Literature review

The impact of digital communications technology on radicalization and recruitment

ALEXANDER MELEAGROU-HITCHENS, AUDREY ALEXANDER AND NICK KADERBHAI

Introduction

In 1998, David Duke, the figurehead of America's white supremacist movement, wrote that the internet would help to 'facilitate a worldwide revolution of White awareness' by circumventing the mainstream media.[1] Years later, in 2006, global jihad strategist Abu Mus'ab al-Suri argued that Al-Qaeda's 'informational resistance' against the West must be 'conducted through the use of modern technology of all forms, especially satellite and the Internet'.[2] Worlds away from each other, Duke and Al-Suri shared a vision for their respective movements: if used effectively, contemporary media technologies were the key to success.

With the rise of right-wing and jihadist movements, the current security climate drives the demand for insights into the complex and evolving ventures of violent extremists in the digital sphere. While it is undeniable that extremist groups across the ideological spectrum have identified digital communications technologies as an important resource, the precise impact of these mediums remains unclear. Consequently, this article presents a literature review to provide an up-to-date assessment of the role of digital communications in the processes of radicalization and recruitment.

By surveying existing research, the review strives to interrogate three central questions vexing policy-makers, law enforcement officials, and academics.

- **Question 1:** What is the relationship between violent extremists and communications technology?
- **Question 2:** Have digital communications technologies transformed radicalization and recruitment dynamics?
- **Question 3:** Can social dynamics in the digital sphere replace, or have a similar impact to, those in the physical world among extremist groups and their sympathizers?

After providing clarification and context, the following sections will draw on works that investigate the relationship between media communications and violent radicalization and recruitment. First, this review will examine the connec-

[1] Anti-Defamation League, *Poisoning the web: hatred online* (New York, 1999).
[2] Abu Musab al-Suri, *The call for global Islamic resistance* (2006), p. 857.

International Affairs **93**: 5 (2017) 1233–1249; DOI: 10.1093/ia/iix103

tion between violent extremists and communications technology, laying the groundwork for a nuanced discussion of the effect of digital communications technologies on radicalization and recruitment. Next, this review will address the possibility of the digital sphere replacing the physical world among violent extremists and their followers. Finally, after summarizing key findings, the authors will identify questions that require further examination.

Clarification and context

Before analysing the relevant literature, it is useful to contextualize the issue at hand, identify caveats and clarify key terminology. First and foremost, it is important to underline that the presence of extreme and violent actors in the digital sphere is not unique to the global jihad movement or to the twenty-first century; American neo-Nazis first realized the potential of the web as early as 1983.[3] Reflecting this, the predominant research on extremists' use of communications technology tends to fall into two camps, the global jihad movement and the far right.

A surge of research met the rise of home-grown jihadist terrorism in the West and the influx of foreign fighters into Iraq and Syria, as analysts sought to understand how digital communication technologies, namely the internet, affect the proliferation of extremist activity. The bulk of analysis on this phenomenon emerged in the last decade in the form of books, journal articles, reports and testimony from governmental hearings, allowing a range of actors, from academics to policy-makers, to address the issue. The subject is embedded within a diverse array of disciplines, methodologies and data. Consequently, comparative observations must account for the context within which they occur.

To address necessary caveats, several terms require additional consideration. First, it is crucial to identify the scope of the digital sphere and highlight its intersection with broader radicalization and recruitment trends. Although this nexus is colloquially known as 'online radicalization' among theorists and practitioners in the field, the authors are wary of confining the conversation to pre-existing constructs. Rather than interrogating the online space exclusively, this review considers the impact of digital communications technologies, including, but not limited to, the internet, email, mobile phones, messaging, apps and physical digital media such as flash drives.

Much like 'terrorism' and 'extremism', the precise definition of 'radicalization' is contested among scholars and practitioners. According to Anthony Richards, the concepts of 'terrorism', 'radicalization' and 'extremism' have 'merged into a single discursive framework', blurring the scope of counterterrorism efforts.[4] Ultimately, the main fault-lines in the broader debate emerge around the connec-

[3] George Michael, 'The new media and the rise of exhortatory terrorism', *Strategic Studies Quarterly*, vol. 40, Spring 2013, p. 43.

[4] Anthony Richards, 'From terrorism to "radicalization" to "extremism": counterterrorism imperative or loss of focus?', *International Affairs* 91: 2, 2015, p. 317.

tions between radicalization and violence as well as beliefs and behaviours.[5] Some suggest that radicalization is a 'process' that leads towards increased preparation or commitment to inter-group violence.[6] Other definitions regard radicalization as the adoption of extremist ideas that are in conflict with liberal democratic values, while calling for far-reaching changes to society that may or may not lead to violent action.[7] Alex Schmid succinctly notes that radicalization is 'a very problematic concept'.[8] Given the politicized divisions over the causes of terrorism, such confusion and debate over the term are likely to continue. Rather than pinning down one particular interpretation, this review embraces the semantic fluidity of the term 'radicalization' which allows the authors to pull from a broad swath of research.

To compound the problems posed by elusive terminology, there is little consensus on the preconditions and precipitants of radicalization. Existing theories and models cite various explanations for what causes it. Though beyond the scope of this review, many theories are divided between a top-down and a bottom-up process. Top-down approaches critically focus on the role of an external radicalizer, often a recruiter for a terrorist group or a religious figure with extremist sympathies.[9] Bottom-up theories, however, argue that radicalization derives from an individual's interaction in physical social networks.[10] Both approaches take into account the effect of the internet. In addition, many top-down and bottom-up theories provide sequential or stage-based models that present radicalization as a linear progression.[11] However, the theories that avoid both the sequential approach and the strict division between bottom-up and top-down are the most compelling.[12] As the focus of this review is on the role of digital communications, the following sections unpack and assess views on how different methods of digital communication impact the aforementioned dynamics of radicalization and recruitment.

[5] Peter Neumann, 'The trouble with radicalization', *International Affairs* 89: 4, 2013, pp. 873–93 at p. 873; Manni Crone, 'Radicalization revisited: violence, politics and the skills of the body', *International Affairs* 92: 3, 2016, pp. 587–604.

[6] Donatella Della Porta and Gary LaFree, 'Processes of radicalisation and de-radicalisation', *International Journal of Conflict and Violence* 6: 1, 2012, pp. 4–10; Clark McCauley and Sophia Moskalenko, 'Mechanisms of political radicalization: pathways toward terrorism', *Terrorism and Political Violence* 20: 3, 2008, pp. 415–33 at p. 416.

[7] Algemene Inlichtingen- en Veiligheidsdienst, *Violent jihad in the Netherlands: current trends in the Islamist terrorist threat* (The Hague, 2006); Danish Security and Intelligence Service, *Radikalisering og terror*, 2008; Royal Canadian Mounted Police, *Radicalization: a guide for the perplexed*, June 2009.

[8] Alex Schmid, *Radicalisation, de-radicalisation, counter-radicalisation: a conceptual discussion and literature review*, International Centre for Counter-Terrorism research paper, March 2013, p. 6.

[9] Danish Security and Intelligence Service, *Radikalisering og terror*; Bruce Hoffman, 'The myth of grass-roots terrorism', *Foreign Affairs* 87: 3, May–June 2008; Bruce Hoffman, 'How can I miss you if you won't go away?', *The National Interest*, 1 Oct. 2010.

[10] Marc Sageman, *Understanding terror networks* (Philadelphia: University of Pennsylvania Press, 2004); Arvin Bhatt and Mitchell Silber, *Radicalization in the West: the homegrown threat*, New York Police Department Intelligence Division, 2007.

[11] Randy Borum, 'Understanding the terrorist mind-set', *FBI Law Enforcement Bulletin* 72: 7, July 2003, pp. 7–10; Fathali Moghaddam, 'The staircase to terrorism: a psychological exploration', *American Psychologist* 60: 2, 2005, pp. 161–9; Bhatt and Silber, 'Radicalization in the West'; Thomas Precht, *Home grown terrorism and Islamist radicalization in Europe: from conversion to terrorism*, Danish Ministry of Defence, Dec. 2007.

[12] Quintan Wiktorowicz, *Radical Islam rising: Muslim extremism in the West* (Lanham, MD: Rowman and Littlefield, 2005); Tinka Veldhuis and Jørgen Staun, *Islamist radicalisation: a root cause model*, Netherlands Institute of International Relations Clingendael, Oct. 2009.

Question 1: What is the relationship between violent extremists and communications technologies?

There is a broad consensus that communications technologies offer tremendous opportunities to those who seek to change the status quo. Within the scope of radicalization and recruitment literature, researchers examine and compare various actors' use of platforms. Throughout history, participants in opposition movements have opportunistically exploited contemporary media to engage with their respective audiences. The French Revolution used pamphlets, while the 1917 Russian Revolution preferred posters. Similarly, the Iranian Revolution used cassette tapes, and the Arab Spring used Twitter. Although this is a vast oversimplification of the relationship between media and resistance movements, it illustrates the way in which organizations can use different media to reach their target audiences.

In *Insurgent archipelago*, John Mackinlay expands on this tendency, stating that 'insurgents exploited whatever resources lay to hand, their actions and reactions following a consistent logic by which they focused their insurgent energy into whatever gaps and opportunities were afforded by the environment'.[13] Mackinlay argues that 'the techniques of an insurgency evolve with the societies from which it arises'.[14] In a globalized world with a wealth of digital communications technologies, it is only natural that violent extremists also seek to optimize their influence across various platforms. To understand this dynamic, it is necessary to review research on the most relevant channels and highlight extremists' propensity to change over time.

Most notably, since the advent of the internet, terrorist communications have evolved exponentially. The phrase 'web 2.0' is commonly used to refer to the internet's transition over the last decade and a half into a platform which encompasses 'a growing array of interactive communications systems facilitated by a rapidly expanding set of platforms'.[15] This development has seen the advent of 'numerous websites, blogs, forums and message boards'[16] and, most recently, applications (or 'apps') and instant messaging services.

Websites

Although American white nationalist Louis Beam is credited with pushing the right-wing extremist movement in America 'from the age of the Xerox to the age of the computer', Donald Black set a new precedent after creating Stormfront, 'one of the most prominent extremist sites on the World Wide Web'.[17]

[13] John Mackinlay, *The insurgent archipelago: from Mao to Bin Laden* (New York: Columbia University Press, 2009), p. 44.
[14] Mackinlay, *The insurgent archipelago*, p. 5.
[15] John Curtis Amble, 'Combating terrorism in the new media environment', *Studies in Conflict and Terrorism* 35: 5, 2012, pp. 339–53 at p. 339.
[16] Benjamin Ducol, 'Uncovering the French-speaking jihadisphere: an exploratory analysis', *Media, War and Conflict* 5: 1, 2012, pp. 51–70 at p. 51.
[17] Joseph Schafer, 'Spinning the web of hate: web-based hate propagation by extremist organisations', *Journal of Criminal Justice and Popular Culture* 9: 2, 2002, pp. 69–88 at p. 69; Jeffrey Kaplan and Leonard Weinberg, *The*

Among jihadists, some ideologues and their respective hierarchical groups created official, top-down websites as a way to communicate their goals and collective grievances through a cost-effective and uncensored global platform.[18] Such websites commonly shared ideological and tactical documents and facilitated contact among like-minded sympathizers without significant surveillance by law enforcement.[19] In the process, extremists preserved records over time by storing the documents produced as archives or databases.[20]

Traditional, hierarchical websites that have controversial or violent histories are now in decline. This decline is due to a combination of the sites being blocked or taken down, growing concerns over government surveillance among users, and a general shift to other platforms, including social media.[21] The turn away from dynamic terrorist websites also fuelled the rise of static websites. Static websites produce a subtler narrative that slowly and more implicitly escalates in rhetoric, eventually pushing the user into more hard-line and extremist views.[22] In the context of far-right movements, often these narratives use fictional storytelling as a way of promoting their vision.[23] The power of storytelling lies in its ability to 'make an argument without eliciting mental resistance'[24] which leads to fewer counter-arguments and less resistance to persuasion.[25]

Extremist forums and chat rooms

For jihadist organizations, extremist forums and chat rooms replaced static websites as the main platforms from which to spread jihadist propaganda and create online networks.[26] As the platforms evolved, strategies for outreach evolved in tandem; jihadist propaganda turned away from Arabic language content towards English,[27] and consequently became accessible to a more global audience.[28] Online forums and chat rooms allow members of extremist movements to interact with each

emergence of a Euro-American radical right (New Brunswick, NJ: Rutgers University Press, 1998), p. 160.

[18] Aaron Zelin, *The state of global jihad online*, New America Foundation, Washington DC, 2013; Peter Neumann, *Countering online radicalization in America*, Bipartisan Policy Centre, Washington DC, 2012, p. 16.

[19] Schafer, 'Spinning the web of hate', p. 69.

[20] Donatella Della Porta and Lorenzo Mosca, 'Searching the net: web sites' qualities in the global justice movement', *Information, Communication and Society* 12: 6, 2009, pp. 771–92 at p. 777.

[21] Ghaffar Hussain and Erin Saltman, *Jihad trending: a comprehensive analysis of online extremism and how to counter it*, Quilliam, London, 2014, p. 32; Zelin, 'The state of global jihad online', p. 5.

[22] Hussain and Saltman, *Jihad trending*, p. 32; Anthony Bergin, Sulastri Osman, Carl Ungerer, and Nur Yasin, *Countering internet radicalisation in southeast Asia*, Australian Strategic Policy Institute Special Report 22, 2009, p. 7.

[23] Elissa Lee and Laura Leets, 'Persuasive storytelling by hate groups online: examining its effects on adolescents', *American Behavioural Scientist* 45: 6, 2002, pp. 927–57; Megan McDonald, 'Cyberhate: extending persuasive techniques of low credibility sources to the world wide web', in David Schumann and Esther Thorson, eds, *Advertising and the world wide web* (Mahwah, NJ: Lawrence Erlbaum, 1999).

[24] Shems Friedlander, *When you hear hoofbeats think of a zebra* (Costa Mesa, CA: Mazda, 1992).

[25] Michael Slater, 'Processing social information in messages: social group familiarity, fiction vs. non-fiction, and subsequent beliefs', *Communication Research* 17: 3, June 1990, pp. 327–43.

[26] Gilbert Ramsay, 'Conceptualising online terrorism', *Perspectives on Terrorism* 2: 7, 2008, pp. 3–10; Zelin, *The state of global jihad online*, p. 5.

[27] Akil Awan, 'Radicalization on the internet? The virtual propagation of jihadist media and its effects', *The RUSI Journal* 152: 3, June 2007, pp. 71–86 at p. 76.

[28] Ducol, 'Uncovering the French-speaking jihadisphere', p. 52.

other, discuss political and other current events and bond as a cohort in ways that traditional websites could not accommodate.

Aaron Zelin's 2013 analysis of jihadist forums suggests that the proliferation of these platforms may be context-specific, as English-language jihadist forums were far less active than their Arabic counterparts. Nonetheless, Zelin's investigation uncovered a significant reduction in major jihadist forums between 2009 and 2013.[29] Whereas previous jihadist online activism was limited to top-down official Al-Qaeda websites, these new forums 'shattered the elitist nature of *jihadi* communications'.[30] A number of scholars credit the work of Abu Mus'ab Al-Suri in spearheading this change.[31]

For some time, forums and chat rooms have been particularly useful for extremist propagators because of the online anonymity offered to users. Although seemingly counter-intuitive, this aspect of online forums, according to some, helped to facilitate greater feelings of connection.[32] It provided those who would 'never normally engage in criminal or risky behaviour in the physical world' the ability to 'confide in the safety of their surrounding online environment'.[33] Anonymity therefore helped put individuals at ease when asking questions about taboo subjects (e.g. sex, relationships, etc.) and also granted greater authority to users posting as ideological experts on what to do, whether the topic was bomb-making or issues of integration.[34] While likely a feature of the internet as a whole, this dynamic is prominently displayed in online discussion forums because people are more reluctant to act out on personal accounts.[35] Anonymity creates an 'online disinhibition' effect that, in its 'toxic' form,[36] gives people a sense of security in avoiding responsibility for their virtual pronouncements. This can, in turn, foster increased hostility, polarization and even violence.[37] In his work with former German far-right extremists who were active online, Daniel Koehler identified anonymity as the second most common attribute among the interviewees as it provoked individuals to speak out more than they normally would offline.[38]

[29] Zelin, 'The State of global jihad online', p. 2.
[30] Zelin, 'The State of global jihad online', p. 5.
[31] Brynjar Lia, *Architect of global jihad: the life of Al-Qaeda strategist Abu Mus'ab al-Suri* (London: Hurst, 2009); Zelin, *The state of global jihad online*.
[32] Sageman, *Understanding terror networks*.
[33] Bruce McFarlane, *Online violent radicalisation (OVeR): challenges facing law enforcement agencies and policy stakeholders*, Monash University, 2010, p. 5.
[34] Gary Bunt, *Islam in the digital age: e-jihad, online fatwas and cyber Islamic environments* (London: Pluto Press, 2003); Gabriel Weimann, 'Terror on Facebook, Twitter and YouTube', *Brown Journal of World Affairs* 16: 2, Spring/Summer 2010, pp. 45–54; National Coordinator for Counterterrorism, *Jihadists and the internet: 2009 update*, The Hague, 2010; Bilveer Singh, 'Youth self-radicalisation: lessons from the Singapore narrative', *The Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) Journal*, August 2013, pp. 87–103.
[35] Piet Bakker and Sanne Hille, 'Engaging the social news user: comments on news sites and Facebook', *Journalism Practice* 8: 5, 2014, pp. 563–72 at p. 563.
[36] John Suler, 'The online disinhibition effect', *International Journal of Applied Psychoanalytic Studies* 2: 2, June 2005, pp. 184–8.
[37] Daniel Koehler, 'The radical online: individual radicalization processes and the role of the internet', *Journal for Deradicalization*, vol. 1, Winter 2014/15, pp. 116–34 at p. 118.
[38] Koehler, 'The radical online'.

Social media

Though traditional forums have become less reliant on password protection, extremists began to look at more publicly available communication.[39] This use of social media made online jihadist activism far more accessible to the general public. It also means that the traditional relationship between mainstream media and violent actors has been somewhat reversed—with the former now relying more on the latter's social media output for information gathering and non-state violent actors no longer requiring the mainstream media to disseminate information.[40]

Some authors suggest that online social networks can have the same or a similar effect on radicalization and mobilization as face-to-face interactions.[41] Jerome Bjelopera takes this argument further, claiming that the level of interactivity between jihadists and their audience encourages the consumers 'to more easily see themselves as part of broader jihadist movements and not just casual readers or online spectators'.[42]

Koehler has found that this dynamic is as true for neo-Nazis as it is for jihadists, arguing that extremist use of social media helps to create an impression among online followers that a critical mass has built up within the movement. This effect then motivates individuals to become further involved in the movement and take part in more extreme actions.[43] This trend mirrors the group dynamics that Marc Sageman observed in the physical world, where 'groupthink' took hold and opinions gradually became increasingly extreme as members of the groups he analysed become more insular and exclusively reliant on the group for social interaction.[44] As Maura Conway and others note, while more work needs to be done on proving the assertion that online networks can have the same impact as physical ones, it remains an interesting and fruitful avenue for future research.[45]

Social networking sites have also maximized the accessibility of extremist groups and content. Drawing from one of the largest databases of Twitter accounts used by European members of the Islamic State in Iraq and Syria (ISIS), the authors of *#Greenbirds* note how social networking sites have been used to establish webs through which 'a large number of foreign fighters receive their

[39] Weimann, 'Terror on Facebook, Twitter and YouTube'; Gabriel Weimann, *Terrorism in cyberspace: the next generation* (New York: Columbia University Press, 2015).

[40] Jytte Klausen, 'Tweeting the jihad: social media networks of western foreign fighters in Syria and Iraq', *Studies in Conflict and Terrorism* 38: 1, 2015, pp. 1–22 at p. 6.

[41] Rachel Briggs, *Radicalisation: the role of the internet*, Institute for Strategic Dialogue, London, 2011; Maura Conway, 'From Al-Zarqawi to Al-Awlaki: the emergence of the internet as a new forum of violent radical milieu', *Combating Terrorism Exchange* 2: 4, 2012, pp. 12–22; Elizabeth Pearson, 'The case of Roshonara Choudhry: implications for theory on online radicalization, ISIS women, and the gendered jihad', *Policy & Internet* 8: 1, March 2016, pp. 5–33.

[42] Jerome Bjelopera, *American jihadist terrorism: combating a complex threat*, Congressional Research Service, 2013, pp. 20–21.

[43] Koehler, 'The radical online', p. 121.

[44] Magdalena Wojcieszak, '"Don't talk to me": effects of ideologically homogeneous online groups and politically dissimilar offline ties on extremism', *New Media and Society* 12: 4, 2010, pp. 637–55; Marc Sageman, *Leaderless jihad: terror networks in the twenty-first century* (Philadelphia: University of Pennsylvania Press, 2008), p. 87.

[45] Maura Conway and Lisa McInerney, 'Jihadi video and auto-radicalisation: evidence from an exploratory YouTube study', *Intelligence and Security Informatics*, 2008, pp. 108–18 at p. 116.

information about the conflict not from the official channels provided by their fighting group but through so-called disseminators'.[46] These disseminators are sympathetic individuals who effectively formulate extremist narratives from the relative safety of their homes in the West. They are also able to provide real-time updates from their contacts in far-away battles, and are often seen as major sources of conflict information for foreign fighters.[47] In another study, Jytte Klausen's findings corroborate some of the conclusions in *#Greenbirds*, while identifying social media users with lower profiles as more impactful.[48]

Gabriel Weimann explains how Facebook remains especially important for 'letting terrorists find mainstream Islamic youth who may on occasion view jihadist content and link them to the more … hard-core sympathisers'.[49] The US Department of Homeland Security also argues that Facebook can act as a 'gateway' to extremist sites and operational information.[50] For some time, Twitter served as 'the main hub for the active dissemination of links directing users to digital content hosted on a range of other platforms',[51] while YouTube has fostered a 'thriving subculture which uses it to communicate, share propaganda, and recruit new individuals'.[52] Weimann highlights the development of comments sections below videos as a crucial step, noting that the 'ability to exchange comments about videos and to send private messages to other users help *jihadists* identify each other rapidly, resulting in a vibrant *jihadist* virtual community'.[53] Instagram and Flickr have also been 'littered with radical propaganda glorifying terrorist masterminds such as Osama Bin Laden and Anwar al-Awlaki'.[54] Western countries, in particular the United States, protect the freedom of user-generated content, causing extremist propaganda disseminators to flock to these regions.[55]

Ultimately, social media have emerged as a key tool for extremist groups as they provide a level of accessibility that allows users to selectively implant themselves in communities and milieux of like-minded individuals.[56] The process of isolation has been described as entering into 'echo chambers'[57] or 'cyberbalkanisation'.[58]

[46] Joseph Carter, Shiraz Maher and Peter Neumann, *#Greenbirds: measuring importance and influence in Syrian foreign fighter networks*, International Centre for the Study of Radicalisation, London, 2014, p. 1.
[47] Carter, Maher and Neumann, *#Greenbirds*.
[48] Klausen, 'Tweeting the jihad'.
[49] Gabriel Weimann, *New terrorism and new media*, The Wilson Center, Wasgington DC, 2014, p. 6.
[50] Department of Homeland Security, 'Terrorist use of social networking: Facebook case study', Dec. 2010.
[51] Ali Fisher and Nico Prucha, 'Tweeting for the Caliphate: Twitter as the new frontier for jihadi propaganda', *CTC Sentinel* 6: 6, June 2013, p. 21.
[52] Weimann, *New terrorism and new media*, p. 10.
[53] Weimann, *New terrorism and new media*, p. 10 (emphasis in the original).
[54] Weimann, *New terrorism and new media*, p. 13.
[55] Committee on Homeland Security House of Representatives, *Using the web as a weapon: the internet as a tool for violent radicalization and homegrown terrorism*, hearing before the subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 110th Congress 1st Session, no 110-83 (Washington DC: US Government Printing Office, 6 Nov. 2007), pp. 1–6.
[56] Claudia Carvalho, '"Okhti" online: Spanish Muslim women engaging online jihad—a Facebook case study', *Online-Heidelberg Journal of Religions on the Internet* vol. 6, 2014, pp. 24–41.
[57] Neumann, *Countering online radicalization in America*; Sanne Geeraerts, 'Digital radicalization of youth', *Social Cosmos* 3: 1, 2012, pp. 25–32; Seamus Hughes and Lorenzo Vidino, *ISIS in America: from retweets to Raqqa*, George Washington University Program on Extremism report, Washington DC, Dec. 2015.
[58] Marshall Van Alstyne and Erik Brynjolfsson, *Electronic communities: global village or cyberbalkans?*, MIT Sloan School, 1997, p. 3.

Many studies argue that such echo chambers allow for the unchallenged support and amplification of the most extreme views in a community.[59] This also leads to fewer dissenting voices, and helps users embrace extreme ideas: 'As a result', according to Neumann, 'people acquire a skewed sense of reality so that extremist attitudes and violence are no longer taboos but—rather—are seen as positive and desirable'.[60] Platforms like Twitter and Facebook are particularly conducive to the creation of echo chambers because they help users curate content using complex algorithms. In doing so, media companies inadvertently expose their extremist users to content that reinforces their interest and beliefs, failing to integrate dissenting voices and alternative opinions.

Encryption and the dark web

Research on the use of encryption technologies and the so-called 'dark web' by terrorists is understandably limited given the closed and less accessible nature of these platforms. However, mounting concerns over operational security and account shut-downs on broad-based sites like Facebook are known to have pushed extremists onto less transparent, more secure mediums such as Tor, an anonymous browser, and ProtonMail, an encrypted email service.[61] Moreover, as Seamus Hughes and Alexander Meleagrou-Hitchens explain, 'The emergence of applications such as Telegram, SureSpot, Kik, and—since its recent offering of end-to-end encryption—WhatsApp has been a particular game changer for the Islamic State and its efforts in the West'.[62]

In one of the most in-depth studies to date on the use of Telegram by ISIS, Nico Prucha argues that Telegram has not only become 'the most important information outlet' for the group, but that it 'has been used to recruit and guide attackers in Europe'.[63] In their study of ISIS-related terrorism in Europe, Petter Nesser and his co-authors discovered that out of 38 plots and attacks in Europe between 2014 and October 2016, 19 were found to have involved 'online instruction from members of IS's networks'.[64] Although various digital communications remain relevant, they explain that 'the ways in which attackers are instructed via encrypted social media are unprecedented'.[65]

In the digital domain and on the web in particular, people are 'not bound by the same kinds of social limitations and legal constraints' as they are in the real world.[66] As law enforcement practitioners and private companies work to restrict

[59] Briggs, *Radicalisation: the role of the internet*, p. 6; Bjelopera, *American jihadist terrorism*, p. 18.
[60] Neumann, *Countering online radicalization in America*, p. 18.
[61] Laith Alkhouri and Alex Kassirer, 'Tech for jihad: dissecting jihadists' digital toolbox', Flashpoint report, July 2016.
[62] Seamus Hughes and Alexander Meleagrou-Hitchens, 'The threat to the United States from the Islamic State's virtual entrepreneurs', *CTC Sentinel* 10: 3, March 2017, pp. 1–8 at p. 1.
[63] Nico Prucha, 'IS and the jihadist information highway—projecting influence and religious identity via Telegram', *Perspectives on Terrorism* 10: 6, 2016, pp. 48–58.
[64] Petter Nesser, Anne Stenersen and Emilie Oftedal, 'Jihadi terrorism in Europe: the IS effect', *Perspectives on Terrorism* 10: 6, 2016, pp. 3–24.
[65] Nesser, Stenersen and Oftedal, 'Jihadi terrorism in Europe', p. 9.
[66] Jarret Brachman and Alix Levine, 'You too can be Awlaki!', *The Fletcher Forum of World Affairs* 35: 1, Winter

radical actors through the legal system and content-based regulations, extremists continue to move to new platforms when opportunities arise. Although an internet is at the core of many digital communications technologies, subsequent works must examine the secondary effects of these mediums within the context of radicalization and recruitment. Messaging apps, for example, likely have different effects from forums and other social media platforms.

Question 2: Have digital communications technologies transformed radicalization and recruitment dynamics?

Many studies have found that digital technologies have helped to transform the dynamics of terrorist radicalization, recruitment and participation by facilitating communication and the movement of people and resources. On a rudimentary level, communication technologies provide the primary locus for individuals 'to access radicalizing material, instruction manuals and videos'.[67] For Tim Stevens, a crucial way the internet facilitates radicalization is by allowing extremists to disseminate their own narratives without relying on journalists as middlemen, provided the radicals possess cheap equipment such as laptops and video cameras.[68] Peter Neumann poignantly notes that the rise of web 2.0 allows extremists to reach a wider demographic of potential sympathizers.[69] Simone Molin Friis expands on these points, arguing that digital media technologies 'facilitate new ways of communicating the horrors of war', particularly in the context of visual media such as photo and video.[70]

In a broader sense, digital technologies change how people communicate with each other, thus influencing group dynamics and radicalization and recruitment trends. Bruce Hoffman and Sageman, two seminal figures in the fields of terrorism and radicalization studies, consider the role of the digital sphere in their respective studies of terrorists' organizational structure and recruitment strategy. Their differing positions on the directionality of terrorist recruitment, whether it be hierarchical or network, transcend the physical world, emerging across digital communications, too. Both scholars were also among the first to write and comment extensively on the topic, and while their work dates back to the last decade, it is worth reviewing it in the context of how this discussion has evolved.

Hoffman examines the use of new media and the internet by Al-Qaeda recruiters, understanding radicalization as a process primarily influenced by the messaging efforts of global jihadist leadership figures.[71] He argues that 'from the

2011, pp. 25–36 at p. 34.

[67] Weimann, *New terrorism and new media*.

[68] Tim Stevens, 'Regulating the "dark web": how a two-fold approach can tackle peer-to-peer radicalisation', *The RUSI Journal* 154: 2, 2009, pp. 28–33 at p. 28; see also David Betz, 'The more you know, the less you understand: the problem with information warfare', *The Journal of Strategic Studies* 29: 3, 2006, pp. 505–33 at p. 510.

[69] Neumann, *Countering online radicalization in America*, p. 17.

[70] Simone Molin Friis, '"Beyond anything we have ever seen": beheading videos and the visibility of violence in the war against ISIS', *International Affairs* 91: 4, 2015, pp. 725–46 at p. 726.

[71] Bruce Hoffman, 'The use of the internet by Islamic extremists', testimony presented to the United States House Permanent Select Committee on Intelligence, 4 May 2006.

start its [Al-Qaeda's] leadership seems to have intuitively grasped the enormous communicative potential of the Internet and sought to harness this power both to further the movement's strategic aims and facilitate its tactical operations'.[72] Hoffman narrows his analysis to Al-Qaeda's ideological, tactical and strategic output via the internet. He is particularly attentive to online global jihadist magazines such as *Sawt al-Jihad*, which emerged in 2004 carrying a 'message that was less one of attacking U.S. and other western targets than the importance of mobilizing Muslim public opinion and support of jihad'.[73] In Hoffman's view, violent radicalization and recruitment efforts by jihadists, while top-down, are dependent on effective communication.[74]

In *Leaderless jihad,* Sageman argues that terrorist networks form at a grass-roots level and carry out operations without oversight from Al-Qaeda or any other formal, hierarchical group.[75] The radicalization process is therefore born out of interpersonal dynamics rather than leadership. Sageman contends that the internet has breathed new life into the process, facilitating the development of networks and allowing for the provision of 'general guidelines' that act as a 'virtual glue'.[76] With a minimal level of ideological, strategic and tactical coherence, Al-Qaeda central could still advertise its 'demands for terrorist operations on the Internet'.[77] In this framework, the internet allowed various actors to pursue the same goal without reporting to structural hierarchies.

In practice, Sageman's and Hoffman's analyses are not mutually exclusive. Evolving digital communications technologies offer a fusion of top-down, bottom-up, lateral and even self-guided radicalization and recruitment opportunities. The case of English-speaking jihadist ideologue Anwar al-Awlaki exemplifies the existence and efficacy of multi-directional recruitment dynamics. As a top-down, quasi-leadership figure within Al-Qaeda in the Arabian Peninsula (AQAP), Awlaki widened the parameters of participating in the global jihad movement by giving near-equal significance to other forms of jihad, such as the online dissemination of propaganda.[78] Through online lectures and publications, Awlaki fuelled grass-roots radicalization in the West and encouraged sympathizers to participate in the movement in both violent and non-violent roles. AQAP's *Inspire* magazine, which was largely produced by Awlaki and Samir Khan, contained a section called 'Open source jihad', which equipped 'aspiring jihadist attackers with the tools they need to conduct attacks without travelling to jihadist training camps'.[79]

Awlaki's reach also illustrates the ways psychological mechanisms and group dynamics, both real and perceived, exist in the digital sphere because of

[72] Hoffman, 'The use of the internet by Islamic extremists', p. 5.
[73] Hoffman, 'The use of the internet by Islamic extremists', p. 9.
[74] Hoffman, 'The use of the internet by Islamic extremists', p. 15.
[75] Sageman, *Leaderless jihad*.
[76] Sageman, *Leaderless jihad,* p. 144.
[77] Sageman, *Leaderless jihad,* p. 144.
[78] Alexander Meleagrou-Hitchens, *As American as apple pie: how Anwar al-Awlaki became the face of western jihad*, International Centre for Study of Radicalisation, London, 2011; Scott Shane, *Objective Troy: a terrorist, a president, and the rise of the drone* (New York: Tim Duggan Books, 2015).
[79] Weimann, *New terrorism and new media*; Anti-Defamation League, *Homegrown Islamic extremism in 2013: the perils of online recruitment and self-radicalization*, New York, 2014.

communications technologies.[80] Propagandists like Awlaki, through the use of grandiose discourse[81] and behavioural affirmation,[82] make recruits feel included and enhance a sense of mission and self-importance.[83] In 'You too can be Awlaki', Jarret Brachman and Alix Levine recognize American convert Zachary Chesser's online activism as an effort to emulate the prolific voices of Awlaki and Khan.[84] Awlaki's broader validation of online jihad furthered self-radicalization for some individuals like Nidal Hassan, the Fort Hood shooter.[85] Brachman and Levine argue that radical sympathizers may experience 'dissonance' when their online efforts outdo their physical contributions, leading some to make up for the difference by adopting their virtual identity in the real world.[86] Neumann reinforces this argument by suggesting that the internet can catalyse self-idealization, projecting the traits and characteristics that the individual aims to possess.[87]

In support of the 'self-radicalization' phenomenon, the Anti-Defamation League (ADL) notes, 'face-to-face interaction with terrorist operatives is no longer a requirement for radicalization'. Individual extremists, or lone actors, are therefore 'increasingly self-radicalizing online'.[88] In a study conducted by the Southern Poverty Law Center on the popular American white nationalist site Stormfront, the author found that 'registered Stormfront users have been disproportionately responsible for some of the most lethal hate crimes and mass killings since the site was put up in 1995'.[89] In view of these trends, among others, it appears that traditional group membership is no longer a prerequisite for involvement in terrorism.[90]

In this context, it is crucial to touch on the 'self-radicalization' phenomenon, as the literature often intersects with discourse about radicalization in the digital sphere. Scholars who study violent extremists of various ideological persuasions rarely state that the internet *alone* has the power to 'self-radicalize' an individual.[91] Aidan Kirby does, however, explain that the 'self-starter' phenomenon has been seriously affected by the rise of the internet.[92] Similarly, in their study of lone

[80] Cristina Archetti, 'Terrorism, communication and new media: explaining radicalisation in the digital age', *Perspectives on Terrorism* 9: 5, 2015, pp. 49–59 at p. 52; Sageman, *Understanding terror networks*; Neumann, *Countering online radicalization in America*, p. 18.

[81] Anne Gerdes, 'Al-Qaeda on web 2.0: radicalisation and recruitment strategies', in James Braman, Alfreda Dudley and Giovanni Vincenti, eds, *Investigating cyber law and cyber ethics: issues, impacts and practices* (Hershey, PA: Information Science Reference, 2012); Maura Conway, 'From "cyberterrorism" to "online radicalisation"', in Mahmoud Eid, ed., *Exchanging terrorism oxygen for media airwaves: the age of terroredia* (Hershey, PA: Information Science Reference, 2014).

[82] Neumann, *Countering online radicalization in America*, p. 18.

[83] Bergin et al., *Countering internet radicalisation in southeast Asia*; Jennifer Hui, 'The internet in Indonesia: development and impact of radical websites', *Studies in Conflict and Terrorism* 33: 2, 2010, pp. 171–91; Bjelopera, *American jihadist terrorism*.

[84] Brachman and Levine, 'You too can be Awlaki!', p. 36.

[85] Bjelopera, *American jihadist terrorism*; Brachman and Levine, 'You too can be Awlaki!'.

[86] Brachman and Levine, 'You too can be Awlaki!', p. 34.

[87] Neumann, *Countering online radicalization in America*, p. 19.

[88] Anti-Defamation League, *Homegrown Islamic extremism in 2013*, p. 1.

[89] Heidi Beirich, *White homicide worldwide: Stormfront*, Southern Poverty Law Centre, 31 March 2014, p. 2.

[90] Bergin et al., *Countering internet radicalisation in southeast Asia*.

[91] Aidan Kirby, 'The London bombers as "self-starters": a case study in indigenous radicalisation and the emergence of autonomous cliques', *Studies in Conflict and Terrorism* 30: 5, 2007, pp. 415–28; Anti-Defamation League, *Homegrown Islamic extremism in 2013*.

[92] Kirby, 'The London bombers as "self-starters"', p. 416.

actors, Paul Gill and his co-authors note that while not causing an increase in the number of attacks, the internet has certainly altered individuals' means of radicalization and learning.[93]

In a study of ISIS's strategy for attracting western foreign fighters, J. M. Berger unpacks specific details about online radicalization and recruitment practices.[94] Using a database of approximately 1,600 Twitter accounts, he found that during 'first contact', ISIS recruiters make themselves available for interaction with sympathetic recruits while monitoring the activity of other potential recruits, perhaps interacting through 'retweets' and 'favourites' to establish familiarity.[95] Once contact is made, recruiters will seek to create a micro-community in which the individual is bombarded with content and encouraged to isolate themselves from others, particularly those who follow more mainstream interpretations of Islam.[96] Following this, the recruit is asked to transition on to private, encrypted messaging platforms such as Telegram, where they are then encouraged to take action, often in the form of either terrorist attacks or making *hijrah* (migration) to ISIS-controlled territory.[97]

The evolution of smartphones, for example, makes recruiters an omnipresent voice in the ear of the recruit. Moreover, within one tool, broad-based social media platforms such as Facebook and Twitter are a click away from encrypted messaging apps like Telegram. This synergistic combination of social media and encrypted messaging apps has sparked one of the most recent developments in the terrorist threat: the emergence of 'virtual plotters'.[98] A number of ISIS-inspired attacks in America, Europe and south Asia, which were initially assumed to be the work of lone actors, later proved to be coordinated and directed over the internet by ISIS members residing in the group's territories in Syria, Iraq and Afghanistan. One of the most effective thus far has been Rachid Kassim who, using his encrypted Telegram channel, contacted willing ISIS recruits in France and gave them ideological validation and operational guidance.[99] Jean-Charles Brisard of the Centre for the Analysis of Terrorism in Paris has also claimed that Kassim guided over half of the 17 foiled jihadist plots in France in 2016.[100]

In a similar manner, a group of jihadists in Raqqa, dubbed by the FBI as 'the Legion', used social media and messaging apps to direct different plots and

[93] Paul Gill, Maura Conway, Emily Corner, and Amy Thornton, *What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists*, VOX-Pol Network of Excellence, 2015.

[94] J. M. Berger, 'Tailored online interventions: the Islamic State's recruitment strategy', *CTC Sentinel* 8: 10, Oct. 2015, pp. 19–23.

[95] Berger, 'Tailored online interventions', pp. 19–21.

[96] Berger, 'Tailored online interventions', p. 21.

[97] Berger, 'Tailored online interventions', p. 22.

[98] Rukmini Callimachi, 'Not "lone wolves" after all: how ISIS guides world's terror plots from afar', *The New York Times,* 4 Feb. 2017; Amarnath Amarasingam, 'An interview with Rachid Kassem, jihadist orchestrating attacks in France', *Jihadology,* 18 Nov. 2016; Bridget Moreng, 'ISIS' virtual puppeteers: how they recruit and train "lone wolves"', *Foreign Affairs*, 21 Sept. 2016; Prucha, 'IS and the jihadist information highway'; Hughes and Meleagrou-Hitchens, 'The threat to the United States from the Islamic State's virtual entrepreneurs'.

[99] Amarasingam, 'An interview with Rachid Kassem, jihadist orchestrating attacks in France'.

[100] Ryan Browne and Paul Cruickshank, 'US-led coalition targets top ISIS figure in Iraq strike', CNN, 15 Feb. 2017.

attempted attacks in the United States.[101] In their study on the impact of what they term 'virtual entrepreneurs' in America, Hughes and Meleagrou-Hitchens found that, 'out of a total of 38 Islamic State-inspired domestic plots and attacks in the United States between March 1, 2014, and March 1, 2017, at least eight (21 percent) have involved some form of digital communication with virtual entrepreneurs'.[102] After acknowledging that internationally directed attacks are not fundamentally new, they suggest that the proliferation of virtual plotters represents an evolution of jihadist terrorist tactics that was made possible by the rise of social media and encrypted messaging apps.[103] In the future, this threat will likely continue to pose a critical challenge to western governments and technology companies.

In the face of emerging threats, many scholars question the extent to which digital technologies, and the internet in particular, facilitate radicalization, suggesting that communication tools are auxiliary to preconditions, antecedent behaviours and root causes.[104] Bill Durodié and Ng Sue Chia, for example, argue that no individual approaches the internet in isolation, rather 'they come to it already bearing a vast number of ideas, assumptions and emotions'.[105] For these authors, the internet is largely seen as a medium to communicate content and ideology and, while important it is neither novel nor deserving of such an inflated reputation for facilitating radicalization.[106] While the precise influence of digital communications remains incalculable, emerging technologies will continue to present new opportunities for extremist organizations and their sympathizers.

Question 3: Can the digital sphere replace the physical world among extremist groups and their sympathizers?

The broader discussion of radicalization and recruitment contests the influence of interactions that use digital communications technologies compared to interactions in the physical world. In this context, scholars question how relationships in the digital sphere might substitute for physical interactions. Meanwhile, others highlight the ways in which real-world social networks materialize in the virtual world and vice versa.

The majority of the literature takes a nuanced position that asserts the importance of online influences without negating the requirement of offline interactions. In their content analysis of 336 right-wing websites, for example, Manuela Caiani and Patricia Kröll find that the internet acts as a 'bridge' between digital and

[101] Adam Goldman and Eric Schmitt, 'One by one, ISIS social media experts are killed as result of F.B.I. program', *The New York Times,* 24 Nov. 2016.
[102] Hughes and Meleagrou-Hitchens, 'The threat to the United States from the Islamic State's virtual entrepreneurs', p. 1.
[103] Hughes and Meleagrou-Hitchens, 'The threat to the United States from the Islamic State's virtual entrepreneurs'.
[104] Jonathan Githens-Mazer and Robert Lambert, 'Why conventional wisdom on radicalisation fails: the persistence of a failed discourse', *International Affairs* 86: 4, July 2010, pp. 889–901; Michael Mealer, *Internet radicalization: actual threat or phantom menace?*, PhD dissertation, Naval Postgraduate School, 2012, p. 10.
[105] Bill Durodié and Ng Sue Chia, 'Is internet radicalization possible?', *RSIS Commentaries,* Nov. 2008, p. 2.
[106] Mealer, *Internet radicalization*, p. 10.

physical arenas, particularly in the context of mobilization.[107] Many stress that the impact of the real-world environment is crucial in determining a person's vulnerability to turning to violence. Briggs subscribes to this argument but concedes that future instances of individuals radicalizing 'entirely online' may increase.[108] The authors of *Radicalisation in the digital era* punctuate the influence of the digital sphere in their study, arguing that virtual interactions enable radicalization.[109] Hughes and Lorenzo Vidino find some support for this argument in their study of American ISIS affiliates on Twitter where they found that 'purely web-driven' radicalization is evident in some cases.[110]

The case of Colleen LaRose is offered by Jeffry Halverson and Amy Way as a prime example of how real-world socialization is not necessarily a factor in an individual's radicalization, thus challenging the view of many experts that 'the Internet can support and facilitate but never completely replace direct human contact and the ties of friendship and kinship'.[111] LaRose allegedly 'never set foot in a mosque, kept no religious books, hung no religious images or symbols in her apartment, and, according to several of her neighbours, never spoke about her religious beliefs'.[112] For Jenna Park and Yeap Suyin, the case of Muhammad Fadil Abdul Hamid is another illustration of this apparently rare phenomenon.[113] Hamid became exposed to extremist religious ideologies on the web before attempting to contact Anwar al-Awlaki and a suspected Al-Qaeda recruiter with the 'hopes of undertaking militant jihad in places such as Palestine, Iraq and Afghanistan'.[114] These cases, among others, are often cast as exceptional.[115]

Analysts and scholars who emphasize the importance of physical networks in the processes of radicalization and recruitment are generally unconvinced by the notion of solitary self-radicalization.[116] Hoffman, for example, places the onus on the importance of hierarchy within terrorist organizations, stating that 'official websites' and the ideological elite play the key role in facilitating radicalization in both physical and virtual spheres.[117] Sageman does not ascribe to solitary self-radicalization either; instead he places an emphasis on the impetus from interaction between peers, which creates opportunities for 'in-group love'.[118]

[107] Manuela Caiani and Patricia Kröll, 'The transnationalization of the extreme right and the use of the internet', *International Journal of Comparative and Applied Criminal Justice* 39: 4, 2015, pp. 331–51.
[108] Briggs, *Radicalisation: the role of the internet*, p. 3.
[109] Ines Von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, *Radicalisation in the digital era: the use of the internet in 15 cases of terrorism and extremism*, RAND Europe, 2013.
[110] Hughes and Vidino, *ISIS in America*, p. ix.
[111] Jeffry Halverson and Amy Way, 'The curious case of Colleen LaRose: social margins, new media, and online radicalization', *Media, War & Conflict* 5: 2, 2012, pp. 139–53 at p. 140.
[112] Halverson and Way, 'The curious case of Colleen LaRose', p. 143.
[113] Jenna Park and Yeap Suyin, 'Countering internet radicalisation: a holistic approach', RSIS Commentaries, July 2010.
[114] Park and Suyin, 'Countering internet radicalisation', p. 1.
[115] Mealer, *Internet radicalization*, p. 57; Gill et al., *What are the roles of the internet in terrorism*?; Pearson, 'The case of Roshonara Choudhry'.
[116] Sageman, *Understanding terror networks*, p. 91; Durodié and Ng, 'Is internet radicalization possible?'; Bergin et al., *Countering internet radicalisation in southeast Asia*; Chatham House, 'Terrorism, radicalization and the internet', report of a private roundtable, 2008; Raffaello Pantucci, 'The jihad will be YouTubed', *Foreign Policy*, 15 Dec. 2011; Hussain and Saltman, *Jihad trending*; Hughes and Vidino, *ISIS in America*.
[117] Hoffman, 'The use of the internet by Islamic extremists'.
[118] Sageman, *Understanding terror networks* and *Leaderless jihad*.

Conway and Lisa McInerney suggest that a bottom-up theory explains the initial entry for youths seeking extremist content, while digital communication can enable the radicalization of individuals with no prior connection to the movement by providing contact between the individual, extremists and other aspiring radicals online.[119] Simultaneously, they demonstrate that terrorist organizations actively employ a top-down approach to connect with vulnerable individuals using virtual communications.[120]

Neumann also shows how the internet radicalizes by providing a platform for like-minded individuals to build a network, and potentially turn their terrorist aspirations into a reality. For terrorist recruiters, 'it has also offered a pool of potential members that can be tapped into, with less risk than there would be involved in approaching an individual in the real world'.[121] Charlie Winter has also suggested that the internet has in some ways replaced physical spaces when he argues that social media have emerged as 'the decade's radical mosque'.[122] Weimann concurs, writing that the 'interactivity, reach, frequency, usability, immediacy and permanence that the virtual world has come to provide now heighten and mimic those processes that took place previously inside places of worship'.[123]

This is not to discount the power of physical interaction, however, and Koehler's interviews with former German far-right extremists, for example, reveal a belief among them that, while the internet created an effective and efficient space in which to interact, they only felt truly part of the movement after attending rallies and meeting members in the real world.[124] In their study of American jihadists, Hughes and Vidino also demonstrate that in many cases, radicalized individuals 'initially cultivated and later strengthened their interest in ISIS's narrative through face-to-face relationships', arguing that 'online and offline dynamics complement one another'.[125] In a like manner, Neumann points to the case of Irfan Raja, whose entire radicalization appears to have occurred in the digital domain, but it was only after real-world contact with four other like-minded individuals that he decided to go to Pakistan to receive training.[126]

While varying perspectives and caveats emerge within the literature, evidence suggests that the digital sphere does not replace the real world in most instances. Further investigation is required in the rare cases where the digital domain is the primary or sole means of radicalization and recruitment. In such circumstances, it is crucial to question the extent to which virtual connections, information sharing and validation have real-world implications. Like the fusion of top-down and bottom-up group dynamics, the synergistic convergence of real-world and

[119] Conway and McInerney, 'Jihadi video and auto-radicalisation', p. 116.
[120] Conway and McInerney, 'Jihadi video and auto-radicalisation', p. 10.
[121] Neumann, *Countering online radicalization in America*, p. 19.
[122] Charlie Winter, *The virtual 'Caliphate': understanding Islamic State's propaganda strategy*, Quilliam, (London, July 2015), p. 7.
[123] Weimann, *New terrorism and new media*, p. 2.
[124] Koehler, 'The radical online', p. 123.
[125] Hughes and Vidino, *ISIS in America*, p. ix.
[126] Peter Neumann, *Joining Al-Qaeda: jihadist recruitment in Europe*, International Institute for Strategic Studies, 2008, p. 57.

virtual connections creates a highly combustible environment for radicalization and recruitment.

Conclusion

There are no unified theories of radicalization or standardized steps for recruitment, but violent extremists and their respective organizations continue to exploit digital communications technologies in their efforts to change the status quo. Consequently, this review attempts to provide an up-to-date assessment examining the role of digital communications in the processes of radicalization and recruitment. It draws from a range of existing research in order to interrogate three questions vexing policy-makers, law enforcement officials and academics.

To answer the first question, this review examined the connection between violent extremists and communication platforms. On a rudimentary level, it is clear that that violent extremists seek to optimize their influence across various platforms, exploiting new media as opportunities emerge. Most notably, this section used existing literature to move away from a monolithic understanding of the internet and showcase the opportunities afforded by different communication technologies within the context of radicalization and recruitment.

After laying the groundwork for a nuanced discussion, moving on to the second question, the review examined the effect of digital communications technologies on radicalization and recruitment dynamics. In this context, there is a consensus that despite significant exceptions to the rule, the internet alone does not act as a radicalizing agent, but rather serves as a facilitator and catalyst for terrorist organizations and their respective networks. More than ever before, digital technologies change how people communicate with each other, thus influencing group dynamics and radicalization and recruitment trends. Consequently, the virtual sphere offers a fusion of top-down, bottom-up, lateral and even self-guided radicalization and recruitment opportunities.

In response to the third question, this review addressed the possibility of the digital sphere replacing the physical world among violent extremists and their followers. Varying analyses emerge from the literature, but at present there is agreement that the virtual sphere does not replace the real world in most instances. Instead, the evidence suggests that online and offline dynamics complement one another, reinforcing extremist views.

Above all, this review of the current literature demonstrates that, in order to answer the crucial questions posed in this article, much more empirically based research is required. Over the last few years, however, a number of notable analysts and scholars have tried to address this by making use of the new primary data afforded them by extremists' use of social media. As their use of the internet continues to rapidly evolve and effectively adapt to a constantly shifting online media environment, the answers to these questions will become all the more pressing for counterterrorism authorities who continue to search for effective means to counter extremists' use of digital communications.