Beyond Prevention: The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy

Reed, A.G.; Glazzard, Andrew

DOI
10.1080/03071847.2020.1727165

Publication date
2020

Document Version
Final published version

Published in
The RUSI Journal

Citation (APA)
Reed, A. G., & Glazzard, A. (2020). Beyond Prevention: The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy. *The RUSI Journal*, *165*(1), 74-88. https://doi.org/10.1080/03071847.2020.1727165

The RUSI Journal

Routledge
Taylor & Francis Group

ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: https://www.tandfonline.com/loi/rusi20

Beyond Prevention: The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy

Andrew Glazzard & Alastair Reed

To cite this article: Andrew Glazzard & Alastair Reed (2020) Beyond Prevention: The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy, The RUSI Journal, 165:1, 74-88, DOI: 10.1080/03071847.2020.1727165

To link to this article: https://doi.org/10.1080/03071847.2020.1727165

Research Article
The RUSI Journal

Beyond Prevention

The Role of Strategic Communications Across the Four Pillars of Counterterrorism Strategy

Andrew Glazzard and Alastair Reed

The rise to prominence of Daesh and its expert exploitation of extremist propaganda has brought in to focus the role of strategic communications in counterterrorism (CT) and countering violent extremism policy. Nonetheless, strategic communications tends to be discussed largely in relation to counter-recruitment and counter-radicalisation. Using the UK's CT strategy as a case study, Andrew Glazzard and Alastair Reed argue that strategic communications has a far wider application in CT.

The value of strategic communications to counterterrorism (CT) appears to be widely accepted. In some governments, it is explicitly recognised as a preferred approach: both the US and the UK, for example, have invested in institutions devoted to CT strategic communications. Academics have long recognised that terrorism 'is not simply violence but communication',[1] and research has increasingly focused not only on how terrorists communicate but also on what works in response. Researchers, practitioners – in government, the private sector and NGOs – and policymakers therefore seem to be aligned.

However, there are important and concerning gaps and misconceptions among academics and practitioners. Most fundamentally, what CT and countering violent extremism (CVE) practitioners in government and beyond like to call 'strategic communications' is not, in fact, strategic at all. As a result, strategic communications tends to focus on recruitment propaganda and countering radicalisation at the expense of how it may be used to reduce the threat of terrorism, its impact and our vulnerability to it.

The essence of strategic communications, according to one influential group of researchers working in management studies, is 'communicating purposefully to advance' an organisation's mission, which seems unproblematic. But they go on to say that 'these activities are strategic, not random or unintentional communications – even though unintended consequences of communications can adversely impact the ability of an organization to achieve its strategic goals. Importantly, strategic must not be defined narrowly'.[2] In other words, for communications to be strategic, they must not focus on particular aspects of the mission but should embrace its totality.

Several national and multilateral CT strategies are genuinely strategic, recognising the need for managing risk by addressing vulnerabilities as well as threats, prevention as well as response, and the value of persuasion as well as coercion. The UK's CT strategy, CONTEST, appears to have been the first to be articulated in such a strategic way (but it is by no means the only one).[3] And yet, despite the prevalence of strategic approaches, research and practice in the communications field has not followed a similarly

1. Neville Bolt, *The Violent Image: Insurgent Propaganda and the New Revolutionaries* (London: Hurst, 2012), p. 18.
2. Kirk Hallahan et al., 'Defining Strategic Communication', *International Journal of Strategic Communication* (Vol. 1, No. 1, 2007), pp. 4, 27.
3. HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, Cm 9608 (London: The Stationery Office, 2018). Some national and multilateral counterterrorism (CT) strategies have been modelled on the UK's, such as the EU's (2005) and Nigeria's (2014). For discussions of these strategies, see Rik Coolsaet, 'EU Counterterrorism Strategy: Value

© RUSI Journal Vol. 165, No. 1, January 2020 pp. 74–88

Then Home Secretary Sajid Javid makes a speech at the Southbank Centre in London to launch a strengthened version of the government's CONTEST strategy, June 2018. *Courtesy of PA Images/Stefan Rousseau*

holistic, balanced and therefore strategic framework. In academia, most attention has been paid to communications that prevent radicalisation, and much of this is highly critical of what governments have practised, and while there is evidence that governments do use communications tools in other areas of CT, these have been subjected to much less scrutiny by researchers.[4]

Moreover, CT communications needs to pay attention to all forms of communication used directly and indirectly by terrorists – mainstream and social media, images, music, videos and writing, and actions as well as representation. Nineteenth-century anarchists saw terrorism as 'propaganda of the deed',[5] while in the age of the terrorist 'spectacular' in 1974, Brian Jenkins famously equated terrorism with theatre: terrorists' acts, words and images are all part of their communications.[6] Furthermore, it is not simply a question of recognising that terrorist attacks and terrorist propaganda are different forms of communication; terrorists have many things to say to many different groups of people: 'Mistakenly, terrorist acts are widely assumed, at best, to be a "one message fits all" form of address'.[7] Terrorists communicate using a wide variety of media including video games, poetry, songs, murals, oral narratives and more.[8]

This article seeks to make two important contributions to the field. The first is a reconceptualisation of how the role of 'strategic communications' within CT policy is understood. The article argues that what is largely perceived as 'strategic communications' within policy and

Added or Chimera?', *International Affairs* (Vol. 86, No. 4, 2010), pp. 857–73; Eugene Eji, 'Rethinking Nigeria's Counter-Terrorism Strategy', *International Journal of Intelligence, Security, and Public Affairs* (Vol. 18, No. 3, 2016), pp. 198–220.

4. See, for example, Jack Holland, 'The Language of Counterterrorism', in Richard Jackson (ed.), *Routledge Handbook of Critical Terrorism Studies* (London: Routledge, 2016), pp. 203–13; and Bill Durodie, 'Securitising Education to Prevent Terrorism or Losing Direction?', *British Journal of Educational Studies* (Vol. 64, No. 1, 2016), pp. 21–35. For a rare example of a study examining CT strategy holistically through a communications lens, see Ronald D Crelinsten, 'Analysing Terrorism and Counter-Terrorism: A Communication Model', *Terrorism and Political Violence* (Vol. 14, No. 2, 2002), pp. 77–122.
5. Propaganda of the deed 'is planned dramaturgically with precision, rendering it primarily strategic. For propaganda of the deed to become a fully-fledged act of communication requires viewers. A tank that explodes under insurgent fire is a military tactical strike. But place a camera before it, and it becomes strategic propaganda of the deed'. See Bolt, *The Violent Image*, p. 3.
6. Brian M Jenkins, *International Terrorism: A New Kind of Warfare* (Santa Monica, CA: RAND Corporation, 1974), p. 4.
7. Bolt, *The Violent Image*, p. 258.
8. See, for example, Thomas Hegghammer (ed.), *Jihadi Culture: The Art and Social Practices of Militant Islamists* (Cambridge: Cambridge University Press, 2017).

DOI: 10.1080/03071847.2020.1727165

practice is rarely strategic in its nature; instead, communications tends to be seen as an 'add-on' to CT policy. But strategic communications, in order to actually be strategic, should be at the core of any CT strategy, as a thread that runs through all aspects of it.

Second, in large part because of this misconceptualisation, strategic communications has too often been reduced in the eyes of policymakers to purely 'counternarrative' or 'counter-messaging' campaigns. As we shall argue, strategic communications has largely been confined to the preventive sphere of CT policy – countering terrorist attempts at radicalisation and recruitment. This article argues that strategic communications has applications across the whole of CT policy. Through an analysis of the four pillars of the UK CONTEST strategy, the wider application of strategic communications is demonstrated, highlighting promising avenues of exploration within each CONTEST pillar where strategic communications can deliver added value.

CONTEST: The UK's Counterterrorism Strategy

The aim of CONTEST is 'to reduce the risk to the UK and its citizens and interests overseas from terrorism, so that our people can go about their lives freely and with confidence'.[9] In order to achieve this, the strategy is structured around four pillars:

- Prevent: Safeguard and support vulnerable people to stop them from becoming terrorists or supporting terrorism.
- Pursue: Stop terrorist attacks happening in the UK and threatening UK interests overseas.
- Protect: Strengthen protection against a terrorist attack in the UK or UK interests overseas.
- Prepare: Save lives, reduce harm and aid recovery quickly in the event of a terrorist attack.

CONTEST was most recently updated in June 2018 following a review. Despite widespread agreement over the potential of strategic communications for CT, CONTEST has little to say on the topic. Within the 100-page document, 'strategic communications' is only mentioned twice. The first is in reference to the need to counter terrorist narratives,[10] and the second is an acknowledgement of Daesh's successful strategic communications campaigns online.[11] Beyond this, the role of communications in general is discussed in a limited number of places across the pillars, most prominently within the Prevent pillar, highlighting the need to disrupt the spread of terrorist propaganda online and to develop strong counternarratives.[12] The last three pillars all note the importance of public-awareness campaigns, highlighting the Action Counters Terrorism (ACT) campaign encouraging members of the public to report suspicious behaviour (Pursue);[13] the British Transport Police's 'See it. Say it. Sorted' campaign to raise vigilance on the rail network (Protect);[14] and the 'Run, Hide, Tell' campaign of practical advice for what to do in the event of a terrorist attack (Prepare).[15] The discussion of communications in parts rather than holistically is far from the strategic application of communications. However, as we will show, the value of communications is implicit in much of CONTEST, but it requires close reading and contextual knowledge to appreciate this.

The Prevent Pillar

The Prevent pillar's aim is 'to safeguard and support vulnerable people to stop them from becoming terrorists or supporting terrorism'.[16] Preventing the recruitment and radicalisation of potential terrorists has been the major focus of strategic communications efforts in CT/CVE. Indeed, a glance at the published literature would suggest it has been an almost exclusive focus: strategic communications in CT/CVE is widely assumed to be preventive.[17] This is illustrated by the prevalence of so-called counternarrative or counter-speech in policy prescriptions, CVE handbooks, and

9. HM Government, *CONTEST*, p. 7.
10. *Ibid.*, p. 71.
11. *Ibid.*, p. 74.
12. *Ibid.*, p. 71.
13. *Ibid.*, p. 46.
14. *Ibid.*, p. 58.
15. *Ibid.*, p. 68.
16. *Ibid.*, p. 31.
17. See, for example, Haroro J Ingram, 'Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility and Behavioural Change', *ICCT Research Paper* (No. 9, September 2016).

government and non-government interventions. Although counternarrative and counter-speech can be distinguished from strategic communications – the former seeks to delegitimise terrorist propaganda and/or offer a more positive alternative, sometimes (but not always) in narrative form, while the latter is usually seen as an organisation's use of the full range of communications channels to achieve a strategic objective[18] – the terms are sometimes used interchangeably and both counternarrative and counter-speech, when practised by governments, may be seen as a component of CT/CVE strategic communications.

The definitional scope of these terms is important. The potential of strategic communications to prevent radicalisation and recruitment cannot be understood without attending to the range of activities implied by these two terms. The published literature on CT/CVE communications, at least in the West, focuses overwhelmingly on the use of interventions to challenge terrorist ideology and propaganda by '[e]ngaging in the battle of ideas – challenging the ideologies that extremists believe can justify the use of violence, primarily by helping Muslims who wish to dispute these ideas to do so'.[19] This emphasis is largely a response to the popular and political anxiety in Western countries at the capacity of jihadist groups, in particular, to recruit and radicalise through online propaganda despite a wealth of research which shows that the internet may be an enabler of radicalisation and recruitment, but is rarely the principal cause of behavioural change.[20] For this reason, academic research tends to be sceptical about the efficacy of counternarrative or counter-speech, both on the grounds of its theoretical underpinning and on what is known about its actual effect.[21] Communications theory suggests that violent words do not necessarily lead to violent deeds, that people are not so susceptible that they can be 'inoculated' by consuming communications products, and that a message or a narrative can simply be countered by another.[22] In the field of CVE, counternarrative interventions, meanwhile, are notoriously lacking in independent evaluation, with authors often proudly citing 'vanity metrics' such as numbers of views on YouTube or 'likes' on Facebook.[23]

The most infamous example of an unsuccessful counter-speech campaign is the US State Department's 'Think Again, Turn Away' social media campaign in 2013–14, which was widely criticised for drawing attention to the terrorists' material while making the US government appear leaden and amateurish by comparison.[24] In one example, the State Department replied to a leader of the Al-Nusra Front in Syria with a taunt about Islamic State's ethics, apparently unaware that the Al-Nusra Front was engaged in a violent feud with Islamic State.[25] There are other counter-speech interventions, such as Saudi Arabia's Sakinah initiative, in which religious scholars working for the Ministry of Islamic Affairs engaged potentially vulnerable individuals on the internet to undermine extremist ideology and promote

18. Foreign and Commonwealth Office, 'Memorandum of Understanding on Project Funding', 2016, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/696952/Memorandum_of_Understanding_on_Project_Funding.pdf>, accessed 14 November 2019; Henry Tuck and Tanya Silverman, 'The Counter Narrative Countering Violent Extremism Handbook', Institute for Strategic Dialogue, <https://www.isdglobal.org/wp-content/uploads/2016/06/Counter-narrative-Handbook_1.pdf>, accessed 18 December 2019. Content removal and other methods to restrict access to terrorist content is not considered to be within the scope of this article.
19. HM Government, *Countering International Terrorism: The United Kingdom's Strategy*, Cm 6888 (London: The Stationery Office, 2006), p. 2.
20. Alexander Meleagrou-Hitchens and Nick Kaderbhai, *Research Perspectives on Online Radicalisation: A Literature Review 2006–2016* (Dublin: VOX-Pol Network of Excellence, 2017); Ghaffar Hussain and Erin Marie Saltman, *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter It* (London: Quilliam Foundation, 2014), pp. 13–17.
21. Kate Ferguson, 'Countering Violent Extremism Through Media and Communication Strategies: A Review of the Evidence', Partnership for Conflict, Crime and Security Research, 1 March 2016.
22. Cristina Archetti, *Understanding Terrorism in the Age of Global Media: A Communication Approach* (Basingstoke: Palgrave Macmillan, 2013), p. 179.
23. Louis Reynolds and Henry Tuck, *The Counter-Narrative Monitoring and Evaluation Handbook* (London: Institute for Strategic Dialogue, 2016), p. 24.
24. Clive Walker and Maura Conway, 'Online Terrorism and Online Laws', *Dynamics of Asymmetric Conflict* (Vol. 8, No. 2, 2015), p. 169.
25. Rita Katz, 'The State Department's Twitter War with ISIS is Embarrassing', *Time Magazine*, 16 September 2014.

'moderate' interpretations of Islam.[26] And there is such a wealth of counternarrative material that Hedayah, the Abu Dhabi-based international centre of excellence for CVE, has developed an online library devoted to it.[27] What is lacking is compelling evidence of positive effect of what has so far been attempted.

> For a communications campaign to be truly strategic, it needs to be integrated with wider government communication and action

Even within the Prevent pillar, strategic communications in CT/CVE means more than counternarrative or counter-speech. What distinguishes strategic communication from any other type of communication is its strategic aim, and the Prevent pillar's aim is to reduce recruitment and radicalisation. But strategic communications are not limited by form (such as narrative or message), audience (terrorists, vulnerable individuals, the public), or medium (social media, television broadcast, parliamentary statement). A broader view, therefore, of strategic communications in Prevent might include campaigns that go beyond social media, that seek to influence a much broader range of audiences, and which are not focused on undermining or replacing terrorist ideological material. What, then, might such communications include?

For a start, given that terrorist radicalisation and recruitment is a highly variable but usually complex and multi-factorial process of socialisation, strategic communications interventions could attend to what James Khalil and Martine Zeuthen call 'structural factors' of radicalisation and recruitment (otherwise known as 'push factors', such as political and economic grievances), as well as 'enabling factors' (for example, channels of communication via social media) and 'individual incentives' (things which attract individuals to a violent group or cause, such as the appeal of charismatic ideologues or financial incentives).[28] Adding further categories to the recruitment/radicalisation model, strategic communications might also attend to group dynamics (for example, socialisation processes) and, on the countervailing side of the process, to protective factors (sources of individual or community resilience, such as supportive social environments).

To illustrate, governments could look to mitigate the effect of economic and political grievances and other structural factors, seek to undermine the charismatic (as opposed to ideological) appeal of terrorist recruiters, undermine terrorist group cohesion, and promote protective factors (including what is sometimes called 'individual resilience'), for example by promoting sources of advice and support within communities. Preventive strategic communications could also address audiences beyond those judged vulnerable to radicalisation, such as opinion-formers and wielders of cultural influence, to reduce social and community tensions. And strategic communications campaigns need not restrict themselves to social media.

Furthermore, for a communications campaign to be truly strategic, it needs to be integrated with wider government communication and action, and there is evidence that a lack of organisational coherence is one rapid route to ineffectiveness.[29] Even a positive, well-managed communications intervention may be undermined or even become counterproductive if it is not congruent with other messages.[30] And perhaps most importantly, given the evidence that direct challenges are at best ineffective at achieving positive behaviour change and may even be counterproductive, prevention of terrorism should not be focused on ideological confrontation.[31]

One important strand of recent terrorism research approaches the problem within the framework of public health interventions, dividing responses into: treatment of offenders; active

26. Christopher Boucek, 'The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia', *CTC Sentinel* (Vol. 1, No. 9, 2008), pp. 1–3.
27. Hedayah, 'Counter Narratives Library'.
28. James Khalil and Martine Zeuthen, 'Countering Violent Extremism and Risk Reduction: A Guide to Programme Design and Evaluation', *RUSI Whitehall Report*, 2-16 (June 2016), p. 9.
29. Haroro J Ingram, 'A Brief History of Propaganda During Conflict: Lessons for Counter-Terrorism Strategic Communications', *ICCT Research Paper* (June 2016).
30. Paul Cornish, Julian Lindley-French and Claire Yorke, *Strategic Communications and National Strategy* (London: Chatham House, 2011), p. 14.
31. Ferguson, 'Countering Violent Extremism Through Media and Communication Strategies, p. 15.

interventions targeted at 'vulnerable' or 'at-risk' populations; and public campaigns designed to sensitise the general population to the risks and to 'reduce the incidence of risky behaviours or to promote social causes important to the betterment of the community'.[32] Public health interventions in the latter category are primarily communicative, and evidence for their effectiveness can be found in campaigns to reduce smoking or cut down on sugar and fat.[33] And yet the application of this type of model to terrorism has focused particularly on the second category (generally equated to preventing and countering violent extremism, or P/CVE), and there is a striking lack of insights from public health communications in the academic literature on terrorism.

Despite the restricted focus on counternarrative and counter-speech in the literature, there are signs that some governments have in fact taken a broader view. Most notably, the UK's Home Office created the Research Information Communications Unit (RICU) in 2007, with a broad mandate to improve government communications about terrorism.[34] After the election of the coalition government in 2010, RICU refocused its attention on counter-radicalisation, drawing criticism from academics in the 'critical terrorism studies' tradition (which critically evaluates the theory and practice of CT rather than focusing on terrorism) for allegedly propagandising deceptively, creating suspect communities and inappropriately importing the techniques of counterinsurgency (COIN) practised abroad in the War on Terror to the domestic sphere.[35]

In the Middle East, the increase in terrorist attacks following the 2003 invasion and occupation of Iraq led to a range of communications interventions, some apparently supported by the US government,[36] that included the use of public service advertisements to strengthen ties between Iraq's ethnic and confessional groups – especially between Sunnis and Shias, at exactly the time that Al-Qa'ida was seeking to foment inter-community violence in Iraq. The evidence suggests this campaign was not successful, possibly due to poor design and a failure by its authors to understand the complex socio-political context of Iraq, but it illustrates the point that communication in the Prevent pillar need not be restricted to challenging terrorist propaganda.[37]

The Pursue Pillar

The Pursue pillar – to stop terrorist attacks happening in the UK and against UK interests overseas[38] – encompasses the tools and approaches of more hard-edged CT – essentially the use of the criminal justice system, intelligence agencies and the military to capture (or kill) terrorists, bring them to justice, and to disrupt terrorist operations and networks through pre-emptive intelligence and law enforcement.[39]

At first glance, this may not seem to be promising territory for communications interventions, strategic or otherwise, which are concerned with influencing and persuading. However, this overlooks the fact that strategic communications approaches have been widely applied in conflicts by military forces – going back at least as far as the Malayan Emergency (1948–60), during which General Sir Gerald Templer, who led the British counterinsurgency response as High Commissioner in Malaya from 1952 to 1954, said: 'The answer lies not in pouring more troops into the jungle, but in the hearts and minds of the people'.[40]

CT is not the same thing as COIN, but they have enough in common for similar strategic

32. Hallahan et al., 'Defining Strategic Communication', pp. 5–6.
33. Magdalena Cismaru and Anne M Lavack, 'Social Marketing Campaigns Aimed at Preventing and Controlling Obesity: A Review and Recommendations', *International Review on Public and Non Profit Marketing* (Vol. 4, No. 1–2, 2007), pp. 9–30.
34. Rachel Briggs, 'Community Engagement for Counterterrorism: Lessons from the United Kingdom', *International Affairs* (Vol. 86, No. 4, July 2010), pp. 979–80.
35. Rizwaan Sabir, 'Blurred Lines and False Dichotomies: Integrating Counterinsurgency into the UK's Domestic "War on Terror"', *Critical Social Policy* (Vol. 37, No. 2, 2017), pp. 202–24.
36. Ahmed K Al-Rawi, 'The Anti-Terrorist Advertising Campaigns in the Middle East', *Journal of International Communication* (Vol. 19, No. 2, 2013), pp. 182–95.
37. *Ibid*.
38. HM Government, *CONTEST*, p. 43.
39. Basia Spalek and Doug Weeks, 'Counterterrorism Measures', in Bryan S Turner (ed.), *The Wiley Blackwell Encyclopedia of Social Theory* (Wiley, 2017), p. 111.
40. This sentiment was later converted by an anonymous US officer during the Vietnam War into the more famous aside, 'Grab 'em by the balls and their hearts and minds will follow', both quoted in Paul Dixon, '"Hearts and Minds"? British Counter-Insurgency from Malaya to Iraq', *Journal of Strategic Studies* (Vol. 32, No. 3, 2009), p. 354.

communications approaches to be applied to both. Indeed, terrorists themselves recognise the similarities between (counter)terrorism and (counter)insurgency and the centrality of strategic communications to both: most famously, Al-Qa'ida leader's Ayman Al-Zawahiri echoed Templer in his advice in 2005 to Abu Musab Al-Zarqawi, then commander of Al-Qa'ida in Iraq, to remember that 'we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the *hearts and minds* of our *Umma* [the Muslim nation]'.[41]

> Communications interventions to demoralise or dissuade terrorists may conceivably work by suggesting that violence is counterproductive

Both CT and COIN are concerned with reducing the will of violent actors to fight, so that individuals desist or disengage, and leaders contemplate ceasefires or accept amnesties. In both cases, communications interventions can potentially undermine morale by seeking to persuade violent actors that their cause is better pursued politically, peacefully or not at all. Studies of terrorist disengagement at both the organisational and the individual level suggest that communications interventions changed perceptions of the value of armed action and that these changes were critical to these groups' and individuals' decisions.[42]

Communications interventions to demoralise or dissuade terrorists may conceivably work by suggesting that violence is counterproductive (by highlighting failures, unintended consequences or unintended victims, such as those from the same identity group as the terrorist), ineffective (for example, by reducing what former British Prime Minister Margaret Thatcher famously called 'the [terrorists'] oxygen of publicity',[43] by suppressing their public communication or reducing the prominence of terrorism in news reporting), or futile (by maintaining strong and consistent messages that terrorist attacks will not achieve their desired objectives). As these examples suggest, the means to achieve these communication ends may vary, from public diplomacy to active censorship. That is not to say that all are necessarily successful or ethical – the British government's widely derided attempt to effectively censor Sinn Féin as a means of combating the Provisional IRA in the 1990s is a case in point[44] – but they do at least illustrate the range of possible communications interventions in the Pursue pillar.

CT and COIN are also concerned with the support bases for belligerents, and here again a strategic communications approach has the potential to shape the terrorists' operating environment. Indeed, one famous description of insurgency differentiates it from conventional warfare by emphasising its integration within communities – 'the guerrilla must swim in the people as the fish swims in the sea'.[45] Not all terrorist movements in history have benefited from community support, but some of the most long-lasting have, and at times even campaigns of suicide attacks have generated strong support from communities, as measured by opinion polls.[46] It stands to reason that a terrorist operating in a

41. Federation of American Scientists , 'Letter from Al-Zawahiri to Al-Zarqawi', 2005, p. 10, <https://fas.org/irp/news/2005/10/letter_in_english.pdf>, accessed 4 December 2019. Emphasis added.
42. Mary Beth Altier et al., 'Why They Leave: An Analysis of Terrorist Disengagement Events from Eighty-Seven Autobiographical Accounts', *Security Studies* (Vol. 26, No. 2, 2017), pp. 305–32; Tore Bjørgo and John Horgan (eds), *Leaving Terrorism Behind: Individual and Collective Disengagement* (Abingdon: Routledge, 2008).
43. Margaret Thatcher Foundation, 'Margaret Thatcher Speech to American Bar Association', 15 July 1985, <https://www.margaretthatcher.org/document/106096>, accessed 14 November 2019.
44. Gary Edgerton, 'Quelling the "Oxygen of Publicity": British Broadcasting and "The Troubles" During the Thatcher Years', *Journal of Popular Culture* (Vol. 30, No. 1, 1996), pp. 115–32.
45. This aphorism was attributed to Mao Zedong, but his more considered observation was: 'Many people think it impossible for guerrillas to exist for long in the enemy's rear. Such a belief reveals lack of comprehension of the relationship that should exist between the people and the troops. The former may be likened to water; the latter to the fish who inhabit it'. Mao Zedong, *On Guerrilla Warfare*, translated by Samuel B Griffith (Eastford, CT: Martino Fine Books, 2017, first published 1937), Chap. 6.
46. Mia M Bloom, 'Palestinian Suicide Bombing: Public Support, Market Share, and Outbidding', *Political Science Quarterly* (Vol. 119, No. 1, 2004), pp. 61–88; Bart Schuurman, 'Defeated by Popular Demand: Public Support and Counterterrorism in Three Western Democracies, 1963–1998', *Studies in Conflict and Terrorism* (Vol. 36, No. 2, 2013), pp. 152–75; Daniel Byman, 'Passive Sponsors of Terrorism', *Survival* (Vol. 47, No. 4, 2005), pp. 117–44.

supportive environment will benefit from practical and operational support of various kinds, such as funding, passive surveillance (what the Provisional IRA referred to as 'dicking'), and the supply of facilities such as safe houses and vehicles.

The potential for communications interventions in Pursue is not, though, limited to sapping community support for terrorist causes, important though that may be operationally. In the West, at least, there is a long history of counterterrorist authorities promoting public awareness of terrorist threats and urging the public not only to be vigilant and protect itself and others, but also to report any suspicions to the authorities and thereby provide operational leads for interdicting terrorist attacks. Public communications campaigns of this type have included New York's '16 million eyes' campaign in 2007, which carried the words: 'There are 16 million eyes in the city. We're counting on all of them. If you see something, say something', and Scotland Yard's 'Life Savers' 2004 campaign, which stated: 'Terrorists need places to live and to make plans ... they need vehicles and people to help them. If you have any suspicions about terrorist activity ... do not hesitate ... call [the] confidential anti-terrorist hotline'.[47] The encouragement of what some critics call 'citizen-detectives' is not without controversy, but these are clear examples of CT in the communication sphere which is designed to create operational opportunities. Such campaigns, wittingly or not, may work to counter the bystander effect – the reluctance of individuals to intervene in emergency situations, a phenomenon which is well known to psychologists.[48]

Pursue pillar objectives may also be served by communications interventions that enhance perceptions of counterterrorist authorities in terms of legitimacy and competence. Many, if not most, law enforcement organisations benefit from public relations departments, and while there is little attention paid to this aspect of communications in the academic literature, it is clearly the case that terrorists themselves recognise the importance of delegitimising their opponents. The Syrian theorist of jihad, Abu Mus'ab Al-Suri, for instance, wrote:

> The enemy regime will not sit idle while we wage our political and military campaigns, they will initiate their own propaganda blitz and psychological warfare trying to portray us as a bunch of thugs, criminals and terrorists with no connection to the nation, and they will flood the media with rumors. The reputation of the regime should work in our favor, we should affix the label of 'lies and liars' to them.[49]

As Richard English has pointed out, maintaining credibility in government and law enforcement through CT communications is critical not only to winning 'hearts and minds' but also to achieving operational objectives.[50]

The Protect Pillar

CONTEST's Protect pillar aims to 'strengthen protection against a terrorist attack in the UK or UK interests overseas'.[51] Four objectives serve this aim: to detect suspected terrorists and harmful material at the border; to reduce the risk and improve the resilience of transport and critical national infrastructure (CNI); to reduce the vulnerability of crowded places; and to prevent access to materials and information that could be used to conduct attacks.[52]

Whilst at first glance there may appear little space for communications in a pillar that is largely about physical security of infrastructure, this article argues that strategic communications can in fact deliver added value to the Protect pillar, where strategic communications is relatively undeveloped. These opportunities are not without challenges: in particular, how vigilance campaigns can be designed that do not play into terrorist hands by increasing public fear or overwhelming authorities with false reports.

As the terrorist threat becomes more complex, especially with the increases in 'lone actor' or 'inspired attacks', the role of the public has become increasingly important. As David Parker and colleagues argue, 'public coproduction of security is increasingly necessary, by which we mean the active engagement of private citizens and key non-security stakeholders (e.g., teachers) in aiding authorities in detecting, assessing, and reporting risks of violent

47. Nick Vaughan-Williams, 'Borderwork Beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror', *Space and Polity* (Vol. 12, No. 1, 2008), pp. 63–79.
48. For the bystander effect and CT, see Kumar Ramakrishna, 'The Threat of Terrorism and Extremism: "A Matter of 'When', and Not 'If'"', *Southeast Asian Affairs* (2017), pp. 335–50.
49. Abu Mus'ab Al-Suri, 'Lessons Learned from the Armed Jihad Ordeal in Syria', quoted in Donald Holbrook, 'Approaching Terrorist Public Relations Initiatives', *Public Relations Inquiry* (Vol. 3, No. 2, 2014), p. 154.
50. Richard English, *Terrorism: How to Respond* (New York, NY: Oxford University Press, 2009).
51. HM Government, *CONTEST*, p. 53.
52. *Ibid.*, p. 53.

extremism'.[53] Some public goods, such as security and safety, cannot simply be produced by the state and consumed by the public, rather they need to be co-produced. This is a concept that has informed many areas of public policy, such as policing and crime prevention, with policies such as Neighbourhood Watch schemes. Because the co-production of security is essentially voluntary, it requires encouragement or incentives to overcome inertia as well as the availability of information to help the public play its role – and this is where strategic communications has a vital role.[54]

In the Protect pillar, this has most commonly manifested itself in public vigilance campaigns around public transport. Given the scale and dispersed nature of transport infrastructures, it is impossible to ensure the necessary numbers of police and security staff to observe all locations at all times, so the participation of passengers reporting suspicious behaviour or unattended items becomes invaluable. Vigilance campaigns are aimed at raising awareness of the threat and increasing the likelihood of members of the public reporting information, such as the current British Transport Police's 'See it. Say it. Sorted' campaign,[55] and the US Department of Homeland Security (DHS) campaign 'If you see something, say something'.[56]

In the UK, vigilance campaigns have a long history, encouraging members of the public to look out for and report unattended baggage, in large part due to the Provisional IRA bombing campaigns from the 1970s to 1990s against, for example, the UK rail infrastructure.[57] However, this has not been the case in other countries, such as Denmark and Spain, which have avoided such campaigns, fearing the unintended consequences of scaring the public or receiving an overwhelming number of reports.[58]

As Alex Braithwaite argues, the central objective of terrorism is to provoke a sense of fear in the public, because this is how terrorists believe they can deliver political change. However, 'if terrorists do indeed desire and require the cultivation and proliferation of public fear, then it would appear that such schemes [vigilance campaigns] run the potential of becoming counterproductive'.[59] A call for vigilance against the terrorist threat, it is argued, will inevitably raise the threat perception and level of fear in the public. However, these outcomes should not be interpreted as coterminous (in other words, that increasing public fear is the price to pay for increasing public vigilance). Rather, the question should be how can communication campaigns be designed to increase vigilance while reassuring the public and reducing the levels of public fear?

Although most public vigilance campaigns are designed around signs of an imminent attack, such as suspicious behaviour or unattended items, there is also scope for campaigns that focus their attention further upstream in the attack planning cycle. For instance, there is usually a long prior phase in which the actors gain access to the knowledge and precursor materials needed to build an explosive device. Some countries, including the US and the Netherlands,[60] have specific vigilance campaigns to raise awareness of what actions to look out for to prevent malignant actors from acquiring precursor materials to manufacture explosives. As the US DHS Bomb-Making Materials Awareness Program (BMAP) notes:

> Powerful explosives can be made from common consumer goods, like pool sanitizers, fertilizers, and

53. David Parker et al., 'Challenges for Effective Counterterrorism Communication: Practitioner Insights and Policy Implications for Preventing Radicalization, Disrupting Attack Planning, and Mitigating Terrorist Attacks', *Studies in Conflict and Terrorism* (Vol. 42, No. 3, 2019), p. 264.
54. *Ibid.*, p. 264.
55. British Transport Police, 'New National Rail Security Campaign Starts Today: "See It. Say It. Sorted"', 1 November 2016, <https://www.btp.police.uk/latest_news/see_it_say_it_sorted_new_natio.aspx>, accessed 16 December 2019.
56. Homeland Security, 'If You See Something, Say Something', <https://www.dhs.gov/see-something-say-something>, accessed 16 December 2019.
57. Julia M Pearce et al., 'Encouraging Public Reporting of Suspicious Behaviour on Rail Networks', *Policing and Society*, April 2019, DOI: 10.1080/10439463.2019.1607340.
58. *Ibid.*; Parker et al., 'Challenges for Effective Counterterrorism Communication'; Anastasia Loukaitou-Sideris, Brian D Taylor and Camille N Y Fink, 'Rail Transit Security in an International Context: Lessons from Four Cities', *Urban Affairs Review* (Vol. 41, No. 6, 2006), pp. 727–48.
59. Alex Braithwaite, 'The Logic of Public Fear in Terrorism and Counter-Terrorism', *Journal of Police and Criminal Psychology* (Vol. 28, No. 2, 2013), pp. 95–101.
60. Nationaal Coördinator Terrorismebestrijding en Veiligheid [National Coordinator for Counterterrorism and Safety], <https://www.nctv.nl/onderwerpen/aanpak-aanslagmiddelen/campagne-aanslagmiddelen>, accessed 16 December 2019; Homeland Security, 'Bomb-Making Materials Awareness Program (BMAP)', <https://www.dhs.gov/bmap>, accessed 16 December 2019.

> paint removers, that are bought and sold every day in communities across the United States. With the increase in the use of these common items to make homemade explosives (HME) and improvised explosive devices (IED), an educated and proactive public is the key to prevention.[61]

These campaigns have a narrower focus than public information campaigns on, for example, transport systems, targeting a small audience such as companies and employees in the supply chain of precursor materials, highlighting specific actions (such as purchasing for certain chemicals in large quantities).[62]

Such specialised campaigns offer certain advantages over general campaigns. First, rather than addressing a general audience with broad instructions, such as 'be vigilant for suspicious activity', these campaigns are able to target a specific audience with specific instructions, potentially reducing the number of false reports. Second, targeting a smaller audience reduces the likelihood of increasing public levels of fear of the terrorist threat. This raises the question of what other 'niche' vigilance campaigns might be viable options. Reflecting on other CONTEST pillar priorities for protecting CNI (beyond transport) and reducing the vulnerability of crowded places, other more targeted vigilance campaigns aimed at key actors, such as retail workers or bar staff working in high-profile public spaces, may prove to be effective applications of strategic communications.

A further role for communications within the Protect pillar is in deterrence. While much emphasis is placed on physical security to protect CNI, communicating these measures to potential hostile perpetrators can produce a deterrent effect. The objective of deterrence in this context is to be able to influence the potential perpetrator's analysis and assessment in planning hostile action, and to make it less attractive to carry out that action.[63] Although in strategic theory deterrence is often about the cost–benefit analysis of retaliation, within Protect it is about influencing the perpetrators' assessment of whether an attack would be successful. As the Centre for the Protection of National Infrastructure explains: 'If a hostile believes a site has excellent security measures due to what they've read online, seen on a poster or witnessed through their physical reconnaissance, it may be enough to deter them from their target altogether. This process has the added benefit of reassuring staff and visitors; they will feel that they are in a safer environment'.[64] The success of any deterrence strategy rests on being able to effectively communicate the desired message to potential perpetrators.

A further role for communications within the Protect pillar is in deterrence

This is common practice in security and crime prevention: buildings with CCTV often advertise the fact with warning signs to provide a deterrence effect.[65] Similarly, Neighbourhood Watch groups often advertise their presence to potential criminal perpetrators. However, using strategic communication techniques to provide deterrence has been largely overlooked within CT strategy. In CONTEST, deterrence is seen largely through the lens of the Pursue pillar, through the investigation, disruption and prosecution of terrorist activities. However, for many ideologically motivated terrorists, prosecution is not an effective deterrence, while deterrence by communicating the unlikelihood of success may prove more effective. Further, a deterrence strategy is a proactive approach that seeks to shape the behaviour of potential attackers, which can provide a less resource-intensive addition to the CT toolkit, compared with conventional Protect pillar strategies.

Such a deterrence strategy has two potential pitfalls. The first is that rather than deterring potential perpetrators, too much information is communicated, allowing them to take steps to circumvent the protective features in place. The second is displacement: that the deterrence effect is successful and leads to the unintended

61. Homeland Security, 'Bomb-Making Materials Awareness Program (BMAP)'.
62. Nationaal Coördinator Terrorismebestrijding en Veiligheid [National Coordinator for Counter terrorism and Safety], <https://www.nctv.nl/onderwerpen/aanpak-aanslagmiddelen/campagne-aanslagmiddelen>, accessed 16 December 2019.
63. Frans-Paul van der Putten, Minke Meijnders and Jan Rood, 'Deterrence as a Security Concept Against Non-Traditional Threats', In-Depth Study, Clingendael Monitor, 2015, <https://www.clingendael.org/sites/default/files/pdfs/deterrence_as_a_security_concept_against_non_traditional_threats.pdf>, accessed 16 December 2019.
64. Chartered Institute of Public Relations and Centre for the Protection of National Infrastructure, 'Crisis Management for Terrorist Related Events', <https://www.cpni.gov.uk/system/files/documents/de/eb/Crisis_Management_for_Terrorist_Related_Events.pdf>, accessed 17 December 2019.
65. This can also be to comply with data-protection rules.

consequence of terrorist actors changing targets and identifying less protected and more vulnerable targets. However, while displacement does exist, research has shown that in practice the displacement to more vulnerable targets is relatively rare.[66]

> In the post-incident space, terrorist groups normally aim to shape the narrative through their communications strategy to maximise the attack's impact

Strategic communications has an important role to play within the Protect pillar. Beyond the role of traditional vigilance campaigns, there is scope for more targeted campaigns and the application of strategic communications designed to have a deterrence effect.

The Prepare Pillar

CONTEST describes the role of the Prepare pillar as to 'save lives, reduce harm and aid recovery quickly in the event of a terrorist attack'.[67] How can strategic communications add to the delivery of these aims?

As terrorism is not simply violence but also the communication of violence (or threat of violence) to a target audience, the immediate victims are not the ultimate recipient of the communication. Instead, violence is used to communicate a message to a wider audience, to 'terrorise' enemies or to motivate and encourage potential supporters. Traditionally, CT/CVE strategic communications has focused on 'upstream' challenges, such as preventing radicalisation and recruitment. Once a terrorist attack has taken place, it is clearly too late to ensure any preventive action. However, as the attack itself is only a means to an end, it is possible to interrupt or influence the communication of this event and its impact on intended audiences, and the Prepare pillar suggests a need to develop a 'downstream' communication strategy to counter the impact and harm caused by terrorist incidents. Ultimately, since it is impossible to prevent every attack, it is only prudent to be prepared to mitigate the impact of a terrorist attack in its aftermath.[68]

Alastair Reed and Haroro J Ingram have argued for the importance of viewing terrorist incidents through the lens of 'meaning formation' (or 'public sense-making').[69] It is in the space following a terrorist incident that individuals interpret and give meaning to what they have just experienced, a process that tends to peak as the initial shock response to the attack subsides.[70] How these events are perceived and interpreted by the public, and the meaning subsequently assigned to them, will in part determine the social harm and impact of the event.[71] For example, if an attack is aimed at terrorising a given audience, the success of this objective will depend on how this audience processes the event and the meaning they assign to it. This process is not passive and is influenced by the context and communications received by the audience. Hence, in the post-incident space, terrorist groups normally aim to shape the narrative through their communications strategy to maximise the attack's impact. However, this also opens up the opportunity for communications interventions to counter the terrorists' meaning generation and thereby minimise the impact on the audience.

However, in the post-incident space it is not just terrorists who aim to shape and manipulate the narrative, and there is unlikely to be a

66. Ronald V Clarke and Graeme R Newman, 'Police and the Prevention of Terrorism', *Policing: A Journal of Policy and Practice* (Vol. 1, No. 1, 2007), pp. 9–20.
67. HM Government, *CONTEST*, p. 63.
68. Martin Innes et al., 'From Minutes to Months: A Rapid Evidence Assessment of the Impact of Media and Social Media During and After Terror Events', research report prepared for the Five Country Ministerial Countering Violent Extremism Working Group, Crime and Security Research Institute, July 2018, <https://static1.squarespace.com/static/57875c16197aea2902e3820e/t/5bc74f950d929708f7733b3c/1539788716177/M2M+Report+%5BFinal%5D.pdf>, accessed 16 September 2019.
69. Alastair Reed and Haroro J Ingram, 'Towards a Framework for Post-Terrorist Incident Communications Strategies', Global Research Network on Terrorism and Technology Paper No. 12, RUSI and ICCT, 2019, pp. 4–5.
70. See, for example, Brenda Dervin and Charles M Naumer, 'Sense-Making', in Stephen W Littlejohn and Karen A Foss (eds), *Encyclopedia of Communication Theory*, Vol. 2 (Thousand Oaks, CA: Sage, 2009), pp. 877–81.
71. Martin Innes, Diyana Dobreva and Helen Innes, 'Disinformation and Digital Influencing After Terrorism: Spoofing, Truthing and Social Proofing', *Contemporary Social Science*, 25 January 2019, DOI: 10.1080/21582041.2019.1569714; Matthew L Williams and Pete Burnap, 'Cyberhate on Social Media in the Aftermath of Woolwich: A Case Study in Computational Criminology and Big Data', *British Journal of Criminology* (Vol. 56, No. 2, 2016), pp. 211–38.

straightforward contest between the terrorists and the security authorities in public sense-making. The aftermath of any attack may see multiple actors seeking to exploit the communications space, demonstrating the importance of developing and implementing post-incident communication campaigns.

In the period during or following a terrorist incident, the first actors seeking to 'frame'[72] the event and shape the emerging narrative are usually the terrorists themselves. In the age of the terrorist 'spectacular', when terrorists sought to capture attention through exposure via mass media (particularly television), target selection and operational planning would have been focused on visual or dramatic impact. The 9/11 attacks in New York and Washington were major examples of terrorist spectaculars, but they came from a long line of highly dramatic and carefully staged attacks going back to attacks on aircraft in the early 1970s and on iconic buildings in the 1980s and 1990s. For example, the Black September Munich Olympics attack (1972),[73] the bombing of the US Marine barracks in Beirut (1983), the downing of Pan Am Flight 103 over Lockerbie, Scotland (1988), or the dual bombings of the US embassies in Kenya and Tanzania (1998).[74] However, with the emergence of social media and smartphones, members of the public are able to capture the events or the immediate aftermath, with video footage from mobile phones quickly spreading online or being amplified by broadcast on traditional media.[75] One of the first such 'viral' attacks was the brutal murder of British soldier Lee Rigby in Woolwich in 2013. His attackers did not flee the scene but sought out passers-by to film their justification of the attack (whilst still holding the murder weapons with their hands covered in blood).[76]

Terrorists can also direct the social media communication of attacks. The Somalia-based militant group Al-Shabaab, for instance, 'live tweeted' their marauding attack in Nairobi's Westgate shopping mall in 2013.[77] Al-Shabaab's version overwhelmed the government's attempts to control meaning formation and enabled it to dominate the public sense-making.[78] The events of the Christchurch mosque attack in New Zealand in March 2019, livestreamed using Facebook Live, took terrorist self-coverage to new heights and a wider audience. The perpetrator's extensive preparations ensured that the video of the attack and his justifying manifesto would go viral.[79] Social media platforms struggled in the immediate aftermath to prevent the posting of the video – Facebook alone reported it being uploaded 1.5 million times to its platform in the 24 hours after the attack.[80] The sheer volume of the uploads brings home not only the scale of the challenge

72. 'Framing' is a concept in communication theory that 'refers to how the media packages and presents information to the public. According to the theory, the media highlights certain events and then places them within a particular context to encourage or discourage certain interpretations. In this way, the media exercises a selective influence over how people view reality'. See Communication Studies, 'Framing Theory', <https://www.communicationstudies.com/communication-theories/framing-theory>, accessed 16 December 2019.
73. Andrew Silke and Anastasia Filippidou, 'What Drives Terrorist Innovation? Lessons from Black September and Munich 1972', *Security Journal*, 22 May 2019, DOI: 10.1057/s41284-019-00181-x.
74. Daniel Arce and Todd Sandler, 'Terrorist Spectaculars: Backlash Attacks and the Focus of Intelligence', *Journal of Conflict Resolution* (Vol. 54, No. 2, 2009), pp. 354–73.
75. Jason Burke has written extensively on the communication strategies of jihadists in the age of social media and smartphones. See, for example, Jason Burke, 'The Age of Selfie Jihad: How Evolving Media Technology is Changing Terrorism', *CTC Sentinel* (Vol. 9, No. 11, 2016), pp. 16–22.
76. *The Telegraph*, 'Woolwich Attack: The Terrorist's Rant', 23 May 2013; *The Telegraph*, 'Woolwich Attacker Told Me He "Wanted to Start a War", Says Woman Who Confronted Knifeman', 22 May 2013; *BBC News*, 'Lee Rigby Jury Shown Adebolajo "Eye For Eye" Video', 3 December 2013.
77. David Mair, '#Westgate: A Case Study: How Al-Shabaab Used Twitter During an Ongoing Attack', *Studies in Conflict and Terrorism* (Vol. 40, No. 1, 2017), pp. 24–43.
78. Maura Conway and Joseph Dillon, 'Case Study: Future Trends – Live-Streaming Terrorist Attack?', Vox-Pol, 2016, <http://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf>, accessed 19 December 2019; Mair, '#Westgate: A Case Study'; Innes et al., 'From Minutes to Months', p. 37.
79. Elizabeth Lopatto, 'The Mass Shooting in New Zealand was Designed to Spread on Social Media', *The Verge*, 15 March 2019. Although, it should be noted, it was not the first live-streamed attack. See Conway and Dillon, 'Case Study: Future Trends – Live-Streaming Terrorist Attack?'.
80. Elizabeth Dwoskin and Craig Timberg, 'Inside Youtube's Struggles to Shut Down Video of the New Zealand Shooting – And the Humans who Outsmarted its Systems', *Washington Post*, 18 March 2019; Chris Sonderby, 'Update on New Zealand',

faced by tech companies, but also the complex and integrated media ecosystem in which the material was disseminated and the current limits to systems for spotting and removing such events. Following this event, the 'Christchurch Call to Action', led by New Zealand's Prime Minister Jacinda Ardern, highlighted the need for governments and tech companies to work together 'to respond rapidly, effectively and in a coordinated manner to the dissemination of terrorist or violent extremist content following a terrorist event'.[81]

Importantly, however, it is not only the actors that carried out the attack that seek to control the emerging narrative for their own ends. Frequently, other extremist groups quickly emerge to exploit the events for their own agenda. In the aftermath of the attack on Lee Rigby, the British far-right organisation, the English Defence League (EDL), was quick to exploit the attack, tweeting in the hours after the attack:

> @Official_EDL: ****Confirmed we have been subject to a terror attack by Islam, we are currently under attack**** (18:06)[82]

In their work analysing the social media response to the attack, Colin Roberts and colleagues highlighted: 'Two features of this message are important to tease out. First, there is a collectivization of the threat by invoking that it is "we" who have been attacked, not just the victim. Second, there is an attribution to "Islam" rather than just the two suspects'.[83] The EDL exploited the attack as a means to galvanise existing supporters and to reach out to new supporters, but also framed the event to justify retaliatory action.[84] These tweets were quickly followed up by others seeking to mobilise supporters on the ground:

> @Official_EDL: EDL leader Tommy Robinson on way to Woolwich now, Take to the streets peeps ENOUGH IS ENOUGH (18:26)[85]

> @Official_EDL: Message from Tommy—Feet on the streets anyone want to go to Woolwich contact him/me, he will be there around 9pm (18:59)[86]

By 9pm that evening, there were EDL members on the streets of Woolwich demonstrating and throwing bottles and stones at the police.[87] In the wake of the attack, 'retaliatory' acts took place against mosques and Islamic centres across the UK, including arson, explosives devices and graffiti.[88] Online, the attack was followed by a marked spike in cyberhate.[89] These post-incident reactions are not unusual: numerous studies have shown that jihadist terrorist attacks are often followed by a spike in Islamophobic hate speech and physical violence.[90] Such retaliatory violence after a terrorist attack is highly influenced by the dynamics of meaning generation in the wake of the attack.[91] Hence, there is potential for post-incident communications campaigns to influence meaning generation in a way to minimise follow-on violence. One study has highlighted the absence of a spike in reported hate incidents following the Westminster Bridge attack in March 2017, attributing this in part to the Metropolitan Police's implementation of their National 14-Day Plan (terror incident response plan),[92] for the first

Facebook, 18 March 2019, <https://newsroom.fb.com/news/2019/03/update-on-new-zealand/>, accessed 19 December 2019; Hadas Gold, 'In the New Zealand Mosque Attack, the Media Faces an All-Too-Familiar Problem', *CNN*, 15 March 2019.

81. Christchurch Call, 'The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online', <https://www.documentcloud.org/documents/6004545-Christchurch-Call.html>, accessed 29 July 2019.
82. Martin Innes et al., 'Ten "Rs" of Social Reaction: Using Social Media to Analyse the "Post-Event" Impacts of the Murder of Lee Rigby', *Terrorism and Political Violence* (Vol. 30, No. 3, 2018), p. 465.
83. Colin Roberts et al., 'After Woolwich: Analyzing Open Source Communications to Understand the Interactive and Multi-Polar Dynamics of the Arc of Conflict', *British Journal of Criminology* (Vol. 58, No. 2, 2018), p. 442.
84. Innes et al., 'Ten "Rs" of Social Reaction'; Roberts et al., 'After Woolwich'.
85. Innes et al., 'Ten "Rs" of Social Reaction', p. 465.
86. *Ibid.*, p. 465.
87. Roberts et al., 'After Woolwich', p. 441.
88. *Ibid.*, p. 441.
89. Williams and Burnap, 'Cyberhate on Social Media in the Aftermath of Woolwich'.
90. For a collection of related studies, see John Esposito and Derya Iner, *Islamophobia and Radicalization: Breeding Intolerance and Violence* (Basingstoke: Palgrave Macmillan, 2018).
91. Innes et al., 'Ten "Rs" of Social Reaction'.
92. The National 14-Day Plan is a communication plan designed to respond to predicted public responses to a terrorist attack, with the objective to shape headlines and wider reporting on the attack.

time and called for all police forces to develop similar response plans.[93]

Another category of communications actor is those who, by accident or design, spread rumours, conspiracies or misinformation. Terrorist attacks are often followed by various conspiracy theory claims. An hour after the Westminster Bridge attack, for example, 'twitter was flooded with conspiracy theories that the entire event had been "spoofed", was a "false flag", a hoax or staged incident'.[94] In the wake of the Woolwich attack, conspiracy theories circulated on the internet, 'that Fusilier Rigby's murder was plotted by MI5 to encite [sic] Islamaphobia in Britain'.[95] At their core, conspiracy theories often latch on to the inevitable discrepancies in early reports or connect unrelated facts and build them into an elaborate theory, which is then presented as 'the truth'.

Whilst rumours and conspiracies are not new, social media as a medium of dissemination and amplification has added to their potency. Traditional media historically functioned as 'gatekeepers' in the circulation of information, usually (but of course not always) filtering out the unverified and obviously false. Social media is now a central part of the media ecosystem and can facilitate the unabated flow of such claims.[96] The issue of misinformation[97] has allegedly become such a problem following mass shootings that Google has had to amend its algorithm to compensate, by increasing 'the weight of "authority"' in the rankings so that high-quality information is returned rather than misinformation in the critical time period.[98]

Perhaps the most worrying trend is that of foreign influence campaigns targeting the post-incident communications space

As well as playing an important role in meaning generation, disinformation and misinformation can play a disruptive role in ongoing incidents and during emergency services' responses. Following the 2017 Manchester Arena bombing, a rumour circulated across social media of an active shooter at the local Oldham hospital. As a result, ambulances and fire services were held back at the cordon while the rumour was investigated, ultimately delaying them reaching the victims.[99]

Perhaps the most worrying trend is that of foreign influence campaigns targeting the post-incident communications space. These seek to interfere with and manipulate the communication flows to influence the meaning generation phase to serve a hostile political agenda. In particular, evidence has emerged of Russian influence campaigns at work during the 2017 terrorist attacks in the UK:[100] Martin Innes and colleagues identified 47 fake social media accounts that were active in the aftermath of four terrorist attacks and which attempted to 'influence and interfere in the public debate'.[101] In what appears to be a notable

93. Kim Sadique, James Tangen and Anna Perowne, 'The Importance of Narrative in Responding to Hate Incidents Following "Trigger" Events', research report prepared for TellMAMA, November 2018.
94. Innes et al., 'From Minutes to Months', p. 39.
95. Ryan Jennings, 'Conspiracy Theorist Claimed Lee Rigby Never Existed and his Murder was a Hoax, Court Hears', *The Mirror*, 30 July 2015; Helen Barnett, 'Troll Who Said Lee Rigby Murder was a Hoax Guilty of Harassing Soldier's Grieving Family', *The Express*, 31 July 2015.
96. Brigitte L Nacos, 'Terrorism/Counterterrorism and Media in the Age of Global Communication', paper presented to the United Nations University Global Seminar Second Shimame-Yamaguchi Session, Terrorism – A Global Challenge, Hamada, 5–8 August 2006, <http://archive.unu.edu/gs/files/2006/shimane/Nacos_text_en.pdf>, accessed 16 December 2019; Josh Greenberg and T Joseph Scanlon, 'Old Media, New Media, and the Complex Story of Disasters', in Susan L Cutter (ed.), *Oxford Research Encyclopedia of Natural Hazard Science* (Oxford: Oxford University Press, 2016), p. 16; Paul Reilly and Dima Atanasova, 'A Report on the Role of the Media in the Information Flows that Emerge During Crisis Situations', CascEff project report, 2016.
97. Misinformation is 'information that is false but not created with the intention of causing harm'. In contrast to disinformation, which is 'information that is false and deliberately created to harm a person, social group, organisation or country'. See Cherilyn Ireton and Julie Posetti, *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training* (Paris: UNESCO, 2018), <https://en.unesco.org/fightfakenews>, accessed 29 July 2019.
98. Alex Hern, 'Google Tweaked Algorithm After Rise in US Shootings', *The Guardian*, 2 July 2018.
99. Innes et al., 'From Minutes to Months', p. 33.
100. Westminster, Manchester Arena, London Bridge and Finsbury Park.
101. Martin Innes, 'Russian Influence and Interference Measures Following the 2017 UK Terrorist Attacks', policy brief prepared for Cardiff University Crime and Security Research Institute, Centre for Research and Evidence on Security Threats (CREST), 2017, p. 1, <https://crestresearch.ac.uk/download/4397/>, accessed 16 December 2019.

example of Russian influence, social media 'sock puppets' were used in the wake of the Westminster Bridge attack in a sophisticated attempt to drive polarisation. The now infamous image of a Muslim woman walking over Westminster Bridge, apparently (but incorrectly) ignoring victims as they were being treated, soon became an internet 'meme'. The dispute over the correct meaning of this image was influenced and amplified by fake social media accounts, apparently created in Russia, which participated in a synchronised campaign pushing opposing commentaries to create and drive polarisation.[102] For example, one fake account, @Ten_GOP, forwarded the image accompanied by the comments: 'She is being judged for her own actions & lack of sympathy. Would you just walk by? Or offer help?'. In contrast, a second fake account, @Crystal1Johnson, pushed the narrative 'so this is how a world with glasses of hate look like - poor woman, being judged only by her clothes'.[103] These actions were essentially designed to attempt to manufacture polarisation within the wider public debate in the wake of the attack.

The level of social harm and the impact of a terrorist attack is in part determined by the public sense-making or meaning generation after the event. This process of perception and interpretation can be influenced by both benevolent and malignant actors. Given that multiple malign actors are often active in shaping the narrative in the aftermath of a terrorist attack to suit their own agendas, it is crucial that governments do not surrender this communication space and thereby lose control of the public narrative. In order to ensure this does not happen, it is crucial that the government's strategic communications includes planning for a post-attack response.

Conclusions

This article set out to demonstrate how strategic communications has much to add to an effective CT strategy. Strategic communications, as it is currently applied within UK CT policy, is largely within the Prevent pillar of the CONTEST strategy. However, strategic communications has a much broader application and the potential to make significant contributions across the four pillars of the CONTEST strategy.

A review of CONTEST to incorporate a greater involvement of strategic communications is recommended. However, this should not be done piecemeal, with scattered ad hoc additions of strategic communications to individual aspects of CONTEST. The important point about strategic communications, which is often forgotten, is that it is meant to be strategic. In order to secure this, and to ensure its greatest impact, strategic communications needs to be an integral part of the overall CT strategy. To be strategic, it cannot simply be added on to a few individual aspects, it needs to be applied across the totality of the CT strategy. After all, as communication is central to terrorism, it is inevitable that strategic communications should be central to any effective CT strategy. ■

Andrew Glazzard is a Senior Associate Fellow at RUSI and was formerly Senior Director for National Security Studies at RUSI.

Alastair Reed is an Associate Professor at the Cyber Threats Research Centre (CYTREC) at Swansea University in the UK and at Delft University of Technology (TU Delft) in the Netherlands. He is also an Associate Fellow at RUSI and the Director of the Research Advisory Council at the RESOLVE Network.

102. *Ibid.*, p. 4.
103. *Ibid.*, p. 3.