xw.

Kapoor, Kanupriya, 'Indonesia Blocks Telegram Messaging Service over Security Concerns,' Reuters, 14 July 2017. Available at: https://www.reuters.com/article/us-indonesia-security-apps-idUSKBN19Z1Q2.

Kasprak, Alex, 'Network of Islamophobic Facebook Pages Exposed by Snopes Goes Dark,' *Snopes*, 2019. Available at: https://www.snopes.com/news/2019/05/26/fb-islamophobic-network-down/.

Kasprak, Alex, 'Disgusting Hate: How Radical Evangelicals Spread Anti-Islamic Vitriol on Facebook,' Snopes, 15 May 2019. Available at: https://www.snopes.com/news/2019/05/15/radical-evangelical-facebook/.

Kernan, Erik R., ‘The Islamic State as a Unique Social Movement: Exploiting Social Media in an Era of Religious Revival,’ Honors Thesis, University of Vermont, 2017. Available at: https://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1227&context=hcoltheses.

Key, Thomas Martin and Andrew J. Czaplewski, ‘Upstream Social Marketing Strategy: An Integrated Marketing Communications Approach,’ *Business Horizons,* 60(3), 2017, pp. 325-333.

Koch, Ariel, ‘Jihadi Beheading Videos and their Non-Jihadi Echoes,’ *Perspectives on Terrorism,* 12(3), 2018, pp. 24-34.

Law, Nancy, David Woo, Jimmy de la Torre, and Gary Wong, ‘A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2,’ Paris: UNESCO and Centre for Information Technology in Education, 2018. Available at: http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf.

Lazer, David. M.J., et al., ‘The Science of Fake News,’ Science, 359(6380), 2018, pp. 1094-1096. Available at: https://scholar.harvard.edu/files/mbaum/files/science_of_fake_news.pdf

Lecher, Colin, ‘Aggressive New Terrorist Content Regulation Passes EU Vote,’ The Verge, 17 April 2019. Available at: https://www.theverge.com/2019/4/17/18412278/eu-terrorist-content-law-parliament-takedown.

Levitt, Matthew, ‘How do ISIS Terrorists Finance Their Attacks?’ The Hill, 2015. Available at: http://thehill.com/blogs/pundits-blog/homeland-security/260597-how-do-isis-terrorists-finance-their-attacks.

Liptak, Andrew, ‘Sri Lanka restricts access to social media sites following terror attack,’ The Verge, 21 April 2019. Available at: https://www.theverge.com/2019/4/21/18510006/sri-lanka-restricts-access-social-media-sites-facebook-youtube-instagram-whatsapp-terror-attack.

Lombardi, Marco, ‘IS 2.0 and Beyond: The Caliphate’s Communication Project’; in: Maggioni, Monica and Paolo Magri (eds.), *Twitter and Jihad: The Communication Strategy of ISIS*. ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.

Macdonald, Stuart, ‘Terrorist Narratives and Communicative Devices: Findings from a Study of Online Terrorist Magazines’; in: Zeiger, Sara (ed.), *Expanding Research on Countering Violent Extremism*. Abu Dhabi/Perth: Hedayah/Edith Cowan University, 2016, pp. 127-141.

Macnair, Logan, and Richard Frank, ‘Voices Against Extremism: A Case Study of a Community Based CVE Counter-Narrative Campaign,’ *Journal for Deradicalization*, 10, 2017, pp. 147-174.

Macnair, Logan, and Richard Frank, ‘Changes and Stabilities in the Language of Islamic State

Magazines: A Sentiment Analysis,’ Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide, 11(2), 2018, pp. 109- 120.

Madhani, Aamer, ‘Cleric al-Awlaki dubbed ‘bin Laden of the Internet’,’ *USA Today*, 2011. Available at: http://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm.

Madrazo, Andrea, ‘Recruiting Followers for the Caliphate: A Narrative Analysis of Four Jihadist Magazines,’ Master’s Thesis, University of Central Florida, 2018. Available: https://stars.library.ucf.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=6786&context=etd.

Maggioni, Monica, ‘The Islamic State: Not That Surprising, If You Know Where to Look’; in: Maggioni, Monica and Paolo Magri, (eds.), *Twitter and Jihad: The Communication*

Strategy of ISIS. ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.

Mair, David, '#Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack,' *Studies in Conflict & Terrorism*, 40 (1), 2017, pp. 24-43.

McDowell-Smith, Allison, Anne Speckhard,and Ahmet S. Yayla, 'Beating ISIS in the Digital Space: Focus Testing ISIS Defector Counter-Narrative Videos with American College Students,' *Journal for Deradicalization*, 10, 2017. Available at: https://journals.sfu.ca/jd/index.php/jd/article/view/83.

Meleagrou-Hitchens, Alexander. and Lorenzo Vidino, 'The Challenges and Limitations of Online Counter-Narratives,' Peace Research Institute Frankfurt [Blog], 2018. Available at: https://blog.prif.org/2018/06/04/the-challenges-and-limitations-of-online-counter-narratives/.

Middle East Media Research Institute (MEMRI), 'Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram,' MEMRI, 2017. Available at: https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.

Ministry of Communication and Information Technology, Government of Indonesia, *Trust Positif*, 2010; Available at: https://trustpositif.kominfo.go.id/

Newhouse, Alex, Jason Blazakis, and Kris McGuffie, 'The Industrialization of Terrorist Propaganda: Neural Language Models and the Threat of Fake Content Generation,' Monterey: Middlebury Institute for International Studies at Monterey, 2019. Available at: https://www.middlebury.edu/institute/sites/www.middlebury.edu.institute/files/2019-11/The%20Industrialization%20of%20Terrorist%20Propaganda%20-%20CTEC.pdf?fv=TzdJnlDw.

Nissen, Thomas Elkjer, 'Terror.com: IS's Social Media Warfare in Syria and Iraq,' *Contemporary Conflicts: Military Studies Journal*, 2(2), 2014, pp. 1-8.

Nohria, Nitin and Robert Eccles, *Networks and Organizations: Structure, Form and Action.* Boston: Harvard Business School Press, 1992.

Open Letter to the European Parliament, 8 February 2019. Available at: https://cdt.org/files/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf.

Paganini, Pierluigi, 'Anonymous Affiliate GhostSec has Supported US Law Enforcement and Intelligence Agencies in Thwarting ISIS Terror Plots in New York and Tunisia,' Security Affairs, 2018. Available at: https://securityaffairs.co/wordpress/38860/cyber-crime/ghostsec-thwarts-isis-terror-plots.html

Paganini, Pierluigi, 'The Role of Technology in Modern Terrorism,' INFOSEC, 2018. Available at: https://resources.infosecinstitute.com/topic/the-role-of-technology-in-modern-terrorism/#gref

Peritz, Aki, 'What Whac-A Mole Can Teach Us About How to Fight Terrorism,' *Foreign Policy*, 12 August 2015. Available at: https://foreignpolicy.com/2015/08/12/what-whac-a-mole-can-teach-us-about-how-to-fight-terrorism/.

Perliger, Arie, 'Terrorist Networks' Productivity and Durability: A Comparative Multi-level Analysis,' *Perspectives on Terrorism*, 8(4), 2014, pp. 36-52.

Pirang, Alexander, 'New EU Regulation: Upload Filter Against Terrorist Content?' *Alexander von Humbold Institut für Internet und Gesellschaft Online*, 2019. Available at: https://www.hiig.de/en/new-eu-regulation-upload-filter-against-terrorist-content/.

Plebani, Andrea and Paolo Maggiolini, 'The Centrality of the Enemy in al-Bahdadi's Caliphate' in: Maggioni, Monica and Paolo Magri (eds.) *Twitter and Jihad: The Communication Strategy of ISIS*, ISPI Report. Milan: Italian Institute for International Political Studies (ISPI), 2015.

Porter, Jon, ‘Upload Filters and One-Hour Takedowns: The EU’s Latest Fight against Terrorism Online Explained,’ *The Verge*, 2019. Available at: https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu.

Red Alert, ‘Implement Hierarchy Reconstructing Methods,’ Eötvös Loránd University et al., 2019. Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c3b41079&appId=PPGMS.

Reed, Alastair, ‘An Inconvenient Truth: Countering Terrorist Narratives – Fighting a Threat We Do Not Understand,’ The International Counter-Terrorism Centre –The Hague (ICCT), 2018. Available at: https://icct.nl/publication/an-inconvenient-truth-countering-terrorist-narratives-fighting-a-threat-we-do-not-understand/.

Saifudeen, Omer Ali, ‘Getting out of the Armchair: Potential Tipping Points for Online Radicalisation’ in: Khader, Majeed. (ed.), *Combating Violent Extremism and Radicalization in the Digital Era*. IGI Global, 2016, pp. 129-148.

Scheufele, Dietram A., and Nicole M. Krause, ‘Science Audiences, Misinformation, and Fake News,’ *Proceedings of the National Academy of Sciences of the United States of America*, 116 (16), 2019, pp. 7662-7669.

Schmid, Alex P., ‘Al-Qaeda’s ‘Single Narrative’ and Attempts to Develop Counter-Narratives: The State of Knowledge,’ The International Centre for Counter-Terrorism - The Hague (ICCT), 2014, p. 1. Available at: https://www.researchgate.net/publication/285546585_Al_Qaeda’s_Single_Narrative_and_Attempts_to_Develop_Counter-Narratives.

Shajkovci, Ardian, ‘Engaging English Speaking Facebook Users in an Anti-ISIS Awareness Campaign,’ *Journal of Strategic Security*, 11(3), 2018, pp. 52-78.

Silverman, Tanya, Christopher Stewart, Zahed Amanullah, and Jonathan Birdwell, ‘The Impact of Counter-Narratives,’ London: Institute for Strategic Dialogue, 2016. Available at: https://www.isdglobal.org/isd-publications/the-impact-of-counter-narratives/

Speckhard, Anne and Adrian Shajkovci, ‘PERSPECTIVE: Challenges in Creating, Deploying Counter-Narratives to Deter Would-be Terrorists,’ *GTSC Homeland Security Today*, 2018. Available at: https://www.hstoday.us/subject-matter-areas/terrorism-study/perspective-challenges-in-creating-deploying-counter-narratives-to-deter-would-be-terrorists/.

Splittgerber, Andreas and Friederike Detmering, ‘Germany’s new hate speech act in force: what social network providers need to do now,’ Technology Law Dispatch, 2017. Available at: https://www.technologylawdispatch.com/2017/10/social-mobile-analytics-cloud-smac/germanys-new-hate-speech-act-in-force-what-social-network-providers-need-to-do-now/?utm_content=bufferd5f9a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#page=1.

Stalinsky, Steven and R. Sosnow, ‘Encryption Technology Embraced by ISIS, Al-Qaeda, Other Jihadis, Reaches New Level with Increased Dependence on Apps, Software,’ *The Middle East Media Research Institute, Inquiry and Analysis Series*, Report No. 1168, 2015.

Stalinsky, Steven and R. Sosnow, ‘Germany-Based Encrypted Messaging App Telegram Emerges as Jihadis’ Preferred Communications Platform,’ Part V of MEMRI Series: Encryption Technology Embraced By ISIS, Al-Qaeda, Other Jihadis, September 2015-September 2016. The Middle East Media Research Institute, Inquiry and Analysis Series Report No. 1291, 2016.

Steckler, Steve, ‘Why Facebook is Losing the War on Hate Speech in Myanmar,’ Reuters, 2018. Available at: https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

Stevens, Tim, and Peter Neumann, ‘Countering Online Radicalisation: A Strategy for Action,’ London: International Centre for the Study of Radicalisation (ICSR), 2009. Available at: https://icsr.info/2009/03/16/countering-online-radicalisation-a-strategy-for-action/.

Sunde, Hans Myhre, ‘Stories, Style and Radicalization: A Cultural and Narrative Criminological Study of Jihadi Propaganda Magazines,’ Master’s Thesis, University of Oslo, 2017. Available at: https://www.duo.uio.no/bitstream/handle/10852/57541/Masteroppgave_HMSUNDE.pdf?sequence=1&isAllowed=y.

Tech Against Terrorism, ‘Project Background (Online),’ Tech Against Terrorism, 2017. Available at: https://www.techagainstterrorism.org/project-background/.

Twitter Help Center, ‘Terrorism and Violent Extremism Policy,’ Twitter Help Centre, 2019. https://transparency.twitter.com/content/dam/transparency-twitter/download/2019-jul-dec/Twitter_Transparency-Rules_Enforcement_Jul-Dec-2019.pdf

United Nations Educational, Scientific and Cultural Organization (UNESCO), ‘A Teacher’s Guide to Preventing Violent Extremism,’. Paris: UNESCO, 2016. Available at: https://en.unesco.org/sites/default/files/lala_0.pdf.

US Department of Homeland Security, ‘Rep. Max Rose Calls for Counterterrorism Budgets from Social Media Companies,’ Committee on Homeland Security, 2019. Available at: https://homeland.house.gov/news/correspondence/rep-max-rose-calls-for-counterterrorism-budgets-from-social-media-companies.

US Department of Homeland Security, ‘Thomson, Rose: Social Media Companies Must be Transparent about Efforts to Counter Terrorism,’ Committee on Homeland Security, 2019. Available at: https://homeland.house.gov/news/press-releases/thompson-rose-social-media-companies-must-be-transparent-about-efforts-to-counter-terrorism.

Waters, Gregory, and Robert Postings, ‘Spiders of the Caliphate: Mapping the Islamic State‘s Global Support Network on Facebook,’ Counter Extremism Project (CEP) Report, 2018.

We Are Social, ‘Digital in 2019,’ We Are Social, 2019. Available at: https://wearesocial.com/global-digital-report-2019.

Weimann, Gabriel, ‘Going Dark: Terrorism on the Dark Web,’ *Studies in Conflict & Terrorism,* 39(3), 2015, pp. 1-24.

Weis, Caleb, ‘Philippines-based Jihadist Groups Pledge Allegiance to the Islamic State,’ FDD, *Long War Journal*, 2016. Available at: https://www.longwarjournal.org/archives/2016/02/philippines-based-jihadist-groups-pledge-allegiance-to-the-islamic-state.php.

Withnall, Adam, ‘Were Paris Attacks the First Case of al-Qaeda and ISIS Working Together? Six Questions Raised in Aftermath of France Shootings,’ *The Independent*, 2015. Available at: http://www.independent.co.uk/news/world/europe/were-paris-attacks-the-first-case-of-al-qaeda-and-isis-working-together-six-questions-raised-in-9975349.html.

Xu, Jie, Daning Hu, and Hsinchun Chen, ‘The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad,’ *Journal of Homeland Security and Emergency Management,* 6(1), 2009, pp. 1-33.

Yang, Chih-Hsiang, Jaclyn P. Maher, and David E. Conroy, ‘Implementation of Behavior Change Techniques in Mobile Applications for Physical Activity’, *American Journal of Preventive Medicine,* 48(4), 2015, pp. 452-455. Available at: https://pubmed.ncbi.nlm.nih.gov/25576494/.

YouTube Help, ‘YouTube Trusted Flagger Program,’ YouTube Help, 2019. Available at: https://support.google.com/youtube/answer/7554338?hl=en.

Zanini, Michele and Sean. J.A. Edwards, ‘The Networking of Terror in the Information Age,’; in: Arquilla, John and David Ronfeldt (eds.), Networks and Netwars: The Future of Terror, Crime, and Militancy, RAND, 2001, ch. 2. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

Zannettou, Savvas, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivvianos, Gianluca Stringhini, and Jeremy Blackburn, ‘What is Gab? A Bastion of Free Speech or an Alt-Right Echo Chamber?’ Computer Science, Cornell University, March 2018. Available at: https://arxiv.org/abs/1802.05287.

Zeiger, Sara, ‘Undermining Violent Extremist Narratives in South East Asia: A How-To Guide,’ Abu Dhabi: Hedayah, 2016. Available at: https://hedayah-wp-offload.s3.eu-central-1.amazonaws.com/hedayah/wp-content/uploads/2019/11/17120110/File-3182016115528.pdf.

Zeiger, Sara, Undermining Violent Extremist Narratives in East Africa: A How-To Guide,’ Abu Dhabi: Hedayah, 2018. Available at: https://www.hedayahcenter.org/resources/reports_and_publications/undermining-violent-extremist-narratives-in-east-africa-a-how-to-guide-2