Bytes not waves: information communication technologies, global jihadism and counterterrorism

MICHAEL CHERTOFF, PATRICK BURY AND DANIELA RICHTEROVA*

Information technology has transformed our society. The internet, mobile phones and social networking platforms have fundamentally changed the ways in which states, groups and individuals interact. Despite difficulties defining it,[1] terrorism, generally viewed as a 'tactic'[2] used for 'the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change',[3] has also profoundly changed as a result of technological advance, becoming increasingly global, lethal and complex. Remarkably, however, current scholarship lacks a systematic assessment of the impact information communication technologies (ICTs) have had on jihadist organization, their tactics and strategies. ICTs are technologies that provide access to information through telecommunications. To date, terrorism scholars have produced a vast number of typologies, focused variously on terrorist causes,[4] motivations,[5] types[6] and acts,[7] as well as some that seek to be as comprehensive as possible.[8] However, none of these works focuses on technology. This gap exists despite a notable growth in scholarship—including in this journal—on the impact of digital communications on terrorist radicalization and recruitment, learning, financing and propaganda,[9] which may be attrib-

* The authors would like to acknowledge the support of the UK Research and Innovation Future Leaders Fellowship grant reference MR/S034412/1, and the GLOBSEC Intelligence Reform Initiative. They would also like to thank the anonymous reviewers for their helpful comments.

1 Alex P. Schmid, *Political terrorism: a research guide to concepts, theories, data bases and literature* (New Jersey: Transaction, 1983).

2 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington DC, 2004), ch. 12.

3 Bruce Hoffman, *Inside terrorism*, 2nd edn (New York: Columbia University Press, 2006), p. 41.

4 Martha Crenshaw, 'The causes of terrorism', *Comparative Politics* 13: 4, 1981, pp. 379–99.

5 Paul Wilkinson, 'Current and future trends in domestic and international terrorism: implications for democratic government and the international community', *Strategic Review for Southern Africa* 23: 2, 2001, pp. 106–23.

6 Alex Schmid and J. F. A. de Graaf, *Violence as communication: insurgent terrorism and the western news media* (London: Sage, 1982).

7 Martha Crenshaw, *Revolutionary terrorism* (Stanford, CA: Hoover Institution Press, 1979).

8 Boaz Ganor, 'Terrorist organization typologies and the probability of a boomerang effect', *Studies in Conflict and Terrorism* 31: 4, 2008, pp. 269–83.

9 On recruitment, see Alexander Meleagrou-Hitchens, Audrey Alexander and Nick Kaderbhai, 'The impact of digital communications technology on radicalization and recruitment', *International Affairs* 93: 5, 2017, pp. 1233–49; Helle Malmvig, 'Soundscapes of war: the audio-visual performance of war by Shi'a militias in Iraq and Syria', *International Affairs* 96: 3, May 2020, pp. 649–66; Manni Crone, 'It's a man's world: carnal spectatorship and dissonant masculinities in Islamic state videos', *International Affairs* 96: 3, May 2020, pp. 573–91. On learning, see Magnus Ranstorp and Magnus Normark, eds, *Understanding terrorism innovation and learning: Al-Qaeda and beyond* (Abingdon: Routledge, 2015). On financing, see Michael Jacobson, 'Terrorist financing

International Affairs **00**: 0 (2020) 000–000; DOI: 10.1093/ia/iiaa048

utable to the fast pace of evolution and the resulting difficulties in conducting systematic analyses. This article provides a typology that highlights the centrality of ICTs to the evolution of jihadist activities in the late modern era (from the 1990s to the present) and a coherent classification for understanding the most important characteristics of each of the overlapping epochs within it. Focusing on successful attacks, it details how, in each phase, jihadists have exploited the different strategic, organizational, recruiting, financing and tactical opportunities these developments present. The four distinct phases of global jihadism identified here have not come in mutually exclusive 'waves', but overlap and coexist—influenced by the rapid increase in technological capabilities—or volumes of bytes—in ICTs. Ultimately, we argue that our typology may be applicable to other types of global terrorism.

Rapoport's 'waves' typology, advanced to explain the ideological shifts in modern terrorist motivations from the 1880s to the early 2000s, is one of the most influential in terrorism studies, mainly owing to its simplicity. Rapoport argues that terrorism is best understood as four broad consecutive 'waves' of terrorism; the 'anarchist wave' beginning in the 1880s, the 'anti-colonial wave' in the 1920s, the 'new left wave' in the 1960s and the 'religious wave' that started with the 1979 Iranian Revolution.[10] For Rapoport, each wave lasts 40–45 years, representing 'a cycle of activity in a given time period, characterized by expansion and contraction phases'.[11] While Rapoport was interested in motivating ideologies, he correctly identified that advances in communications technology, in particular the telegram, mass circulation newspapers and railroads, fused with developments in terrorist doctrine, were 'critical' and 'conspicuous' drivers of waves.[12]

The waves typology has also been applied within the most recent 'religious' wave. In 'The four waves of global jihad', Robinson argues that there have been four broad evolutions of global jihadism in the period 1979–2017, each with its own motivations and strategies shaped by key ideologues.[13] The first global jihadist wave began in 1979 with the Soviet invasion of Afghanistan and subsequent call for Muslims to help defend their lands around the world. Robinson argues that key ideologue Abdullah Azzam's signature innovation was the creation of an elite 'solid base' of well-trained *mujahideen* to act as a 'Jihadi International'.[14] Although Azzam's calls for young Muslim men to fight in Afghanistan proved successful, the Soviet withdrawal, along with Azzam's death, marked the end of the first wave of global jihadism. The second wave (1996–2011) was epitomized by Osama

and the internet', *Studies in Conflict and Terrorism* 33: 4, 2010, pp. 353–63. On propaganda, see James Piazza and Ahmet Guler, 'The online caliphate: internet usage and ISIS support in the Arab world', *Terrorism and Political Violence*, publ. online 20 May 2019, https://www.tandfonline.com/doi/full/10.1080/09546553.2019.1606801?src=recsys; Constance Duncombe, 'Social media and the visibility of horrific violence', *International Affairs* 96: 3, May 2020, pp. 609–29. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 18 Feb. 2020.)

[10] David Rapoport, 'The four waves of rebel terror and September 11', *Anthropoetics* 8: 1, Spring–Summer 2002, http://anthropoetics.ucla.edu/ap0801/terror/.

[11] Rapoport, 'The four waves of rebel terror', p. 47.

[12] Rapoport, 'The four waves of rebel terror', pp. 48–9.

[13] Glenn Robinson, 'The four waves of global jihad, 1979–2017', *Middle East Policy* 24: 3, 2017, pp. 70–88.

[14] Robinson, 'The four waves of global jihad', p. 74.

bin Laden and his 'America First' policy of using direct violent action to drive the United States from the Muslim world and thereby weaken apostate regimes in order to establish a future caliphate. This wave ended with the degradation of 'Al-Qaeda Central' (AQC) in response to the 9/11 attacks and the death of Bin Laden. Robinson argues that a third wave is identifiable between the invasion of Iraq in 2003 and the collapse in 2017 of Islamic State in Iraq and Syria (ISIS). In this period, the motivation was to establish a caliphate immediately, with an emphasis on territory, shari'a law and brutality; key ideologues Abu Musab al-Zarqawi and Abu Bakr al-Baghdadi stressed the mass recruitment of fighters, in stark contrast to AQC's emphasis on quality.[15] Robinson labels the fourth and final wave, occurring from 2010 onwards, 'Personal jihad', following its key thinker, Abu Musab al-Suri. Al-Suri was instrumental in promoting a more individualistic or 'lone actor' view of global jihad by emphasizing the cumulative impact of small-scale violence. This was supported by his embrace of the internet not only as a recruitment tool but also as a virtual network for jihadist organization in the absence of a territorial state.[16]

Robinson's application of the wave typology is instructive in terms of the development of global jihadist thought, and accurate in its analysis of the key changes in strategy between these epochs. However, despite its awareness of the importance of the internet to the fourth global jihadist wave, it fails to pay sufficient attention to the influence of ICTs on the organization and tactics of the other waves. Indeed, a technology-centred model of global jihadist evolution may not only strengthen understanding, it may prove applicable to other global terrorist organizations.

The simplicity of the wave typology has also encouraged numerous academics to apply it to predict how future terrorism will emerge in a 'fifth wave', replacing the religious wave in the 2020s. These proposed new 'waves' include Fox's 'new anarchist' anti-globalization wave, Kaplan's 'new tribalism' wave, Honig and Yahel's 'terrorist semi-state' wave and Bartlett's 'green' wave.[17] Meanwhile, Simon has argued that the next 'wave' of global terrorism will be technological.[18] For Simon, whose central proposal is that technology, rather than ideology or doctrine, will drive future terrorism,

> the internet is the 'energy' for the Fifth Wave, continually revolutionizing the way information is gathered, processed, and distributed; the way communications are conducted and social networks formed; and the way single individuals can become significant players by using the internet to learn about technologies, techniques and targets.[19]

[15] Robinson, 'The four waves of global jihad', p. 80.
[16] Robinson, 'The four waves of global jihad', p. 84.
[17] Jonathon Fox, 'The future of religion and domestic conflict', in Berma Goldewijk, ed., *Religion, international relations and development cooperation* (Wageningen: Wageningen Academic, 2007), pp. 129–52; Jeffrey Kaplan, 'The fifth wave: the new tribalism?', *Terrorism and Political Violence* 19: 4, 2007, pp. 545–70; Or Honig and Ido Yahel, 'A fifth wave of terrorism? The emergence of terrorist semi-states', *Terrorism and Political Violence* 31: 6, 2017, pp. 1210–28; Jamie Bartlett, 'The next wave of extremists will be green', *Foreign Policy*, 1 Sept. 2017.
[18] Jeffrey Simon, 'Technological and lone operator terrorism: prospects for a fifth wave of global terrorism', in Jean Rosenfeld, ed., *Terrorism, identity and legitimacy* (New York: Routledge, 2011).
[19] Simon, 'Technological and lone operator terrorism', p. 48.

Therefore, he argues, 'no single type of terrorist ideology will dominate the Fifth Wave'; rather, there will be numerous ideologies all empowered by the exponential increase in information technology, competing to outdo each other in terms of spectacular attacks while avoiding the greater reach of IT-enhanced counterterrorist efforts.[20] Published in 2011, Simon's analysis is both prescient and correct in respect of the internet's impact on terrorism, especially in its application to lone actor terrorism and 'leaderless jihad'.[21]

Nevertheless, despite its useful contribution, a number of important criticisms can be levelled at Simon's arguments. Most importantly, it does not provide any typology for understanding ICT-facilitated change. The exact role of the internet is underdeveloped and its evolution is not related to evolving global terrorist organization. As a result, his analysis is focused on the internet and particular tactics, and does not address the impact of other information technologies on organizational strategies, structures, recruitment, training and financing. Also, in advancing his 'technological wave' argument, Simon still uses the wave typology which, as shown below, is problematic. Indeed, we will show that the fourth phase of ICTs' influence on global jihadism is already under way.

Clearly, then, within the wave literature itself there exist important gaps in our understanding of how global jihadism has been shaped by the evolution of ICTs. Moreover, despite its utility as a basic model for understanding the evolutions of global terrorism, Rapoport's waves typology has itself been heavily criticized by Parker and Sitter. They claim that the model is too simplistic, using historical evidence to show that the reality of terrorist evolution has been much 'messier'.[22] They argue instead that the evolution of terrorism can be better understood in terms of four overlapping motivational 'strains' that influence and interact with one another to drive innovation. Importantly, Parker and Sitter place ideational and technological evolutions—the confluence of motive and means—at the centre of their analysis. However, as their focus is on the modern era, they discuss technological evolutions in terms of the weapons and mass communications developments of, primarily, the nineteenth and early twentieth centuries, rather than more recent ICTs.[23] While they conclude that technological and ideational developments are likely to shape the future development of the four 'strains' of terrorism, they do not provide a detailed analysis of the impact of rapidly evolving ICTs on terrorism, or a typology for conceptualizing it.

In this article, we address these numerous gaps in the literature on classifying terrorism and jihadist activity by developing our 'Jihadism 1.0–4.0' framework, which identifies four overlapping and coexisting phases that broadly reflect the spread and development of ICTs since the 1990s. Like those proposing other terrorism typologies, we adopt a case-study approach that focuses primarily on jihadist

[20] Simon, 'Technological and lone operator terrorism', p. 47.
[21] Marc Sageman, *Leaderless jihad: terror networks in the twenty-first century* (Pennsylvania: University of Pennsylvania Press, 2008), pp. 37–8.
[22] Tom Parker and Nick Sitter, 'The four horsemen of terrorism: it's not waves, it's strains', *Terrorism and Political Violence* 28: 2, 2016, p. 211.
[23] Parker and Sitter, 'The four horsemen of terrorism'.

attacks as these have been the most prevalent globally and have been relatively overlooked in the literature on ICTs and terrorism,[24] and also because successful attacks highlight the confluence of the strategic, organizational, recruitment, financial and tactical ICT-based evolutions necessary to conduct them. Moreover, jihadist activities have evolved the fastest and furthest of all areas of global terrorism since the 1990s owing to their perpetrators' ability to exploit ICT changes. As such, jihadists have been key innovators whose tactics have provided a useful learning mechanism for other global terrorists and an indication of how their activities will evolve.[25]

We are aware of the limitations of this approach. In providing this typology we recognize that ICTs are not a cause of terrorism itself, but we do argue that they have changed its character in important respects—in particular, making it easier to act globally.[26] Nor can technology be a truly independent variable in a terrorism typology; rather, it interacts with groups' identities and interests to co-produce possible innovations. Similarly, although one of the main benefits of typologies is the greater conceptual clarity they encourage,[27] helping to synthesize 'the interaction and effects of the actions of many persons and collectives involving a multiplicity of motivations, psychological effects and subjective evaluations',[28] in striving for this clarity the values typologies assign to categories necessarily simplify the real world.[29] This is particularly the case in respect of terrorism, where both conceptualization and the subsequent proving of causality have proved problematic.[30] We would argue that typologies, supported by strong empirical evidence, work best as broad 'hand rails' that inform understanding and generate new hypotheses. This is precisely our aim here; we do not argue that this typology is definitive, all-encompassing or exclusive of all others; indeed, it displays similar strengths and weaknesses. But it is, we propose, an accurate and original typology through which to better understand the evolution of global jihadism from a technological perspective, using case evidence from numerous organizations from the mid-1990s onwards.

Globalization, new terrorism and technology

Our approach is supported by studies examining the impact of ICTs on terrorism in general and jihadism in particular. Numerous scholars have examined how globalization has shaped terrorism and counterterrorism since the 1990s. Aldrich

[24] Adam Dolnik, *Understanding terrorist innovation: technology, tactics, and global trends* (New York: Routledge, 2007).
[25] Brian Phillips, 'Terrorist group cooperation and longevity', *International Studies Quarterly* 58: 2, 2014, pp. 226–47; M. Fielitz, J. Ebner and M. Quent, *Loving hate: anti-Muslim extremism, radical Islamism and the spiral of polarisation* (Centre for Analysis of the Radical Right, 2018), https://www.idz-jena.de/fileadmin/user_upload/antimuslimextremism_radicalislamism_polarization.pdf.
[26] Andrew Glazzard, 'Shooting the messenger: do not blame the internet for terrorism', *RUSI Newsbrief* 39: 1, Jan.–Feb. 2019, https://rusi.org/sites/default/files/20190215_newsbrief_vol39_no1_glazzard_web.pdf.
[27] Orlando Behling, 'Some problems in the philosophy of science of organisations', *Academy of Management Review* 3: 2, 1978, pp. 193–201.
[28] Paul Wilkinson, *Terrorism and the liberal state* (Hong Kong: Macmillan, 1977), p. 31.
[29] Sarah V. Marsden and Alex P. Schmid, 'Typologies of terrorism and political violence', in Alex P. Schmid, ed., *The Routledge handbook of terrorism research* (London: Routledge, 2011), p. 159.
[30] Leonard Weinberg, Ami Pedahzur and Sivan Hirsch-Hoeffler, 'The challenges of conceptualizing terrorism', *Terrorism and Political Violence* 16: 4, 2004, pp. 777–94.

has shown how increasing globalization—especially interconnectivity and the growth of transnational terrorist groups—has transformed global terrorism,[31] forcing counterterrorism agencies to cooperate more closely.[32] Indeed, Cronin has argued that the global religious wave of terrorism is 'not only a reaction to globalization but is facilitated by it'.[33] Laqueur and Hoffman have argued that globalization has resulted in a change in the nature of terrorism into 'new terrorism'.[34] This is usually defined using four features: religious motivations; a horizontal network structure; a greater desire for inflicting mass casualties; and an intent to use weapons of mass destruction.[35] Neumann has linked these developments with globalization and late modernity, while others have stressed the technological factors enabling them.[36] While the exact applicability of the 'new terrorism' label is still under debate, clearly scholars have observed major patterns of change in terrorism since the 1990s. Moreover, scholars such as Hui, Al-Rawi and Veilleux-Lepage have focused on the ways in which global jihadists have harnessed Web 2.0 and 3.0 in their propaganda campaigns, but Al-Rawi and Hui in particular have not linked these with deep analyses of organization and tactics, and none of them have related these to the wider terrorism typology field, as we do here.[37]

Our typology is supported by evidence on the development of ICTs and their impact on society. While the introduction of more portable video cameras in the 1980s and the increasing availability of satellite broadcasting technologies in the 1990s represented major ICT advances, it is arguably the spread of the internet that has had the most influence on global jihadism. The first manifestation of the internet 'provided a gateway into an essentially static World Wide Web' in which users could read pages but could not alter them.[38] This came to be known as 'Web 1.0'. By 2000, Web 2.0 had emerged as coding and processing developments allowed websites to process user commands, and access and update larger databases much more rapidly. At the same time, content was becoming more visual, user-friendly and user-controlled. This new generation of the internet, dubbed 'Web 2.0', unleashed the exponential growth and ultimately power of social media

[31] Richard Aldrich, 'Globalisation and hesitation: international intelligence co-operation in practice', unpublished paper, 17 Oct. 2008.

[32] Richard Aldrich, 'Transatlantic intelligence and security cooperation', *International Affairs* 80: 3, May 2004, pp. 733–55.

[33] Audrey Cronin, 'Behind the curve: globalization and international terrorism', *International Security* 27: 3, 2003, pp. 30–58.

[34] Walter Laqueur, 'Postmodern terrorism', *Foreign Affairs* 75: 5, 1996, pp. 24–36; Bruce Hoffman, *Inside terrorism* (London: Victor Gollancz, 1998).

[35] Ersun Kurtulus, 'The "new terrorism" and its critics', *Studies in Conflict and Terrorism* 34: 6, 2011, pp. 476–500.

[36] Peter R. Neumann, *Old and new terrorism: late modernity, globalization and the transformation of political violence* (Cambridge: Polity, 2009); John Arquilla, David Ronfeldt and Michele Zanini, 'Networks, netwar, and information age terrorism', in Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt and Michele Zanini, eds, *Countering the new terrorism* (Santa Monica: RAND, 1999); Steven Simon and Daniel Benjamin, 'America and the new terrorism', *Survival* 42: 1, 2000, pp. 59–70.

[37] Jennifer Yang Hui, 'Crowdsourcing terrorism: utopia, martyrdom and citizenship reimagined', *Journal of Asian Security and International Affairs* 4: 3, 2017, pp. 337–52; Ahmed Al-Rawi, 'Video games, terrorism, and ISIS's Jihad 3.0', *Terrorism and Political Violence* 30: 4, 2018, pp. 740–60; Yannick Veilleux-Lepage, 'Paradigmatic shifts in jihadism in cyberspace: the emerging role of unaffiliated sympathizers in Islamic State's social media strategy', *St Andrews Journal of International Relations* 7: 1, 2016, p. 36.

[38] Peter Singer and Emerson Brooking, *LikeWar: the weaponization of social media* (New York: Houghton Mifflin, 2018), pp. 44–5.

platforms. This was combined with the release in 2007 of Apple's iPhone, another leap in mobile telecoms that combined small size with tailored apps. Enabled by a 13-fold increase in processing speed between 1999 and 2017, these innovations would eventually provide similar audio-visual editing capabilities to a studio, on a portable and user-friendly device, linked to the global internet. Complementing this step-change in technology, by 2013 there were 2 billion mobile internet subscriptions, and by 2018, 6 billion.[39] The impact on societies of this ability to access, create, distribute and interact with written and audio visual information globally and in real time has been likened to that of the alphabet.[40] At the same time, it is important to note that these ICTs have facilitated an increase in the pace of societal change. It is perhaps not too much to suggest that these technological evolutions may have had a similarly profound impact on global jihadism.

Jihadism 1.0

In this first epoch, jihadist organizations sought to conduct coordinated mass casualty suicide attacks against iconic targets for maximum dramatic effect. The targets were symbols of western political and military power: global cities and capitals of the 'far enemy' and their transport systems, especially air and rail. In stark difference to the hijackings of the Cold War era, aimed at gaining international attention without causing huge casualties, Jihadism 1.0 deliberately sought to inflict mass harm. Such large terrorist attacks required long-term planning, coordinated collective action with trained operatives and a support network. Bin Laden's AQC, which emerged as a global actor in the 1990s, provides the best example, displaying a top-down, bureaucratic and hierarchical command structure with a physical headquarters. The organization's survival relied on its good relations with, and often support from, host states.[41] New members were primarily recruited from Muslim countries and in many cases were experienced veterans of the Afghan or Balkan wars. In most cases, these jihadists travelled to remote locations to pledge allegiance and receive training, funding and instructions. These expensive recruitment and operational strategies were financed by the leadership and its businesses, by private donors or through foreign fundraising campaigns, including ostensibly charitable activities. Once Jihadism 1.0 had evolved ideologically to the 'America First' position, it ceased to restrict itself to targeting western diplomatic missions in the global South and aimed its attacks instead at western 'enemy' territory and transit routes.

Technologically, Jihadism 1.0 spanned both the late analogue and early digital eras, displaying numerous characteristics that distinguish it from later phases. First, AQC needed the acquiescence of host governments to operate,

[39] Singer and Brooking, *LikeWar*, p. 48.

[40] Manuel Castells, quoted in Paul DiMaggio, Eszter Hargittai, W. Neuman and John Robinson, 'Social implications of the internet', *Annual Review of Sociology* 27: 1, 2001, pp. 307–36.

[41] Ken Booth and Tim Dunne, *Worlds in collision: terror and the future of global order* (Basingstoke: Macmillan, 2002), p. 15.

negotiating deals with the leaders of Sudan and later Afghanistan.[42] Second, reflecting the analogue era in which it was conceived, AQC followed a hierarchical, almost micro-managerial, highly bureaucratic organizational structure.[43] AQC documents captured during the 2011 US special forces raid on Bin Laden's Abbottabad compound revealed he had acted as AQC's 'chief executive, fully engaged in the group's myriad crises, grappling with financial problems, recruitment, rebellious field managers and sudden staff vacancies'.[44] Bin Laden was a 'hands-on' manager; there is evidence of discussions about personnel promotions, and detailed accounting of organizational cash flows. There was even an AQC application form that included questions such as what 'hobbies' the applicant might have.[45] Bin Laden used traditional media—high-profile newspapers and television interviews—to spread his message and recruit followers; propaganda material was also distributed through video cassettes and later DVDs. While AQC's output at this time was dominated by long monologues by Bin Laden berating the West, or on the finer theological points of jihad, neither of which had mass appeal, it did attract a core of about 170 volunteers from across the globe to the organization, including Khalid Sheikh Mohammed.[46] To sustain this network of international jihadists, AQC's leadership communicated with and gave orders to their operators mostly via telephones or couriers.

During AQC's heyday between 1992 and 2001, its targeting evolved. The first bomb attack was planned in 1995 under the name Operation Bojinka—a plot to simultaneously bomb twelve passenger aircraft flying to the United States over the Pacific. One of the plotters, Abdul Hakim Murad, told the police that he had been trained to fly an aircraft into CIA headquarters in Langley, and that his AQC handler was also finalizing a plot to kill the Pope during a visit to the Philippines. Although the authorities disrupted the plot, it signalled a tactical shift from the jihadism of the late Cold War era, focused on action against the 'near enemy', towards much more destructive and dramatic attacks against iconic targets of the 'far enemy'.[47] US diplomatic and military missions in the global South also became targets. In 1998, AQC staged large, simultaneous bombings of the US embassies in Tanzania and Kenya, killing 257 people and injuring thousands more. The scale and simultaneity of these attacks indicated a new sophistication in planning and execution. Bin Laden used a satellite phone to coordinate the attacks, and—to claim responsibility and ensure the maximum exposure—his associates used a fax machine to communicate with the traditional media. During 1998, plots to bomb US embassies in Albania, Uganda and Ivory Coast were also disrupted.[48]

[42] Booth and Dunne, *Worlds in collision*.
[43] Michael Chertoff, comments at International Centre for Countering Terrorism conference, 12 Sept. 2016, https://www.ict.org.il/Article/1831/honorable-michael-chertoff-ict16#gsc.tab=0.
[44] 'Bin Laden's last stand', *Washington Post*, 30 April 2012, https://www.washingtonpost.com/world/national-security/bin-ladens-last-stand-in-final-months-terrorist-leader-worried-about-his-legacy/2012/04/30/gIQAStCjsT_story.html.
[45] 'Secrets of the bin Laden treasure-trove', CNN, 2 May 2016.
[46] Timothy Naftali, *Blind spot: the secret history of American counterterrorism* (New York: Basic Books, 2005), pp. 260, 269–70.
[47] Naftali, *Blind spot*, pp. 239–40.
[48] Naftali, *Blind spot*, p. 265.

Table 1: Jihadism 1.0–4.0: global jihadism from the 1990s to the present and beyond

	ICTs	*Organization*	*Recruitment and training*	*Financing*	*Tactics*	*Targets*	*Responses*
Jihadism 1.0 (1990s–)	Analogue: video cassette, telephones and fax machines, couriers, traditional media Early digital: satellite phones and Web 1.0	Top-down directed, hierarchical, bureaucratic; state acquiescence; analogue communications	Overseas travel to central organization; training camps	From central organization; global fundraising operations	Trained groups; sophisticated planning; large bombs, weaponized aircraft; suicide mass casualty attacks; iconic targets; long preparation time	'Big event'—dramatic scale in centres of western political power and on transport systems	New security architectures: predominantly signals intelligence, coupled with military interventions to deny sanctuaries and integrate forensic data; surgical operations overseas, often via drones; CNI protection; restrictions on immigration and travel to the US
Jihadism 2.0 (2003–)	Early to late Web 2.0: advanced apps, encryption, real-time use of social media in attacks	Distributed command with some higher communication and direction	Some overseas travel to franchises, blended with increasingly rapid home-grown radicalization and criminality	Decentralized franchises, crowdsourced	Trained groups: coordinated and sophisticated marauding gun and skilled bomb attacks, shorter preparation time, suicide	Numerous coordinated smaller attacks on soft targets = cumulative impact	Increased international intelligence liaison; more rapid and professional response teams; increased protective measures at stadiums and large public gatherings; community policing
Jihadism 3.0 (2007–)	Late Web 2.0, Dark Web, virtual reconnaissance	Loose network enabled by lone actors	Online only, individual, little or no training; many recruits have psychological issues	Individual	Untrained and inexperienced individuals: knives, automobiles, guns and homemade bombs; some attacks suicidal, some not	Random, but highly visible, in public places to create constant fear of attack	Metadata and whitelisting; human intelligence, community policing; increased protection of public spaces in general.
Jihadism 4.0 (2015–)	Hacking Web 2.0 and cloud computing, including semi-secure and secure ICT systems; artificial intelligence, deepfakes; quantum computing	Full spectrum, from lone actors to highly organized groups	Online	Crowdsourced; state-sponsored; individual	Trained groups and individuals: cyber attacks to cause physical damage and casualties; reputational damage; intimidation	Critical National Infrastructure (CNI); media outlets; public servants and figures; government websites and databases	Increased protection of CNI cyberspace; raising public awareness of cyberterror evolution; less personal data on social media profiles

Al-Qaeda's fixation on globally iconic targets of the far enemy manifested itself to the full in the attacks of 11 September 2001, when 19 AQC operatives flew two aircraft into the World Trade Center and a third into the Pentagon. A fourth plane crashed before reaching its target in Washington DC. The targets were highly visible global symbols of US political and military power. Killing nearly 3,000 people and injuring twice as many, the events of 9/11 constituted the largest terrorist attack in history, delivering a huge global impact and marking a step-change in global jihadist tactics. The plot was centrally planned over a long period, directed by AQC and carried out by AQC members who had travelled abroad for recruitment, training and funding. The key innovation was the exploitation of gaps in US transportation security architecture to weaponize aircraft as suicide missiles.

The post-9/11 era saw a refinement of Jihadism 1.0. Although still aiming to cause mass casualties and targeting transport infrastructure, global jihadists were forced to adapt under the pressure of western military interventions to reduce their sanctuaries, coupled with increased homeland security and intelligence efforts. Most notably, they began to evolve different forms of strategies, organization, recruitment and financing, moving slowly towards a more decentralized model of loosely structured groups of largely western-based attackers.[49] These were inspired by AQC but were not necessarily in constant or direct communication with the central organization; most claimed to be using jihadist terrorism in response to the western interventions in Afghanistan and Iraq. In a number of cases, post-9/11 jihadists were west European nationals. Later manifestations of Jihadism 1.0, then, exhibited an evolution from foreign terrorists attacking foreign countries to a home-grown/domestic version of global jihad.

An example of Jihadism 1.0 in this latter form is the foiled 'liquid bomb plot' of August 2006—a plan to detonate bombs in seven aircraft in mid-flight over the Atlantic by using homemade liquid explosives disguised as soft drinks and in battery casings. Eighteen suicide bombers were involved in this attempt, inspired by AQC through their handler Rashid Rauf, who had fled his native Birmingham for Pakistan after killing his uncle. Several of the attackers had visited Pakistan from the UK, and were planning to use innovative liquid explosives technology to evade airport security screening. However, their initial communications were intercepted by British and American agencies, as were further efforts to communicate from internet cafés. Despite these efforts to innovate, the jihadists still planned to claim responsibility via traditional pre-recorded martyrdom tapes.[50] Similarly, the 2004 Madrid train bombings and the 2005 London attacks remained focused on transport infrastructure in 'far enemy' capitals; but these plots represented the beginning of the evolution towards Jihadism 2.0 organization and attacks, in that neither displayed much known contact with AQC. This evolution towards decentralized command and control was primarily facilitated by developing major advances in ICTs.

[49] Naftali, *Blind spot*, p. 259.
[50] 'The liquid bomb plot', *Real Stories*, https://www.youtube.com/watch?v=OIJFiqy35KM.

Jihadism 2.0

Jihadism 2.0 embodies the realization that a number of smaller, coordinated attacks by groups of jihadists can have a large global impact. This realization came about largely as a result of the degradation of AQC by international counterterrorism efforts, and it resulted in the beginnings of a less centralized and hierarchical approach to global jihadist organization. This, in turn, was enabled by the increasing connectivity of both Web 2.0 and the advanced mobile phones that access its platforms in real time. Jihadism 2.0 is characterized by more distributed and flexible organization with some, but more limited, communication with the leadership; a mix of radicalization and training at home and abroad; collective, well-planned, marauding attacks assisted by advances in mobile telecommunications and Web 2.0 technologies; and the increasing use of Web 2.0 for recruitment, propaganda and financing. Indeed, without Web 2.0 there would be no Jihadism 2.0. While not a fully networked and decentralized organizational approach, Jihadism 2.0 represents an important evolution towards it.

A number of scholars have noted how the rapid growth of the early Web 2.0 capabilities began to change terrorism in general and global jihadism in particular.[51] By the early 2000s, AQC had begun to disseminate low-quality videos featuring its battle triumphs in Afghanistan and Iraq, uploaded from internet cafés in the global South to increasingly popular jihadist websites on the 'surface', or publicly available, web.[52] Awan and Al-Lami argue that the shift away from Jihadism 1.0 websites was in part the result of their removal by counterterror organizations after 9/11, which forced the creation of web content, like the physical jihadist organizations, to shift away from centralized control.[53] The emergence of Al-Qaeda in Iraq (AQI) in 2004, and of Al-Qaeda in the Arabian Peninsula (AQAP) and Al-Qaeda in the Islamic Maghreb in 2009, highlighted the recognition by jihadists that a more localized and franchised distribution of power would strengthen their resilience. In many respects, AQI and its leader Abu Musab al-Zarqawi were the innovators of early Jihadism 2.0. Organizationally, although AQI took some strategic direction from AQC, it was independently commanded by Al-Zarqawi, and also structured around a more cellular system than AQC, exploiting increasingly available mobile phone technology to communicate. According to General Stanley McChrystal,

> most importantly … [ICTs] allowed [AQI] to control both the pace and the narrative of violence. With the ability to connect its nodes at a rapid pace, [ICTs] facilitated AQI's growth into a broader network, which in turn fuelled its ability to seem larger and speedier than it actually was.[54]

However, this reliance on mobile phones eventually made AQI relatively easy to dismantle with advanced signals intelligence.[55] Al-Zarqawi's emphasis on mass

[51] Gabriel Weimann, *Terror on the internet: the new arena, the new challenges* (Washington DC: United States Institute of Peace, 2006).
[52] Veilleux-Lepage, 'Paradigmatic shifts in jihadism', p. 36.
[53] Aki Awan and Mina al-Lami, 'Al-Qa'ida's virtual crisis', *RUSI Journal* 154: 1, 2009, pp. 56–64.
[54] Sean McFate, *Goliath* (London: Penguin, 2019), p. xii.
[55] Mark Urban, *Task Force Black* (London: Abacus, 2011).

membership also made AQI distinct in its messaging, recruitment and finance. In 2004, Al-Zarqawi outlined his strategy and tactics in a 30-minute online video designed to promote brand recognition, while the emerging brutality of Jihadism 2.0 was highlighted by the video showing the decapitation of Nicholas Berg—viewed over 15 million times online—that followed.[56] These videos combined the user-friendliness of YouTube with better production values and scripted narratives. Complementing this was an increasing use of film-makers to record AQI attacks, which were then posted on video streaming sites for recruitment and funding purposes.[57] A 2008 study of comments below YouTube suicide attack videos in Iraq concluded that global jihadist messaging was 'spreading far beyond traditional Jihadist websites or even dedicated forums to embrace … video sharing and social networking—both hallmarks of Web 2.0—and thus extending their reach far beyond what may be conceived as their core support base'.[58]

The 2008 Mumbai attacks, when ten terrorists assaulted six 'soft' sites across the city for a total of 60 hours, killing 164 people and wounding another 300, provide a striking example of how Web 2.0 enabled a new type of global jihadist tactic. This became known as a marauding attack, where numerous targets in a city are hit simultaneously to cause maximum casualties and media exposure while stretching response teams. The attacks highlighted the effectiveness of coordinated, but comparatively less planned, attacks against soft targets by terrorists with relatively basic weapons who were able to communicate in real time, and were willing to die. But what was truly innovative about the Mumbai attacks was that, as a result of the plethora of social media updates from affected citizens—including pictures and geo-located GoogleMap tags—the attackers' handlers in Karachi could monitor the incidents on the internet in real time and direct them to more targets, including relaying victims' locations through their own social media updates, making the attacks even more lethal.[59] This tactic would not have been possible without Web 2.0. Nor would the response, with internet users quickly censoring content that could benefit the terrorists, spreading messages from the security services and providing them with information in what has been termed the first 'crowdsourced' counterterrorism response.[60]

Although the Taliban conducted a number of complicated marauding attacks in Afghanistan in the following years, it was attacks in Paris and Brussels, linked to ISIS, that provided the starkest evidence of Jihadism 2.0 after Mumbai. Between 7 and 9 January 2015, two brothers, Cherif and Said Kouachi, and Amedy Coulibaly killed 17 civilians and injured 23 in a series of shootings known as the *Charlie Hebdo*

[56] Urban, *Task Force Black*.
[57] Monica Maggioni, 'The Islamic State: not that surprising, if you know where to look', in Monica Maggioni and Paolo Magri, eds, *Twitter and jihad: the communication strategy of ISIS* (Milan: Italian Institute for International Political Studies, 2015), pp. 49–81.
[58] Maura Conway and Lisa McInerney, 'Jihadi video and auto-radicalisation: evidence from an exploratory YouTube study', unpublished paper, 2008, p. 10.
[59] Ohnook Oh, 'Information control and terrorism: tracking the Mumbai terrorist attack through Twitter', *Information Systems Frontiers* 13: 1, 2011, pp. 33–43.
[60] Singer and Brooking, *LikeWar*, p. 64.

attacks.[61] These displayed numerous characteristics of Jihadism 2.0. Tactically, the coordinated marauding assaults were the first by global jihadists in Europe: their selection of numerous soft targets, and their willingness to die, severely tested the French security forces' response. Second, the attackers were initially radicalized in France, but in 2011 both the Kouachi brothers travelled to Yemen, where they received training and funding from AQAP, and their actions were probably coordinated by another ISIS member. Third, the terrorists used firearms bought from criminal networks, exposing a local-crime–global-terror nexus. Perhaps the most sophisticated example of Jihadism 2.0 occurred on 13 November 2015, when three ISIS cells near-simultaneously attacked the Stade de France, Parisian restaurants and the Bataclan Theatre, using suicide vests and assault rifles. The attackers, led by Abdelhamid Abaoud of ISIS' external operations wing, killed 130 people and wounded 494.[62] These Jihadism 2.0 marauding attacks were notable for their complexity, coordination and brutality, including tactics developed to frustrate the counterterrorist response. For example, in the Bataclan Theatre assault gunmen with experience of fighting in Syria were positioned outside exits to kill fleeing civilians and defend the building from French counterterrorism teams. Other attackers had no training and had been radicalized at home, reflecting the blended approach of Jihadism 2.0. The assailants communicated with one another using disposable mobile phones and those taken from their victims, and with their handlers via Web 2.0 apps on encrypted computers, coupled with written notes to evade detection before, during and after the attacks. In all these ways, the Paris attacks marked a significant escalation in the capabilities, intent and tactics of global jihadists in Europe.[63] Indeed, a former director of the United States' National Counterterrorism Center stated the attacks demonstrated a sophistication not seen since Mumbai.[64] Other examples of Jihadism 2.0 are the three coordinated suicide bomb attacks on Zaventem Airport and Maalbeek metro station in Brussels in March 2016. Thirty two civilians were killed, and 316 people injured, when two Belgian-Moroccan brothers, the El-Bakraouis, and another Moroccan attacker, Najim Laachraoui, detonated suicide vests. The El-Bakraouis were dangerous criminals known to Belgian police; one was the subject of an international terrorism arrest warrant and the other had been detained in Turkey for attempting to join ISIS, while Laachraoui had trained with ISIL in Syria and was the skilled bombmaker behind the Paris attacks.

These attacks shared numerous important traits that mark an evolution from Jihadism 1.0. First, they were perpetrated on multiple soft targets, often simultaneously, by small groups whose members were willing to die, involving close coordination and some planning. However, these attacks, while still effective, by their nature produced fewer casualties than those of 9/11 or those planned by

[61] 'Charlie Hebdo attack: three days of terror', BBC News, 14 Jan. 2015, https://www.bbc.co.uk/news/world-europe-30708237.
[62] '2015 Paris terror attacks fast facts', CNN editorial research, 13 Nov. 2019, https://edition.cnn.com/2015/12/08/europe/2015-paris-terror-attacks-fast-facts/index.html.
[63] 'How ISIS built the machinery of terror under Europe's gaze', *New York Times*, 29 March 2016.
[64] 'Paris attacks: ISIS supporters celebrate, but who's to blame?, NBC News, 14 Nov. 2015.

the 2006 airline plotters; there is a difference in scale. Second, they all involved firearms or advanced bomb attacks conducted by groups, some of whose members had travelled overseas for training, and others of whom were radicalized at home, and often had criminal backgrounds. In numerous cases, this home-grown radicalization was much faster than that of Jihadism 1.0. Third, while all the groups involved some form of communication with, and control and funding from, their global terrorist organization, their organizational structure was much more decentralized. This displays both the blend of home-grown and overseas radicalization and training that characterizes Jihadism 2.0 terrorists, and their continuing interaction with organizational handlers. Finally, they displayed increasingly sophisticated ICT skills in both conducting their attacks and communicating them globally through digital technologies, combined with, in some cases, an awareness of counter-intelligence measures, largely enabled by Web 2.0. The Paris attackers displayed the most sophisticated use of these, including so-called Dark Web platforms like Tor (a free and open-source software for enabling anonymous communication, launched in 2006) and Telegram (an encrypted instant messaging, file-sharing and voiceover service, launched in 2013), while some of the weapons used in the attacks are believed to have been bought from criminals using bitcoin on the Dark Web.[65] Bitcoin and other cryptocurrencies offer terrorists the benefit of anonymity, which they exploit to fundraise, and transfer and purchase weapons, illegally in a crowdsourced approach to terrorist financing. Clearly, then, there are marked differences between Jihadism 1.0 and Jihadism 2.0.

Jihadism 3.0

Although some characteristics of Jihadism 3.0 coexist with the latest versions of Jihadism 2.0, the third epoch is distinguished by its embodiment in individually motivated actors, its lack of any assistance from the central terrorist organization and its often crude tactics. Jihadism 3.0 is also impossible without advanced Web 2.0 platforms that enable ostensibly 'lone' operators to become radicalized and launch individual attacks. Tor and Telegram are good examples of such platforms: the growth in Telegram's popularity among jihadists is itself a result of international efforts to remove ISIS-related content from the surface Web and the change of online strategy this caused, and the platform's introduction of its tailored content function in 2015.[66] The use of these ICTs marks another notable shift away from Jihadism 1.0's comparatively open use of surface Web chat boards and forums, and allows individuals susceptible to radicalization to access video and audio content with reduced risk of being traced. A large proportion of jihadist discourse now takes place on the Dark Web; as former FBI Director James Comey stated in December 2015: 'Increasingly, we are unable to see what [terrorists] say, which gives them a tremendous advantage.'[67] At the same time, ISIS is producing

[65] Gabriel Weimann, 'Terrorist migration to the Dark Web', *Perspectives on Terrorism* 10: 3, 2016, pp. 40–45.
[66] Weimann, 'Terrorist migration to the Dark Web', p. 42.
[67] Weimann, 'Terrorist migration to the Dark Web', pp. 40–42.

slickly crafted internet videos and even video games to recruit and finance its organization.[68] Despite big technology companies removing vast quantities of online material, content on the surface Web also remains an enabler of Jihadism 3.0, often rapidly reappearing on another part of the internet after removal from one location.[69]

Enabled by these ICT advances, Jihadism 3.0 seeks out individuals who cannot be (and are not) directly trained or recruited face-to-face, and are not operationally assisted with planning by the central terrorist organization. It is these technologies that Al-Suri's 'personal jihad' strategy directly exploits; 3.0 jihadists are inspired to pick up whatever weapon is at hand (knife, automobile, gun, homemade bomb) and randomly kill. For example, in 2016 ISIS' online English-language magazine, *Rumiyah*, directly called for knife and vehicular attacks in the West in response to the military intervention against the group in Syria and Iraq.[70] These jihadists' methods are crude and their targets are soft, often selected randomly in public spaces. While these types of jihadist attack are not on the same scale even as those of Jihadism 2.0, their effectiveness is derived from their psychological impact—the uncertainty and public fear they generate that at any moment someone may attack—and the fact that they need no organization, direction or funding from the central terror organization.

In the West, the first manifestations of Jihadism 3.0 were apparent in the separate attacks of 20–22 December 2014 in Tours, Dijon and Nantes, which killed one person and injured 25 others in a series of vehicular and knife attacks. All the attackers had radicalized online and none had any direct links with terrorist organizations; two of them had a history of mental illness. The attacks followed the call from ISIS in September 2014 for Muslims in the West to attack infidels with rocks and cars in response to the start of US airstrikes against the group. Another example of Jihadism 3.0 is the attack of 2 December 2015 in San Bernardino, California, in which 14 people were killed and 22 others injured in a mass shooting and an attempted bombing by Syed Farook and Tashfeen Malik.[71] The attackers used easily available but modified weapons, and explosives they had learned how to make on the internet. According to the FBI, although Farook and Malik had both self-radicalized individually online before they met and were possibly inspired by foreign terrorist organizations, there was no indication that they were directed by any such group or were part of a broader cell.[72] Another example came on 14 July 2016 in Nice, when a 19-tonne cargo truck was deliberately driven into crowds of people celebrating Bastille Day on the Promenade des Anglais, killing 86 and injuring 450.[73] The driver, Mohamed Lahouaiej-Bouhlel, a Tunisian French resident, was shot dead by police, and ISIS later claimed responsibility for the attack. According to the French authorities, although Lahouaiej-Bouhlel had

[68] Al-Rawi, 'Video games, terrorism and ISIS's Jihad 3.0'.
[69] Glazzard, 'Shooting the messenger'.
[70] 'ISIS recently called for the type of attack that just happened at Ohio State', *Business Insider*, 29 Nov. 2016.
[71] 'San Bernardino shooting: 22nd injured victim steps forward, FBI says', *The Press-Enterprise*, 9 Dec. 2015, https://www.pe.com/2015/12/09/san-bernardino-shooting-22nd-injured-victim-steps-forward-fbi-says/.
[72] 'San Bernardino shooting: couple radicalized before they met, FBI says', CNN, 10 Dec. 2015.
[73] 'France remembers the Nice attack: "We will never find the words"', *New York Times*, 14 July 2017.

a record of petty crime, he was 'completely uninvolved in religious issues and not a practising Muslim, who ate pork, drank alcohol, took drugs and had an unbridled sex life'.[74] Lahouaiej-Bouhlel also had a history of psychiatric problems, and, like some of the Paris attackers, had been rapidly radicalized. After the attack his computer was found to contain photos of ISIS fighters and beheadings, Bin Laden, the ISIS flag, and images linked to extreme Islamism.[75] While Lahouaiej-Bouhlel had communicated with known extremists in his neighbourhood, French authorities did not uncover links to ISIS central authority. Other examples of this type of crude, individually inspired Jihadism 3.0 attacks have occurred in Westminster, the Champs-Élysées, Milan, Linz, Brussels and New York since 2017.

Clearly, the development of ICTs has enabled, rather than caused, the emergence of Jihadism 3.0; each attacker had his own motivations for becoming a terrorist, which were simply facilitated by the presence of internet propaganda. Even so, a number of trends are apparent: first, the relative rapidity of radicalization and its online-only nature, often juxtaposed with a previous history of un-Islamic behaviours such as drinking and drug-taking; second, the use of cruder tactics; third, learning from the internet rather than physical weapons training and planning abroad (including use of the internet for planning: for example, the 2017 Westminster Bridge attacker conducted a prior reconnaissance of targets using Google Streetmaps); fourth, a lack of communication with the central terrorist organization and the increasing prominence of individual attackers; fifth, an increasing incidence of attackers with psychiatric problems and links to criminality. Clearly, none of these trends are mutually exclusive with Jihadism 1.0 or 2.0; rather, we can observe a coexistence between the characteristics of the various phases as terrorist strategy, organization, training, funding and tactics evolve to exploit ICTs. For example, the August 2017 Barcelona attackers blended both crude vehicular and homemade bomb attacks with a decentralized organizational structure more fitting with Jihadism 2.0, while some of the June 2017 London Bridge attackers had been radicalized abroad but employed crude tactics.

Jihadism 4.0

Jihadism 4.0 represents the evolution of jihadists' use of the internet as an operational tool for conducting attacks. It draws its lineage from Jihadism 2.0 and 3.0 and can coexist with both. Although discussions about terrorists using cyberspace to stage attacks are not new, jihadist groups have not yet obtained the capability of states in this respect. Nevertheless, groups affiliated to ISIS pursue activities in cyberspace which go beyond the recruitment, propaganda or financing associated with Jihadism 2.0 and 3.0. For example, in 2015 ISIS hackers took over the Twitter accounts of the US Central Command and *Newsweek* magazine,[76] highlighting

[74] 'Lahouaiej Bouhlel dragueur impénitent et ultraviolent à l'interêt récent pour le jihadisme', *La Nouvelle Republique*, 18 July 2016.
[75] 'Attack on Nice: who was Mohamed Lahouaiej-Bouhlel?', BBC News, 19 August. 2016.
[76] Spencer Ackerman, 'US Central Command Twitter account hacked to read "I love you Isis"', *Guardian*, 12 Jan. 2015.

their increased capability, and spreading fear. In 2015 and 2016, two online groups pledging allegiance to ISIS emerged in the cyber domain—the Islamic State Hacking Division (ISHD) and the United Cyber Caliphate (UCC).[77] The UCC published 'kill lists' containing names of government and military personnel and civilians with instructions for ISIS supporters to assassinate them.[78] Similarly, in 2015 the ISHD published its own 'kill list' of 1,400 mostly US military personnel.[79] Although there is no available evidence of deaths resulting from these lists, by publicizing the names of US government employees ISIS clearly demonstrated an increased appetite for creating synergy between its online operations and actions in the physical space, both of which spread fear and cause personnel to enhance their security. That ISIS did this at minimal cost, via publicly available hacking technology, highlights the impact of cheap ICTs on jihadist tactics. When defined as 'unlawful attacks … against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives', these operations meet the criteria of 'cyberterrorism'.[80] Other definitions are harder to meet, as attacks would have to result in violence against persons or property, or cause enough harm to generate widespread fear.[81] Meeting this higher threshold might prove more difficult in the short term, but counterterrorism professionals expect terrorists to continue to develop this kind of capability. At its most extreme, Jihadism 4.0 could evolve into malware attacks to cause human casualties and physical damage to infrastructure.

Evolving responses

Each of these phases of the jihadist phenomenon usually displays one or two defining attacks that highlight the changed paradigm to security services. In the aftermath of 9/11, the security agencies in the United States recognized they were dealing with a group of jihadists largely from overseas, where they had elaborately planned, trained and financed their attacks over a long period. These jihadists' hierarchical, almost micro-managerial, approach meant that they had to move money, travel and communicate globally. This type of organization had a relatively loud signal, and each of these preparation and planning elements was a vulnerability that could be exploited by an intelligence apparatus correctly built to collect, analyse and share what was happening. This response included a focus on using signals intelligence abroad, complemented with human intelligence assets, to disrupt 1.0 jihadists. This approach was supported by the military intervention in Afghanistan to disrupt training sites and laboratories, and the incorporation of law enforcement techniques on the battlefield in order to extract forensic data to

[77] Dominika Giantas and Dimitrios Stergiou, 'From terrorism to cyber-terrorism: the case of ISIS', SSRN paper, publ. online 12 March 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927.
[78] Giantas and Stergiou, 'From terrorism to cyber-terrorism', p. 15.
[79] Michael Safi, 'Australians on ISIS-aligned group's hit list include Victorian MP', *Guardian*, 13 Aug. 2015.
[80] Dorothy Denning, 'Cyberterrorism', testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, Washington DC, 23 May 2000.
[81] Lee Jarvis and Stuart Macdonald, 'What is cyberterrorism? Findings from a survey of researchers', *Terrorism and Political Violence* 27: 4, 2015, pp. 657–78 at p. 659.

build the intelligence picture. For example, FBI forensic specialists were deployed at safe houses in Afghanistan and Iraq to take fingerprints which were then fed back into US border security systems.[82] This contributed to the creation of an integrated system to vet who entered the United States and to reduce vulnerabilities of critical infrastructure, including air and other transport. This approach to dealing with externally imported Jihadism 1.0 was very successful.

Recognizing the critical differences between Jihadism 1.0, 2.0 and 3.0 is essential to shaping counterterrorism responses. One key feature of the latter forms is that the line between ideological jihadist terrorism and criminality is less clear than with Jihadism 1.0. Unlike the early global jihadists, most 2.0 and 3.0 jihadists have not been radicalized over a long period of time and gradually motivated to become operational; instead, a number of 2.0 and 3.0 jihadists have been observed drinking whiskey, taking drugs and attending nightclubs, demonstrating little adherence to Islam, a week before their attacks.[83] Many have been petty criminals known to police; some have been serious criminals; many have been living at the margins of society. In this case the organization or ideology can act like a gang—attracting recruits through their powerful and marginalized narrative while also offering redemption from past sins through jihadist struggle. Jihadism 2.0 recruitment therefore presents a different set of problems from those of Jihadism 1.0 in terms of the collection and analysis of information. A second key feature of Jihadism 2.0 and 3.0 is their low signature. Compared with Jihadism 1.0, there is less global communication, less international travel and fewer flows of money to track with traditional high-tech signals intelligence. For example, the San Bernardino attackers did not need to communicate over the internet as they lived together. There is also, especially in the case of Jihadism 3.0, a shorter time between radicalization and operationalization—the so-called 'flash to bang' effect—increasing the pressures on intelligence agencies and counterterrorist response teams. A third feature of Jihadism 2.0 and 3.0 is the plethora of targets; efforts to identify critical infrastructure (as was done after 9/11) will not be effective when everything and anyone can be a target, from shopping centres and cinemas to arenas and public streets. Fourth, although smaller in scale than Jihadism 1.0 attacks, the greater frequency of attacks in Jihadism 2.0 and in particular 3.0 is important, as it undermines public trust in governments' ability to protect citizens. This is particularly the case as the terrorist use of drones increases. Thus, restoring confidence by 'flooding the zone' has proved critical in maintaining trust in the wake of attacks, as evidenced in France's 24-month state of emergency following the Paris attacks. Finally, in terms of responses to Jihadism 4.0, US Cyber Command has for a number of years been conducting network attacks against ISIS and other jihadist groups. The most high-profile of these was the Joint Task Force ARES operation in 2016; it hacked ISIS accounts to disrupt not only their online media wing, but also the group's finance and recruitment operations. ARES drained members'

[82] Authors' information.

[83] 'Two suspects sold bar in Brussels not long before Paris attacks', *Wall Street Journal*, 18 Nov. 2015; 'Europe's joint-smoking, gay-club hopping terrorists', *Foreign Policy*, 13 April 2016.

mobile phone batteries though the internet, weakening command and control, while also using hacks to spread fear and confusion.[84]

Potential application to other forms of terrorism

We argue that the utility of our 1.0–4.0 ICT typology may well extend beyond jihadism. In terms of 'Terrorism 1.0', US far-right terrorists were the first to organize on Web 1.0, while the mid-1990s saw the Irish Republican Army begin to target iconic sites on the British mainland with much larger bombs, as in the attacks on Bishopsgate (1993), Manchester (1994) and Canary Wharf (1996). In terms of 'Global Terrorism 2.0', scholars have shown how New IRA splinter groups have used Web 2.0 in similar ways to jihadists.[85] Elements of far-right Terrorism 2.0 were evident in the activities of a British Army neo-Nazi cell whose members were convicted of terrorist offences in 2018, while 'Global Terrorism 3.0' has clear resonances with the far-right attacks on the Pittsburgh Synagogue in 2018 and in Dayton and Christchurch in 2019—the latter marking a gruesome but not unexpected evolution when the attacker streamed his actions live on Facebook. The 2011 Norwegian attacks were perpetrated by an individual radicalized online but were well planned and lethal for a lone attacker, highlighting the overlap between 2.0 and 3.0 in far-right terrorism.[86] In terms of 'Global Terrorism 4.0', there is also growing evidence of far-right use of social media to intimidate individuals, while in 2011 the radical hacking group Lulz took down the websites of the CIA, the US Senate, the Arizona State Police and the British Serious Organized Crime Agency, publishing sensitive information.[87] Similarly, in 2015 a British hacker used the internet to 'terrorize' US security chiefs over a sustained period.[88] We suggest, then, that our typology may provide a fruitful basis for future research on other terrorist organizations. Moreover, there is ample evidence to suggest that our technology typology is more widely applicable to recent developments in international security, international relations and politics.

In order to address the challenges that both Jihadism and Terrorism 2.0 and 3.0 create, counterterrorism organizations must also evolve. First, and most important, the way intelligence has traditionally been conceived in terms of spies and satellites needs to be broadened to include bottom-up community intelligence. Traditionally, some nations have been better than others at this, but it is clear that Terrorism 2.0 and 3.0 require a greater emphasis to be placed on the community

[84] Michael Martelle, ed., *Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's internet war against ISIL*, briefing book no. 637 (Washington DC: National Security Archive, 13 Aug. 2018).

[85] Matthew Warren and Shona Leitch, 'New media and Web 2.0: an Irish Republican example', *Journal of Information Warfare* 11: 1, 2012, pp. 1–11.

[86] 'Norway attacks: at least 92 killed in Oslo and Utøya island', *Observer*, 23 July 2011, https://www.theguardian.com/world/2011/jul/23/norway-attacks.

[87] Parmy Olson, *We are Anonymous: inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency* (New York: Back Bay Books, 2013), pp. 244, 441–2; Ellen Messmer, 'Alleged members of hactivist group LulzSec busted; LulzSec leader "Sabu" allegedly turns in fellow hackers', *Network World*, 6 March, 2012, https://www.networkworld.com/article/2187413/alleged-members-of-hactivist-group-lulzsec-busted.html.

[88] 'Two years for teen "cyber terrorist" who targeted US officials', *BBC News*, 20 April 2018, https://www.bbc.co.uk/news/uk-england-leicestershire-43840075.

than has been the case in many polities, so that information can be collected and better integrated into the intelligence picture. Clearly, community-based police officers, community leaders, teachers and mental health professionals may have useful insights suggesting that an individual may be moving in a dangerous direction; and, given some training, they may be able to help potential terrorist cases to be addressed much earlier. Second, global information-sharing must increase. The Paris and Brussels attacks showed how jihadists exploited significant seams in European information exchange at both national and international levels.[89] While respect for different national privacy laws, and the protection of intelligence sources and methods, are of crucial importance, there are proven platforms available for increasing multilateral information exchange and trust, including an international counterterrorism hub, case-based task forces, hit–no-hit database search technologies (which allow users to see that data exist but not their nature in order to facilitate follow-up coordination) and centres of excellence. Third, measures and architectures that successfully disrupted Jihadism 1.0 attacks need to be enhanced to disrupt attacks of the latest kind. For example, one major response to Jihadism 1.0 was to increase the security envelope around air travel, and later stadiums, with increased screening measures. Jihadists and other perpetrators of Terrorism 3.0 frequently target those waiting to get inside this envelope, and this vulnerability needs to be addressed through reassessment of some of the architectures originally installed. Fourth, although some 2.0 and 3.0 attackers may not be known to the authorities, metadata can be used to help build intelligence pictures. Many rapidly radicalized terrorists demonstrate abrupt changes in behaviour before their attacks that could have been highlighted by financial tracking, location data and network analysis. Individuals could consent to allowing the authorities access to their broad pattern behaviour data in return for placement on a 'whitelist' that would allow them to access airports and stadiums with less or no screening. Fifth, efforts to counter violent extremism need to incentivize friends and families to report radicalized individuals to create earlier 'off ramps', or exit pathways, for those at risk. Finally, domestic and international law must be updated to help effectively counter 4.0 terrorism, along with increased cyber resilience measures.

Conclusion

In this article we have argued that focusing on the rapid development and spread of ICTs offers a new and fruitful way of understanding the four broad evolutions of global jihadism since the 1990s. Drawing on case evidence from successful jihadist attacks, we have shown how, in each phase, jihadists have exploited the different strategic, organizational, recruiting, financing and tactical opportunities these developments present. In clearly delineating epochs of ICT transformation

[89] Michael Chertoff, Daniela Richterova and Patrick Bury, 'GLOBSEC Intelligence Reform Initiative: reforming transatlantic counter-terrorism' (GLOBSEC Policy Institute, 2016), https://www.globsec.org/wp-content/uploads/2017/09/giri_report_1.pdf.

and linking these to the tactical and organizational advantages global jihadists have gained from these evolutions, we have provided a coherent typology for understanding how ICTs influence jihadists. We have also outlined how counterterrorism responses have adjusted to meet the demands of jihadism as it has evolved over these four epochs. We hope that our typology will help scholars, policymakers and practitioners to conceptualize some of the major effects changes in ICTs have had, and are having, on successful global jihadist activities. More broadly, we have also argued that this typology may be applicable to other forms of terrorism, providing a fruitful avenue for future researchers. Our focus on ICTs highlights the way in which these evolutions are continually refined, and, *contra* Rapoport's waves theory, how they overlap and coexist. The next step in our research will be exploiting quantitative jihadist databases to complement our new typology. In the meantime, as new ICT evolutions such as artificial intelligence, deepfakes (machine learning image and video methods to replace one person's likeness with another), quantum computing and advanced cyber techniques continue to emerge, governments, practitioners and scholars will need foresight and imagination to prepare for the coming manifestations of Global Terrorism 4.0.