Global Research Network on Terrorism and Technology: Paper No. 12

Towards a Framework for Post-Terrorist Incident Communications Strategies

Alastair Reed and Hararo J Ingram
Key Findings and Recommendations

Terrorism is fundamentally a type of violent communication designed to influence audiences broader than the direct recipients of that violence. Consequently, post-terrorist incident responses may significantly shape how a terrorist attack is perceived and its implications. Social media platforms, especially, play a significant role in the modern crisis-communication media ecology and the processes of public sense-making. This paper identifies the need for post-terrorist incident communications strategies, draws out pertinent lessons from a multidisciplinary literature analysis and outlines key considerations for the technology, government and media sectors when creating guidelines to respond to terrorist events.

This paper identifies six key lessons that should guide the development of a post-terrorist incident response framework:

• Post-incident responses need to be calibrated to ‘compete’ against malignant actors (such as terrorist propagandists) in an effort to shape meaning-generation processes in target audiences.
• Post-incident guidelines must harness the ecology of crisis communications of which social media is an important, but not the only, component. No medium of communication is inherently positive or negative. Instead, strategies need to be devised to harness its potential positive effects.
• Social media platforms can play a key role in assisting emergency services and, rather than shutting down after a terrorist attack, these mediums can be used to reassure, advise and inform.
• Social media platforms and media organisations will need to work collaboratively to ensure post-incident reporting frameworks are complementary.
• Social media companies will need to be prepared to remove terrorist content, especially that which is designed to trigger and amplify fear in target audiences, in a timely and appropriate manner.
• Social media platforms can play a significant role in post-incident responses in appreciating and assisting the importance of the online space for bringing communities together in the wake of a terrorist attack as a shared space for grieving and sense-making.

Introduction

Terrorism is communication through violence intended to have psychological, social and political effects beyond mere target destruction. The primary target of modern terrorism is often not the immediate victims of its violence but the wider audience of perceived enemies, who the perpetrators seek to terrorise, and potential supporters, who they seek to inspire. As Paul Wilkinson says, ‘terrorism by its very nature is a psychological weapon which
depends upon communicating a threat to the wider society’. Hence the communication of an attack plays an essential part in achieving the terrorist’s objectives and maximising the harm experienced by society.

Traditionally, counterterrorism and countering violent extremism strategic communications have focused on challenges such as preventing radicalisation and recruitment. However, there is a clear need to develop communication strategies to counter the potential post-incident impact and harm caused by terrorist violence. Ultimately, since it is impossible to prevent every attack, it is important to be prepared to mitigate the impact in the aftermath of an incident. Research from various disciplines has demonstrated how responses to terrorist incidents (and other violent crimes) may amplify the impact of terrorist attacks, inadvertently assisting terrorists to achieve their aims, and even act as a catalyst for a cycle of retaliatory violence, collective victimisation and widespread fear.

Guidelines for shaping how social media companies, governments and the media respond to terrorist activities are essential. This paper explores what lessons can be drawn from various bodies of research and practice to inform such a framework of guiding principles. It synthesises research on post-incident communications from a range of fields – including terrorism, crisis communications, mass-shooter incidents, serial offenders, and suicide studies – to identify guidelines for the development of a post-terrorist incident communications framework. It begins by examining the interplay of terror, inspiration and retaliation in the aftermath of a violent event and considers its implications for guideline development. The paper concludes by outlining key lessons for developing a post-incident framework that the technology sector, government and media organisations should consider.

**Terror, Inspiration, Retaliation: The Role of Social Media in Terror’s Compounding Cycle of Effects**

When terrorist acts are seen as communicative in seeking to achieve a propagandistic purpose beyond immediate rudimentary aims of destruction, the violence itself emerges as merely the initial trigger that is designed to set off secondary and tertiary effects. Key to these efforts are inducing terror in ‘enemy’ target audiences and inspiration in potential communities

---

of support. These effects may in turn motivate retaliatory speech acts (such as hate speech) and actions (such as terrorism) targeting those that are (often incorrectly) identified with the terrorist’s cause. This potentially compounding cycle of terror, inspiration and retaliation effects in the aftermath of a terrorist attack can be exponentially amplified by modern communication technologies. Social media platforms have emerged as primary forums in which the processes of meaning generation occur, often in real time, after a terrorist incident. Understanding these dynamics must be central to the development of nuanced and effective guidelines.

**Fear: The Psycho-Social Impact of Terrorist Acts**

A process of public sense-making, whereby people interpret and give meaning to their experiences, occurs in the aftermath of a terrorist attack.⁴ The influence of social media in shaping how individuals and groups make sense of terrorist incidences must be understood within the context of a complex ecology of communication mediums and information sources deployed by a diverse array of actors. Tony McEnery, Mark McGlashan and Robbie Love, Sofia Patel, and Martin Innes and his co-authors examine the interplay of ‘old’ and ‘new’ media in shaping how audiences understand a terrorist incident and its implications for perceptions of public safety and national security.⁵ All three studies highlight how traditional news media reporting tends to shape discourse on social media. Nevertheless, interactions on social media platforms subsequently shape how news media reporting is understood, interpreted and acted upon. A study by Martin Innes and his co-authors examines 10 forms of social reaction following the 2015 Woolwich terrorist attack examining ‘the complex and somewhat chaotic nature of public sense-making and interpretation that arises in the aftermath of a terrorist attack’.⁶ Such studies have shown that the impact of a terrorist attack may be shaped as much by the response and communications after the incident as by the act itself.⁷

---


7. For example, see 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; Mia Bloom, ‘Terror 101: The
While the process of public sense-making is inevitably complicated and messy, it is not random given both the psychosocial dynamics at play and the fact that certain actors are seeking to influence how events are perceived. For instance, terrorist propagandists will almost inevitably be seeking to deliberately and strategically fuel fears and shape how the violence and its implications are understood. Studies by Brigitte Nacos and Haroro Ingram emphasise the importance of using a nuanced understanding of the rationale driving terrorist ‘propaganda of the deed’ to inform practical guidelines for how journalists engage in responsible reporting and social media companies manage their platforms. For example, when social media is used by terrorists to communicate with target audiences and this propaganda is then used by the news media to inform journalistic reporting, there is a risk of inadvertently amplifying terrorist goals. Indeed, many of the recommendations in the studies related to traditional media reporting are equally applicable for social media companies seeking to manage the type and movement of content on their platforms.

The Immediate Aftermath

Social media forums have assumed an increasingly important role as a major channel of communications in the immediate aftermath of a terrorist attack. Digital communications are part of a ‘new ecology of emergency media’ incorporating traditional mass media alongside other forms such as SMS. For the public, social media can be used for situational awareness, to find safety information from emergency services, to contact friends and family that are missing, and to organise responses and share experiences.

Transnational Contagion Effects of Suicide Bombing’ in Mia Bloom, *Dying to Kill: The Allure of Suicide Terror* (New York: Columbia University Press, 2005).


Members of the public have even been encouraged at times to communicate via social media following an attack as mobile networks can quickly become saturated. Facebook, for example, has invented a Safety Check app that allows users in the vicinity of a terrorist attack (or other extreme events) to report themselves as safe for their friends and family to see.

A key change in the reporting of terrorist attacks is that news of such attacks is often first broken on social media by members of the public on location, circumventing the usual media gatekeepers and leading to the flow of unfiltered information into the public domain. As a result, it is virtually impossible for emergency services and traditional media to control the flow of information from a terrorist attack, creating space for multiple and competing narratives to circulate after an attack. The increase in user-generated-content and the role of first informers as eyewitnesses who share their experiences of crisis situations directly online has resulted in a flood of information into the public sphere chaotically impacting how populations make sense of what is happening and what it means.

Increasingly, traditional media are drawing on user-generated content for their reporting, which raises questions about how the media should treat such sources, especially regarding variability and trustworthiness. Josh Greenberg and T Joseph Scanlon note:

> While there is enormous potential to harness social and mobile media to improve communication flows and facilitate social mobilization during a disaster, there are also important drawbacks and limitations. False information may be an inherent problem, given the number of people creating information at the same time, and often with different interests and vantage points.


One danger in the immediate aftermath of attacks is that misinformation and rumours can spread on social media, which can impede the response of emergency services and aggravate an already dangerous situation. In the wake of the 2017 Manchester Arena bombing, a rumour circulated on social media that there were gunmen active at the local Oldham Hospital. The rumour had a direct impact on the emergency services response, as ambulances and fire crew were initially held at the cordon, delaying them from reaching the victims. The power of rumours on social media has also been seen to escalate apparent minor events into a perceived terrorist attack. On 24 November 2017, reports of an alleged terror attack near Oxford Circus underground station in central London led to a panic with masses running away from the scene, triggering a terrorist incident response from the Met Police. It turned out to be a false alarm, with a minor altercation between two men on the underground having sparked a wave of escalating rumours across social media.

As well as being used for strategic communications by terrorist groups, social media is also being exploited as a tactical tool during terrorist attacks. The unfiltered flow of information from members of the public in the area can provide invaluable situational awareness to terrorist actors operating during an attack. For instance, during the 2008 Mumbai attack the terrorists monitored social media forums to gain situational information that they then used to direct their actions.

Social media has not just been used as a tool by terrorists, but has also become an important medium of communication for emergency services, especially as a direct line of communication to members of the public. Following the 2017 Westminster Bridge attack, the Metropolitan Police put out their first tweet reassuring the public that action was being taken within seven minutes. Further, the multidimensional nature of social media allows ‘key stakeholders to gather information from multiple sources’. It has also proved a successful tool for mobilising and coordinating public responses. For

instance, in the wake of the 2011 Oslo attacks, Twitter was used effectively by Oslo University Hospital to attract and coordinate blood donors.23

Social media has become an essential part of the crisis communication ecology, providing real-time information and multi-directional information flows. It is crucial that emergency services use social media as part of their communications strategy and provide information as quickly as possible to offer reassurance and practical information, and to prevent the spread of rumours from filling the information vacuum. The risk for social media companies is that over-policing could undermine precisely why these platforms can be an effective way to rapidly communicate to large audiences and, in doing so, save lives. First and foremost, harnessing the benefits of social media in the immediate aftermath of an attack will require benevolent actors to be far more strategically and technologically aware – outcompeting malevolent actors – and it is in this way that social media companies may be of greatest help.

The Battle to Frame Terrorist Attacks

As the dust begins to settle after a terrorist attack, the process of sense-making by the public accelerates.24 This period is typically complex and confused, with either limited or too much information, contradictory and competing views, and as such, meaning generation can be chaotic. It is at this point that the battle to frame how events are to be understood is at its most critical.25 In this fluid period, different actors compete for advantage to exploit how the attack is understood, shaping perceptions and thus directing meaning formation. There can be a clear early entrant advantage in shaping perceptions. If there is no early response from benevolent actors, this leaves a vacuum to be filled by other, perhaps more malevolent, actors (such as terrorist and their supporters).26

Terrorist Actors

Terrorists have always been fast adopters of new technology, from dynamite to hijacking jet planes, and social media has proven no exception.27 While previously terrorist groups have had to rely on manipulating the media into covering their actions, social media presents a means of bypassing these

23. Steensen et al., ‘Social Media and Situation Awareness During Terrorist Attacks’.
24. Innes et al., ‘Ten “Rs” of Social Reaction’.
25. Williams and Burnap, ‘Cyberhate on Social Media in the Aftermath of Woolwich’.
26. Innes et al., ‘From Minutes to Months’, p. 34.
traditional gatekeepers.\textsuperscript{28} The advent of Web 2.0 and mobile phones has meant that whenever an attack takes place, there are members of the public to cover the events live.\textsuperscript{29} The 2013 murder of Lee Rigby, for example, was live-tweeted by bystanders and in the aftermath, attackers sought out members of the public to make the now infamous video message of one of the attackers.\textsuperscript{30} The 2015 Bataclan theatre attack in Paris and the 2016 Brussels airport attacks were similarly covered live on social media by members of the public caught up in the violence.\textsuperscript{31}

In recent years, there have been several examples of terrorist groups seeking to cover their own attacks live via social media, rather than relying on bystanders. During the 2013 Westgate shopping centre attack in Nairobi Al-Shabaab terrorists live-tweeted throughout the attack, providing their account of events and justifying their actions.\textsuperscript{32} This allowed them to provide their own framing of the attack and to challenge the narrative presented by journalists and the authorities.\textsuperscript{33} Although not the first live-streamed terrorist attack,\textsuperscript{34} the Christchurch Mosque attacks took the self-coverage of terrorism to a new level. The perpetrator’s extensive preparations ensured that the livestreaming of the attack and his manifesto went viral.\textsuperscript{35} Social media platforms struggled in the immediate aftermath to prevent the posting of the video – Facebook alone reported the video being uploaded 1.5 million times to its platform in the 24 hours after the attack.\textsuperscript{36} Highlighting the complex media ecology at play, coverage of the video in mainstream media appears to have played an important role in driving it viral online.

\begin{itemize}
  \item \textsuperscript{28} Elizabeth Lopatto, ‘The Mass Shooting in New Zealand was Designed to Spread on Social Media’, \textit{The Verge}, 15 March 2019.
  \item \textsuperscript{29} Conway and Dillon, ‘Case Study: Future Trends’.
  \item \textsuperscript{31} Conway and Dillon, ‘Case Study: Future Trends’.
  \item \textsuperscript{33} Innes et al., ‘From Minutes to Months’, p. 37.
  \item \textsuperscript{34} Conway and Dillon, ‘Case Study: Future Trends’.
  \item \textsuperscript{35} Lopatto, ‘The Mass Shooting in New Zealand’.
\end{itemize}
Exploitation by Other Extremist Groups

In the aftermath of a terrorist attack, the events are frequently exploited by other extremist organisations — often of opposing ideology — seeking to shape how the incident is perceived and interpreted for their own ends. For example, following the murder of Lee Rigby by Islamist terrorists, the far-right English Defence League was quick to seize on the events to promote their own agenda. The group tweeted 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)

The tweet was a clear attempt to frame and justify retaliatory action. Similarly, Daesh (also known as the Islamic State of Iraq and Syria, ISIS) sought to exploit the recent Christchurch attacks to call for retaliatory violence. Daesh spokesman Abu Hassan Al-Muhajir broke a six-month silence to release an audio recording, arguing: ‘The scenes of the massacres in the two mosques should wake up those who were fooled, and should incite the supporters of the caliphate to avenge their religion’. Such actors seek to manipulate instinctive human responses to terrible events. In the aftermath of a terrorist incident, it is common for public reaction to transition from shock and sadness to anger. The potential for retaliatory violence after a terrorist attack is highly likely to depend on the dynamics of meaning generation highlighted earlier. For example, there has been a surge in studies analysing how, after jihadist terrorist attacks, there can be a spike in Islamophobic words and actions. Social media platforms act as forums for how people generate meaning and, for some social networks, this has led to growing Islamophobia.

37. Innes et al., ‘Ten “Rs” of Social Reaction’.
39. Innes et al., ‘Ten “Rs” of Social Reaction’.
Rumours and Conspiracy Theories

It is not just terrorist actors that shape the post-incident communication space, but also those who, by accident or design, spread rumours, conspiracies or misinformation. The chaos of sense-making that follows an attack provides the ideal breeding ground for rumours and conspiracy theories to spread. For example, within an hour of the 2017 Westminster Bridge attack, Twitter was flooded by conspiracy theories purporting that the attack was a false-flag attack or an elaborate hoax. Such conspiracy theories often latch onto the inevitable discrepancies in early reports or connect unrelated facts and build them into a narrative, which is then presented as truth. Sometimes conspiracy theories may even try to portray non-terrorist incidents as terrorist attacks that have been covered up. Following the recent fire that devastated the Notre Dame cathedral in Paris, social media platforms saw a surge of conspiracy theories, many of which suggested the fire was set by terrorists, including ‘tweets from accounts purporting to be news outlets such as CNN and Fox News’.

Third-Party Agitators: Foreign Influence Operations

One of the more concerning dimensions of the post-incident environment has been the emergence of malignant third-party agitators who manipulate social media to spread disinformation and amplify the public impacts of terrorist attacks. One study identified 47 different fake social media accounts linked to Russia that were active after four terrorist attacks in the UK in 2017, which attempted to ‘influence and interfere in the public debate’. A striking example of the elaborate attempts to drive polarisation was the use of ‘sock puppets’ by Russian-linked accounts in the wake of the Westminster attack. The now infamous image of a Muslim woman walking over Westminster Bridge apparently (and incorrectly) showing her ignoring victims as they were being treated was circulated by different accounts in synchronisation, but accompanied by opposing commentary to instigate a polarising online debate. It is crucial that government and law enforcement agencies respond with a post-incident communication strategy to limit the harm created, and prevent it being amplified by others. A leading example of good practise is the UK Metropolitan Police’s national 14-day action plan, designed to help

---

42. Innes et al., ‘From Minutes to Months’, p. 39.
43. Sarah Manavis, ‘Conspiracy Theories About the Notre Dame Fire are Already Beginning to Spread: 4chan, Reddit, and Twitter are Rife with Fake News About the Catastrophe’, New Statesman, 16 April 2019.
46. Innes, ‘Russian Influence and Interference Measures’, p. 4.
manage the narrative in the wake of a terrorist attack. A recent report argued that the implementation of the plan in the aftermath of the 2017 Westminster Bridge attack played a significant role in preventing the expected spike in recorded hate incidents that followed other terror attacks.

**Inspiration: Post-Incident Contagion and Copycat Dynamics**

Many studies have addressed how the coverage of violence – from suicide to mass shootings and terrorism – may trigger a ‘contagion’ and/or ‘copycat’ effect in a population. David P Phillips’s seminal research into the ‘Werther effect’ demonstrated a positive correlation between media (newspaper) coverage of suicides and an increase in suicide rates. Phillips further argued that the perceived prestige of the individual (such as celebrity) and the similarity of their circumstances (such as identity and life situation) also increased imitation. The general consensus in the literature is that the Werther effect is empirically supported across time and both ‘old’ and ‘new’ media studies. However, there have also been studies keen to highlight that ‘old’ and ‘new’ media can also have a positive influence on preventing suicide described as the ‘Papageno effect’.

48. Sadique et al., ‘The Importance of Narrative in Responding to Hate Incidents Following ‘Trigger’ Events’.
49. The phrase ‘Werther effect’ is named after the main character of Johann Wolfgang von Goethe’s *The Sorrows of Young Werther*, published in 1774, in which the story’s hero commits suicide. The book was meant to have inspired ‘copycat’ suicides by young men influenced by Werther.
This suggests that coverage of violence, even if self-directed violence, may inspire others. A significant body of literature explores a Werther-like effect for the reporting of violent crimes as a driver of copycats, especially concerning mass shooters and serial offenders. Studies have explored how media reporting may contribute to a ‘role modelling’ dynamic whereby susceptible individuals adopt the traits and tactics of violent criminals, with some arguing that the two weeks after a violent event are the crucial period for contagion effects while others refute this claim. Like the self-harm literature, analysts of mass-shooting phenomena highlight the celebrity-like status bestowed upon mass killers, such as a greater emphasis being placed on the perpetrators over the victims in reporting, as a potential driver of copycat actions. Given the potentially higher rates of narcissism among mass shooters and those that may be inspired by them, old and new media may have a greater responsibility to avoid inadvertently elevating the status of

---


such criminals. While the terrorism-specific literature is comparatively much smaller than the suicide and violent crime literature, much of the former shares broadly similar findings regarding potential clustering in suicide attacks and the catalytic role of social media in ‘lone actor’ sprees.

Conclusion: Lessons and Recommendations from the Literature

The following lessons and recommendations can be drawn from this paper’s literature review:

- The response to a terrorist attack has a major impact on how events will be interpreted by the public. Viewing terrorist incidents through the lens of meaning generation and re-shaping post-incident responses through the lens of a ‘competition’ to shape meaning will be essential to recalibrating strategic policy for government, tech companies and the media.
- Post-incident guidelines must take into account the ecology of crisis communications of which social media is an important, but only one, component. The flow of unfiltered communications via first informers and other user-generated content can have both positive and negative impacts. Traditional media may play an essential role in these dynamics. The challenge is harnessing the potential of the media ecology for positive over negative effects.


63. Nicholas Farnham and Marieke Liem, ‘Can a Copycat Effect be Observed in Terrorist Suicide Attacks?’, International Centre for Counter-Terrorism, 2017.

• Social media platforms can play a key role in assisting emergency services in both planning and raising awareness of mechanisms for supporting those objectives. This should include how to best provide reassurances and practical advice, and how to prevent a news vacuum in which rumours and misinformation thrive. Social media platforms can also greatly assist in situational awareness and understanding for emergency responders and the public.

• Social media platforms and media organisations will need to work collaboratively to ensure post-incident reporting frameworks are complementary. One area where the relationship between old and new media technologies can advance better practice is by providing advice to practitioners and users on how to use their platforms appropriately.

• Social media companies will need to be prepared to remove terrorist content, especially that which is designed to trigger and amplify fear in target audiences, in a timely and appropriate manner. Crisis communication response teams may be necessary to more effectively and efficiently respond to terrorist incidences. This may include social media listening capabilities to monitor social media as a means to identify those seeking to exploit terrorist incidents to incite: hate, polarisation or retaliation; misinformation, conspiracy and rumours; and foreign influence.

• Harnessing the opportunities afforded by social media platforms is perhaps the most significant way in which technology companies can respond to incidents. For example, appreciating the importance of the online space for bringing communities together in the wake of a terrorist attack as a shared space for grieving and sense-making will be essential. In harnessing social media as a forum for ‘positive’ processes of meaning generation, these efforts can increase resilience and nullify efforts to polarise and mobilise towards violence.

This paper has laid the foundations for establishing a comprehensive framework of principles for post-incident strategic communications which will follow in a subsequent publication.

Alastair Reed is an Associate Fellow at the International Centre for Counter-Terrorism (ICCT) and an Associate Professor at Swansea University and TU Delft in the Netherlands,

Haroro J Ingram is an Associate Fellow at the International Centre for Counter-Terrorism (ICCT) and a Senior Research Fellow with the Program on Extremism at George Washington University.
About RUSI

The Royal United Services Institute (RUSI) is the world’s oldest and the UK’s leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today’s complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

About The Global Research Network on Terrorism and Technology

The Global Research Network on Terrorism and Technology is a consortium of academic institutions and think tanks that conducts research and shares views on online terrorist content; recruiting tactics terrorists use online; the ethics and laws surrounding terrorist content moderation; public–private partnerships to address the issue; and the resources tech companies need to adequately and responsibly remove terrorist content from their platforms.

Each publication is part of a series of papers released by the network on terrorism and technology. The research conducted by this network will seek to better understand radicalisation, recruitment and the myriad of ways terrorist entities use the digital space.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel), and the Institute for Policy Analysis of Conflict (Indonesia).

The research network is supported by the Global Internet Forum to Counter Terrorism (GIFCT). For more information about GIFCT, please visit https://gifct.org/.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.