

# SOFT FACTS AND DIGITAL BEHAVIOURAL INFLUENCING AFTER THE 2017 TERROR ATTACKS

FULL REPORT  
FEBRUARY 2020

Martin Innes

# SOFT FACTS AND DIGITAL BEHAVIOURAL INFLUENCING AFTER THE 2017 TERROR ATTACKS

## FULL REPORT

Martin Innes

Crime and Security Research Institute, Cardiff University

This is the full report from the *Soft Facts And Digital Behavioural Influencing* project, funded by CREST. To find out more about this project, and to see other outputs from the team, visit:  
[www.crestresearch.ac.uk/projects/soft-facts-digital-behavioural-influencing](http://www.crestresearch.ac.uk/projects/soft-facts-digital-behavioural-influencing)

This project reflects a growing awareness and concern amongst policymakers and practitioners about how the community impacts of terrorism and other major crime events are frequently amplified as a result of rumours, deliberately generated 'false news' and conspiracy theories. There is interest also in how such effects can be countered through deploying artfully constructed counter-narratives.

### About CREST

The Centre for Research and Evidence on Security Threats (CREST) is a national hub for maximising behavioural and social science research into understanding, countering and mitigating security threats. It is an independent centre, commissioned by the Economic and Social Research Council (ESRC) and funded in part by the UK security and intelligence agencies (ESRC Award: ES/N009614/1).  
[www.crestresearch.ac.uk](http://www.crestresearch.ac.uk)



# TABLE OF CONTENTS

<b>1. EXECUTIVE SUMMARY</b> .....	<b>5</b>
<b>2. INTRODUCTION</b> .....	<b>7</b>
<b>3. SOCIAL REACTIONS AND SOCIAL MEDIA</b> .....	<b>9</b>
<b>4. RESEARCH DESIGN AND METHOD</b> .....	<b>12</b>
<b>5. FOUR ATTACKS IN 2017</b> .....	<b>14</b>
5.1 Westminster.....	14
5.2 Manchester Arena .....	14
5.3 London Bridge.....	15
5.4 Finsbury Park .....	15
<b>6. A CONCEPTUAL MODEL OF INFLUENCE</b> .....	<b>17</b>
<b>7. TECHNIQUES OF DISINFORMATION</b> .....	<b>19</b>
7.1 SEEDING .....	19
7.2 DENIAL OF CREDIBILITY.....	21
7.3 EVENT GHOSTING.....	22
7.4 EMULSIFYING.....	24
7.5 INFILTRATING AND INCITING .....	26
7.6 SPOOFING .....	26
7.7 TRUTHING .....	27
7.8 SOCIAL PROOFING.....	28
<b>8. CONCLUSION</b> .....	<b>30</b>
<b>READ MORE</b> .....	<b>31</b>



---

# 1. EXECUTIVE SUMMARY

---

This report analyses social media data collected in the aftermath of four terror attacks that took place in the UK in 2017, to explore how various rumours, conspiracy theories, propaganda and fake news shaped social reactions to these incidents, and the ways they came to be defined and understood. For the purposes of this analysis we collectively define these informational forms as ‘soft facts’. Where ‘hard facts’ are objective and stable, soft facts are malleable and contested. They are an important feature of the contemporary media ecosystem, especially in moments of emergency and crisis when people are highly influenceable.

The principal output of this analysis is the conceptualisation of eight ‘techniques of disinformation’. Individually and collectively these are designed to capture key methods in terms of *how* misleadingly influential communications are constructed and communicated:

## SEEDING

Seeding involves utilising misinformation to create an element of doubt in the minds of the audience members, in terms of what to believe about an occurrence. In effect, communicating misinformation serves to create the conditions for disinformation, shaping the thoughts, feelings and behaviour of the audience.<sup>1</sup>

## DENIAL OF CREDIBILITY

Denial of credibility is where an attempt to undermine belief or trust in a specific unit of information is predicated upon attacking or undermining the source in some way. This often involves impugning the source’s motives, or past behaviour in some fashion.

## EVENT GHOSTING

‘Event ghosting’ is a way of changing the meaning of an event or episode for an audience, via the insertion of made-up features into narratives about it. Importantly, most of the time this is not accomplished by devising an alternative narrative, but by revising and editing components of one that is already established.

## EMULSIFYING

Emulsifying is based upon blending two separate event narratives together, in order to misdirect audience attention in some way. Typically, this can work in one of two ways: either by ‘loading up’ the level of complexity, such that it renders it so difficult to understand that most people don’t try; the alternative is to drastically simplify things. For instance, by suggesting that one event is just like another (when they are not actually alike).

## INFILTRATING AND INCITING

Infiltrating and inciting is a specific technique where an agent of influence deliberately enters an established thought community by mimicking their social identities and interests, with the intent to message provocatively to fire up their emotions.

## SPOOFING

Spoofing involves imitating an established digital social identity, often by co-opting linguistic tropes and visible symbols of a group.

## TRUTHING

‘Truthing’ is where support for an idea or position is based upon manipulating images, statistics, or other evidence. This can include conspiratorial ‘truth claims’ as well as ones more limited in terms of their purview.

## SOCIAL PROOFING

Social proofing uses affordances designed into social media technologies to create an aura or illusion of support or consensus around a controversial issue. This can, for example, be done by artificially inflating the number of ‘likes’ or supportive comments attached to a message. This is on the basis that such displays of consensus might modify the behaviours of other users.

Taken together, these techniques of disinformation illuminate some of the workings of digital influence engineering in the contemporary information environment. There is increasing political and public consternation about how the communication of misinformation and disinformation within and across media platforms is corroding public trust in key institutions, and democratic processes and values.

---

<sup>1</sup> Misinformation refers to inadvertently misleading communications, whilst disinformation is a deliberate attempt to deceive.

The value of adopting a digital behavioural analytics approach to this problem is in determining how these kinds of influence are being accomplished and by whom. A key aspect of the analysis lies in identifying a range of online actors engaged in constructing and communicating different kinds of soft fact. This includes:

- Citizens at the scene who misinterpret things that they see or hear, but are able to communicate these to large numbers of followers via social media without validating the provenance of the information they are sharing.
- Other citizens who, for their own personal social-psychological needs that are not terribly well understood, seek to interject themselves into the story, in ways that do not necessarily reflect what actually happened.
- Journalists who, under intense pressure to break stories before their competitors, amplify false or misleading information in ways that can have long-term consequences in terms of how an event is publicly defined and understood.
- Groups with strong ideological agendas who want to interpret occurrences in such a way that they can be seen to support their political values and perspectives.
- Hostile states who, by manipulating and amplifying particular messages, seek to exacerbate social tensions between existing groups.

This latter dimension is an especially important finding of the work for policy and practice. Unexpectedly, when analysing the empirical data collected following the four terror attacks, the researchers identified and attributed a number of Russian-linked social media accounts authoring and amplifying provocative and highly antagonistic messages. Collectively, across the accounts concerned, they were adopting a spread of different political standpoints and messaging coherent with these positions. As such, the study has identified a new and troubling dimension to what happens in the aftermath of terror attacks, in terms of what needs to be done in order to manage and mitigate the public impacts of such events.

In documenting the social dynamics and mechanics of how soft fact communications can shape and steer the ways terror events come to be interpreted and defined,

the analysis makes a distinctive contribution to a growing body of research interested in understanding processes of social reaction to terrorism. Social media are very important to such efforts, because they both fundamentally alter these processes, but simultaneously afford digital traces that enable them to be studied in high resolution, in ways that were not previously possible.

Adopting this approach, a key facet of this study is in documenting how the communication of misinformation and disinformation in the wake of a terror attack has the capacity to influence the overall levels of social harm it induces. The implications for policy and practice that flow from this insight concern the importance of actively managing the information environment and being willing to disrupt and counter any soft facts communicated following an attack.

## 2. INTRODUCTION

This document reports findings from a research project studying how a series of soft facts communicated on social media in the aftermath of four terrorist attacks that took place in 2017, functioned to influence public perceptions and understandings of the causes and consequences of these events. The research was designed to generate evidence and insights about three areas:

1. To provide an empirically led dissection of the organisation of social reactions to terrorism and how it is being transformed and altered by emerging patterns of social communication. Whilst previous research has been predicated upon single case study designs, the current project compared social media reactions across four different events.
2. How disinformation and misinformation communicated via social media platforms influences public definitions of the post-terror event situation, and the ways people think, feel and behave in relation to it.
3. To make a more general conceptual and methodological contribution to the rapidly growing literature on disinformation and its effects.

To elaborate these three themes briefly, there has been a general neglect in both policy development and academic research of what happens in the aftermath of terrorist attacks. Far greater attention and effort has been directed towards researching radicalisation interventions. However, terrorist violence is intended to ‘terrorise, polarise and mobilise’ segments of the public audience, and during such times of crisis and uncertainty many people are highly influenceable. The high resolution empirical detail provided herein, based upon systematic and structured collection and analysis of social media data, does much to enrich our collective understandings of how people react to high profile incidents of politically motivated violence.

In making a contribution to understanding these interpretative processes, the work focuses in on the role of soft facts – an umbrella concept covering a number of different ‘knowledge claims’ that are plastic, malleable and contested.<sup>2</sup> Such informational claims can be especially magnified on social media platforms given the design and the ‘media logics’ of the information environment that they are a part of. Where hard facts are ascribed objectivity and stability, a soft fact is frequently manipulated and recast, albeit it is often afforded contingent authority and credibility by some people. Herein, a soft fact is deployed as a ‘master concept’ that covers rumours, conspiracy theories, fake news and propaganda. It encompasses both misinformation (inadvertently misleading communications) and disinformation (involving deliberate attempts to deceive). This conceptual distinction is important in light of the evidence from this research, showing how instances of misinformation and disinformation frequently interact and overlap, mutually creating the conditions for one another.

Introducing the soft fact framing into this milieu, signals an intent to avoid simply repurposing more established concepts originating in a very different media ecosystem, with distinctive dynamics and mechanics. Instead, it is suggested that research needs to develop concepts that reflect the particular qualities of information and communicating in digital environments. For example, a number of recent and influential studies have opted to take as their conceptual base the literature on propaganda.<sup>3</sup> This is despite the fact that propaganda studies is clearly divided as to whether to define as propaganda occasions where the communicative action involved is not purposive. Some authors say the ontology of propaganda requires a deliberate attempt to deceive<sup>4</sup>, whilst others contest this.<sup>5</sup> Layered on top of which are more subtle inflections. For instance, in their attempt to refresh propaganda theory for the contemporary age, Woolley and Howard (2019: 4) define ‘computational propaganda’ as the “use of algorithms, automation and human curation to purposefully distribute misleading information over social networks” (note the accent upon purposive behaviour). Contrast this with another significant contribution which utilises a distinctive

2 Martin Innes, *Signal Crimes: Social Reactions to Crime, Disorder and Control* (Oxford: Oxford University Press, 2014).

3 For example, Woolley, S. and Howard, P. (2019) *Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media*. Oxford: Oxford University Press; Benckler, Y., Faris, R. and Roberts, H. (2018) *Network Propaganda: Manipulation, Disinformation and Radicalization in American Politics*. New York: Oxford University Press.

4 Jowett, G. and O’Donnell, V. (2012) *Propaganda and Persuasion* (5<sup>th</sup> edn.). London: Sage.

5 Stanley, J. (2015) *How Propaganda Works*. Princeton: Princeton University Press.

terminology of ‘network propaganda’ to convey how underpinning social and political dynamics exert a structuring influence upon communication patterns (Benkler, Faris and Roberts, 2018). Moreover, the latter study makes the important point that contemporary propaganda is not always wholly false or misleading (and that it is often difficult to be confident about its validity and reliability), something not always adequately clarified in this tradition. Ultimately, there is a danger that in reworking established concepts to encompass new arrangements, they are stretched so far that they lose their original conceptual centre and essence.

In addition to these intra-field contests over who has the correct definition and descriptor of the phenomenon, there are also inter-field tensions that can be circumvented through the introduction of a new conceptual frame. For example, those who study conspiracies tend to interpret issues in these terms, whilst scholars of rumours and/or propaganda tend towards their own lexicon and theoretical priorities.

The value of the soft fact is that it tilts the conceptual focus away from the intents or purposes of the communicating actor, more to the unit of information being communicated. This is incisive in a decentered media ecosystem, inasmuch as it helps to capture how different audience segments may simultaneously maintain different interpretations of the same material.<sup>6</sup> What counts as one person’s propaganda or conspiracy theory, may be someone else’s ‘suppressed truth’.

Moreover, and as we have seen on many occasions now, perceptions may change over time. What for many originally appeared to have been little more than a conspiracy theory, has turned out to have been a more or less accurate depiction of what actually happened. As noted above, the critical issue in many ways is not the ultimate truthfulness or falsity of the information, but whether people treat it as such – something that the notion of a soft fact articulates better than the pre-existing concepts. A quality that furthermore, is also coherent with growing evidence from social psychology that claims are more persuasive when they ‘go with the

grain’ of an individual or group’s existing beliefs and value structures.<sup>7</sup>

There has been a staggering increase in interest in the symbiotic relationship between disinformation and social media communications. This has been both driven by and reflected in the outputs of a large number of think tanks, journalists and government agencies.<sup>8</sup> Understandably, the majority of this work has been focused upon threats to democratic processes and systems, given recent evidence of attempts to subvert these using a variety of informational methods and techniques. In contrast, the current research explores the distribution and public impact of soft facts in a different security context.

Framed in this way, the report is structured around the following sections:

### **SOCIAL REACTIONS AND SOCIAL MEDIA**

begins by contextualising the concepts and themes outlined above. This involves briefly summarising what is known about the contemporary information environment, and patterns of reaction to terror events.

**RESEARCH DESIGN AND METHOD** discusses the project’s research design and methods, detailing how the empirical data were collected and analysed.

**FOUR ATTACKS IN 2017** provides a brief overview of the circumstances surrounding the four terror attacks that are centred by the conceptual focus.

**A CONCEPTUAL MODEL OF INFLUENCE** sets out a high level theoretical model of digital influence engineering communications, informed by the analysis that has been completed.

**TECHNIQUES OF DISINFORMATION** contains an empirically led discussion of a number of key episodes from across the four events that are used to define eight ‘techniques of disinformation’.

**CONCLUSION** reprises the key findings and seeks to comprehend their implications for policy and practice, as well as future research.

6 *Couldry, N. and Hepp, A. (2016) The Mediated Construction of Reality. Cambridge: Polity Press.*

7 *Kahneman, D. (2012) Thinking Fast and Slow. London: Allen Lane.*

8 *Kakutani M. (2018), The Death of Truth. London: Harper Collins, 2018; Kavanagh, J. and Rich, M. (2018) Truth Decay. Santa Monica, Ca.: RAND Corporation.*

### 3. SOCIAL REACTIONS AND SOCIAL MEDIA

In a speech delivered shortly after the January 2015 terrorist attacks in Paris upon the staff of *Charlie Hebdo* magazine, the Director General of the UK Security Service cautioned it was almost inevitable that there would be future successful attacks on British soil.<sup>9</sup> It was, he elaborated, impossible for the police and security agencies to prevent all of the plots and attempts that are being brought forward. Unfortunately, his remarks proved prescient as four deadly attacks were carried out in London and Manchester in the first half of 2017.

An intriguing aspect implicitly highlighted by these remarks is the relative neglect, in both policy development and the terrorism studies literature, of what happens in the aftermath of terror attacks.<sup>10</sup> Given that terror attacks are designed by their orchestrators to ‘terrorise, polarise and mobilise’ segments of their public audiences, this constitutes a significant gap in terms of the comprehensiveness of our approach. If, as the Director General suggests, future attacks are almost inevitable, there would seem to be considerable public value in understanding what happens following attacks of this kind, in order to better manage any community impacts and consequences.

Over the past decade, there has been a significant uplift in the quantity of research on nearly all facets of terrorism, emanating from a diverse range of disciplines.<sup>11</sup> The vast majority of these studies have been concerned with issues of prediction, pre-emption and prevention, especially in respect of individuals and groups considered likely to engage in terrorist activities. This balance neglects a more

general tendency in research on social reactions to crime. In his case study account of the public impact of the 1991 assault of Rodney King by Los Angeles Police Department officers, Jacobs (1996) made two important generalizable points in respect of the study of social reactions to crime. First, he noted a general failure to attend to the impact of specific and defined events with any rigor. Second, he posited that there was a tendency to portray public reactions in an overly homogenized fashion, neglecting the extent to which differently situated segments of a population can interpret the same event very differently. In part these are methodological artefacts, reflecting the kinds of empirical materials typically available to researchers in such circumstances, typically derived from public opinion polls, or more focused studies utilizing qualitative methods.

Summarising what is known about public reactions to terrorism derived from these more established social research methodologies, Smelser (2007) highlights a tendency for intense but relatively short-lived impacts, comprising: psychic numbing, involving a combination of disbelief, denial and suppression of affect; immediately followed by intense emotions of fear, anxiety, terror, rage and guilt; a surge in solidarity and scapegoating actions; and outpourings of sympathy.<sup>12</sup>

Analysing reactions to the 9/11 terror attacks, Nacos, Block-Elkon & Shapiro (2011) contend that prevalence and distribution of these responses is structured by demographic characteristics, especially gender and race.<sup>13</sup> Moreover, they suggest that, in terms of how such responses get translated into political and social problems, the impacts and consequences can be longer lasting than perhaps implied by Smelser. Coherent with this line of reasoning, Oksanen et al.’s (2018) analysis of the impacts of the November 2015 Paris terror attacks suggests that post-event fear ‘travelled’, with increases detected in Spain, Finland, Norway and the United States, as well as France.<sup>14</sup> Along with the findings of several other studies, they further identified

9 Andrew Parker, ‘Terrorism, Technology and Accountability’, 2015, <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html> [accessed 21/10/18]

10 Martin Innes, Helen Innes, and Diyana Dobrova, *From Minutes to Months: A Rapid Evidence Assessment of the Impact of Media and Social Media During and After Terror Events*, 2018.

11 Richard English, *Does Terrorism Work? A History*. (Oxford: Oxford University Press, 2016).

12 Neil Smelser, *The Faces of Terrorism: Social and Psychological Dimensions* (Princeton, NJ: Princeton University Press, 2007).

13 Brigitte L. Nacos, Yaeli Block-Elkon, and Robert Y. Shapiro, *Selling fear: Counterterrorism, the media and public opinion* (Chicago: University of Chicago Press, 2011).

14 Atte Oksanen, Markus Kaakinen, Jaana Minkinen, Pekka Räsänen, Bernard Enjolras and Kari Steen-Johnsen, ‘Perceived societal fear and cyberhate after the November 2015 Paris terrorist attacks,’ *Terrorism and Political violence*, (2018), 1–20, doi: 10.1080/09546553.2018.1442329.

increases in rates of hate crime (see also Roberts et al., 2018; Williams & Burnap, 2016).<sup>15</sup>

However, more recently and innovatively, a number of authors have sought to overcome the limitations associated with these kinds of methods and data, by utilizing instead the streaming qualities of social media to derive new kinds of empirical material for social research.<sup>16</sup> Reflecting such developments, several recent studies have been published based upon analyses of social media data to provide ‘high resolution’ accounts of what happens in the wake of terror attacks. Of particular interest are a cluster of studies pivoting around the terrorist murder of Fusilier Lee Rigby in London in 2013.

The most detailed and comprehensive analysis of the incident is found in the Intelligence Select Committee's enquiry into the actions of the police and Security Services prior to the killing (ISC 2014).<sup>17</sup> However, prior to this, an early independent analysis was provided by the think tank Demos who analysed 20,000 Twitter messages to the Metropolitan Police Service. The conclusion drawn was that police need to develop an enhanced social media intelligence capacity and capability.<sup>18</sup> Williams and Burnap (2015) similarly employed quantitative techniques to locate instances of ‘cyber-hate’.<sup>19</sup> A more qualitative assessment underpinned McEnery et al.’s (2015) tracking of how information travels across social media and mass media networks.<sup>20</sup> Innes et al. (2016) used social media data to conceptualise patterns of collective reaction around 10 key behaviours.<sup>21</sup> Whereas Roberts et al. (2018) attended to the ‘conflict dynamics’ enacted by different ideological groupings.<sup>22</sup>

Building upon these kinds of developments Innes et al. (2018) proposed a ‘minutes to months framework’,

<sup>23</sup> describing a sequence of temporal phases following an attack, defined by particular communicative actions performed by a range of actors. The framework was informed by a rapid assessment methodology summarising and linking contemporary research on how media and social media functions during and after terror attacks. These were summarised as follows:

- **Minutes:** There are key actions and behaviours observed immediately following an event that can be highly influential in terms of what happens subsequently. Since rapid communications are transmitted during a period of confusion and uncertainty about what precisely has transpired, these actions can often involve the transmission of misinformation.
- **Hours:** As public awareness of the event increases, an ‘information explosion’ can occur via mainstream and social media. During this period official confirmation of the event typically coexists with more speculative soft facts.
- **Days:** As time passes, so does some of the initial confusion and informational ‘fog’. A phase of ‘collective sense-making’ develops and a public definition of the situation tends to be established. During this time frame, a surge in solidarity may be offset, to some degree, by rising social tensions.
- **Weeks:** The first few days following an incident tend to be frantic and fragmented. Over the following weeks however, the tenor and tempo of media and social media commentary tends to adjust, with more reflective and critical reactions to the event being reported, along with developments or outcomes in the police investigation.
- **Months:** The agenda-setting role of the media leads to the specifics of the event being

15 Colin Roberts, Martin Innes, Alun Preece, David Rogers, ‘After Woolwich: analysing open source communications to understand the interactive and multi polar dynamics of the arc of conflict.’ *British Journal of Criminology*, 58, no. 2, (2018), 434–54; Matthew 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*, 56, 2 (2018), 211–38.

16 See for example Sandra Gonzalez-Bailon, *Decoding the social world* (Cambridge, Ma.: MIT Press, 2017). Matthew Salganik, *Bit By Bit: Social Research in the Digital Age* (New Jersey: Princeton University Press, 2017);

17 Intelligence and Security Committee of Parliament, *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (2014), <http://bit.ly/2B-wRT7S> [accessed 21/10/18]

18 Jamie Bartlett and Carl Miller, *@metpolice uk: How Twitter is Changing Modern Policing* (London: Demos, 2013).

19 Williams and Burnap, *Cyberhate on social media*, 211–38.

20 Tony McEnery, Mark McGlashan, and Robbie Love, ‘Press and social media reaction to ideologically inspired murder: the case of Lee Rigby,’ *Discourse & Communication*, 9, n. 2 (2016), 237–259.

21 Martin Innes, Colin Roberts, Alun Preece, and David Rogers, (2016) ‘Ten “Rs” of social reaction: Using social media to analyse the “post-vent” impacts of the murder of Lee Rigby,’ *Terrorism and Political Violence*, 1–21, doi: 10.1080/09546553.2016.1180289

22 Colin Roberts, Martin Innes, Alun Preece, David Rogers, ‘After Woolwich: analysing open source communications to understand the interactive and multi polar dynamics of the arc of conflict,’ *British Journal of Criminology*, 58, 2 (2018), 434–54.

23 Innes, M. et al., *From Minutes to Months*.

absorbed into a wider narrative on terrorism and extremism. This can include political dimensions of response, public inquiries and new legislation, but also radicalising influences that may feed into subsequent terror plots.

The advantage of this framework is that it defines a common set of phases that can be applied to all terror attacks in order to track and trace how reactions to their specific situated details unfold and evolve. Thus enabling comparative analysis of similarities and differences.

## 4. RESEARCH DESIGN AND METHOD

To inform the analysis, a total of just over 30 million data points were collated from across multiple social media platforms utilising the Sentinel platform. Sentinel comprises a suite of data collection and analysis algorithms with similar collection and processing functionality to many commercial packages.<sup>24</sup> However, whereas these data are ‘black boxed’,<sup>25</sup> Sentinel is designed as a ‘glass box’. This allows for higher transparency in the data collection process and enables researchers to shape and adjust the desired data flows. Sentinel’s data collection is organised around a series of channels comprising up to 400 search terms, that are configured in real time by the researchers to filter in the relevant material and capture units of social media traffic that, because of their linguistic content, are likely to be connected to the subject of interest. The results of this real time ‘steering’ can be further

enriched and adjusted by ‘slower time’ procedures once the initial intensity of the unfolding event has declined. This structure enables the system to work within the 1% limit of total traffic volumes that Twitter make freely available through the streaming API.

For the purposes of this study, the data collection was built around a series of search terms relating to the terror attacks. *Figure 1* below provides a sense of the relative volumes of data collected in relation to each of the four attacks that are the focus of this analysis. It is clear that a far greater scale of reaction on social media was generated by the Manchester Arena bombing.

The subsequent data analysis was driven by the project’s conceptual interest in the role of soft facts and digital behaviour influencing techniques in altering the ways in which the public thinks, feels and behaves in the aftermath of terrorism and in relation to various informational stimuli.

Data reduction was performed to filter the 30 million data points into a number of smaller datasets focused on specific cases involving soft facts. This was achieved through the identification of a series of ‘episodes’ that

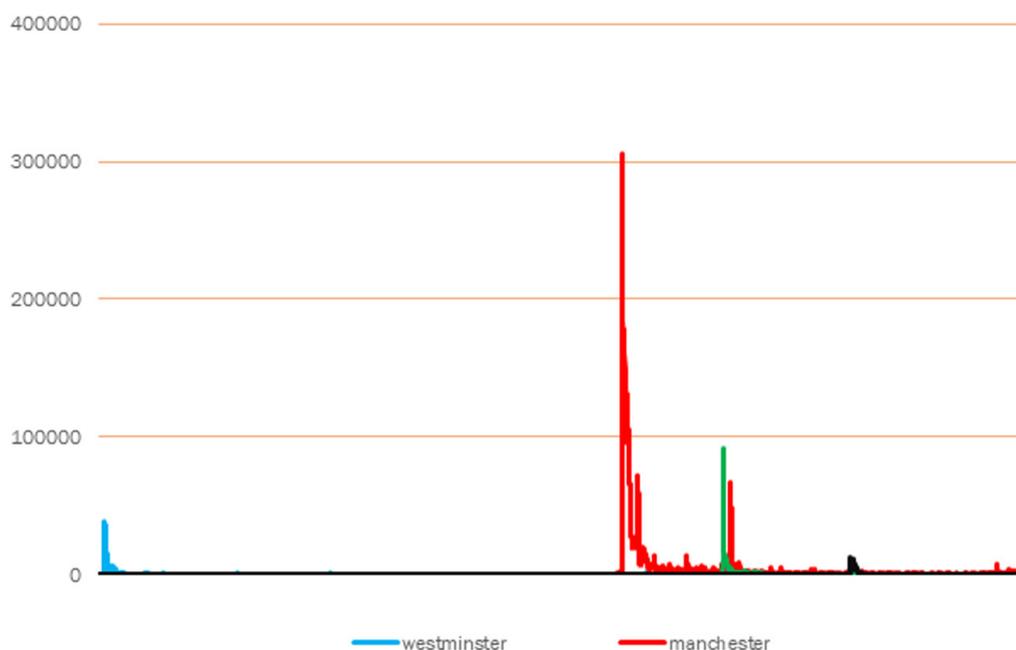


Figure 1: Volume of Social Media Data Collected by Attack

<sup>24</sup> Alun Preece, Irena Spasić, Kieran Evans, David Rogers, William Webberley, Colin Roberts, and Martin Innes, (2018). ‘Sentinel: A codesigned platform for semantic enrichment of social media streams,’ 118 *IEEE Transactions on Computational Social Systems*, 5, 1 (2018), 118–131. doi: 10.1109/TCSS.2017.2763684

<sup>25</sup> Frank Pasquale, *The black box society*. (Cambridge: Harvard University Press, 2015). Ben Popken, *Twitter deleted 200,000 Russian troll tweets*. Read them here. *NBC News*, February, 2018, <https://www.nbcnews.com/tech/social-media/now-available-more-200-000-deleted-russian-troll-tweets-n844731> [accessed 21/10/18]

appeared especially interesting and relevant. Episodes were selected and decided upon by the team during and after the collection process. Some of them were selected in real time (at the time when a particular rumour was circulating) and noted in a digital workspace, and others were discovered during the data exploration phase. Episodes can be understood as defined events within the larger narrative that can be isolated and studied intensively to draw out wider learning in terms of what happens and why. In this sense, clear analogies can be made with the principles of Manning's 'pattern elaborative theory'.<sup>26</sup> Manning suggests that, by engaging in interplay between 'exemplary evidence' and key theoretical precepts, it is possible to discern regularities and patterns in behaviour and conduct not previously recognised or perceived. These can in turn be subject to subsequent, more systematic, empirical testing.

These data-reduction procedures resulted in the identification of a total of 22 episodes involving the communication of one or more soft facts across the four attacks. Fifteen episodes were subsequently developed into detailed case studies as they displayed both sufficient outreach (considerable social media traction) and evidence for behavioural, cognitive and affective effects on the public. The data associated with each of the 15 episodes were subject to qualitative analysis, including of text and imagery as appropriate.

In the process of comparing the results of these analyses, some patterns were distilled. These articulate some key ways in which soft facts are used as part of digital influence engineering designed to modify the perceptions and behaviour of audience members.

Broadly speaking, the approach adopted to the collection and analysis of the empirical data can be cast as a form of digital behavioural analytics. In his analysis of how internet technologies have impacted political communication and democratic processes, Dahlgren identified three main analytic modes adopted by researchers:<sup>27</sup>

**Structural analyses** typically utilise social network analytic methodologies or other big data approaches to capture and articulate the aggregate flows of social communications.

**Representational accounts** are concerned with the contents of what is being communicated. These will typically attend to documenting narratives, rhetoric and other linguistic devices, as well as assessing the emotions that are conveyed.

**Interactional** dimensions are situated somewhere between the other two approaches. This mode is interested in the behaviour of accounts and their users, and the ways in which they seek to engage with other platform users and a wider audience.

The greatest volume of work pivots around the application of network analysis methodologies and quantitative data, mapping the nodes and links that are activated to disseminate disinformation.<sup>28</sup> A second grouping of studies displays traits analogous with Dahlgren's construct of the representational dimension and are concerned with how certain visual and linguistic grammars structure the information and meanings communicated. Located between these two levels is a more interactional focus attending to the behaviours used in transmitting and receiving disinformation communications. It is this kind of mid-range theory that has the most affinity with the approach adopted for this report. The focus upon how certain forms of information are used to explicitly try and steer the behaviour, perceptions and feelings of audience members.

26 Philip Manning, *Goffman and empirical research*. *Symbolic Interaction*, 39, 1 (2016), 143–52. doi: 10.1002/SYMB.220

27 Peter Dahlgren, *The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation*, *Political Communication*, 22, 2 (2005), 147–162, DOI: 10.1080/10584600590933160

28 Daniel Centola, *How Behaviour Spreads: The Science of Complex Contagions*. (New Jersey: Princeton University Press, 2005); Sandra Gonzalez-Bailon, *Decoding the social world* (Cambridge, Ma.: MIT Press, 2017).

## 5. FOUR ATTACKS IN 2017

In the course of only four months (March – June 2017) the UK was subject to four terrorist attacks which killed 41 people (including five of the six attackers) and injured nearly 200. These attacks constituted the deadliest terror attacks on British soil since the 7/7 London bombings.<sup>29</sup>

The impact of the first three attacks was amplified by the fact that they came at a time when there were other high-profile Islamist terrorist attacks in other European countries (France, Belgium and Germany).

### 5.1 WESTMINSTER

Khalid Masood's assault on Parliament started at 2.40pm on 22 March 2017. He drove a Hyundai Tuscon SUV (rented in Birmingham the day before) at speed across Westminster Bridge in the direction of the Palace of Westminster. The vehicle mounted the pavement twice, colliding with crowds of pedestrians (mostly tourists), after which it crashed into the east perimeter gates of the Palace of Westminster. Masood then took two carving knives out of the vehicle and fatally stabbed PC Keith Palmer while he was on duty outside the Houses of Parliament. Masood was then shot by the close protection team of Defence Secretary Michael Fallon, who happened to be leaving Parliament at the same time. The entire incident lasted approximately 82 seconds.<sup>30</sup> Six people died including the assailant and 29 others were injured.

Even though Masood had featured in prior counter-terrorism investigations, there is little evidence to suggest that he was subject to any external direction, or was part of any network. He reportedly sent a WhatsApp message shortly before his attack, stating that his attack was a response to the Western interventions in the Middle East. However, the person to whom the message was sent has been cleared of culpability by authorities. The claiming of responsibility by the Islamic State in

the aftermath of the attack was also dismissed as there was no evidence to support the claim. Islamic State has praised Masood in subsequent publications, including specific incitement for people to follow his example, but the group has never demonstrated possession of information pertaining to Masood that was not already in the public domain.

### 5.2 MANCHESTER ARENA

On the night of 22 May 2017 Salman Abedi exploded a bomb comprising TATP and shrapnel at the end of an Ariana Grande music concert at Manchester Arena. 22 people were killed, 10 of whom were aged under 20 and the youngest was 8. 116 people were injured and treated in hospital. The attacker also died in the explosion.

In the aftermath of the attack the national terrorism threat level was raised by the Joint Terrorist Analysis Centre (JTAC) to its highest level. 20 arrests were made in the following days but no charges were issued. Greater Manchester Police highlighted publicly that even though Abedi may not have acted alone, he was not part of a bigger network.

Abedi was reported to have had significant connections to radical circles in Manchester. Many of Abedi's links tie back to the community of young men going to fight in Syria (e.g. Abdal Raouf Abdallah who is another Libyan-British national jailed for his role in facilitating the travel of others to Syria; and Raphael Hostey, a prominent British Islamic State fighter) from nearby in Manchester. In addition, Abedi's father, Ramadan Abedi, was a prominent member of the now-defunct Libyan Islamic Fighting Group (LIFG) and was well-connected in the community around the jihadi group. It was also revealed that Salman, together with his brother, both left for Libya on 15 April, with Salman returning to the United Kingdom on 18 May, just four days before the bombing.

However, Greater Manchester Police stated:

*"We don't have evidence of a large network. We do, however, suspect others were either aware [of] or complicit in the knowledge of*

<sup>29</sup> Raffaello Pantucci, *Britain on Alert: The Attacks in London and Manchester and the Evolving Threat*, CTC Sentinel, 10, 7 (2017), 1-8.

<sup>30</sup> *The Westminster Bridge terrorist attack: a report on the use of terrorism legislation*. Independent Reviewer of Terrorism Legislation, March 28, 2018.

URL: <https://terrorismlegislationreviewer.independent.gov.uk/operation-classific/>

*this attack ... We do believe that there are other people potentially involved in this ... further arrests are possible,” (Detective Chief Superintendent Russ Jackson, Head of the North-West Counter Terrorism Unit).*

Similar to Masood’s attack, the Islamic State issued a statement praising Abedi’s act, but it demonstrated no proof of any prior knowledge. Notwithstanding the confessions made by his brother (Hashem Abedi), that he and Salman were members of the Islamic State and that Hashem had been in the UK during the planning phase of the attack, there is no evidence to support the claim – no recorded martyrdom video left with the group, and no photographic evidence showing a connection. At the same time, investigators continue to believe that he had some greater degree of links to terrorist groups, albeit the exact nature of these remains unclear.

### 5.3 LONDON BRIDGE

On 3 June 2017, three attackers (Khuram Butt, Youssef Zaghba and Richard Redouane), drove a van into a crowd of people near London Bridge. After ramming the van into a fence adjacent to the pavement near the end of the bridge, the attackers left the van wearing dummy suicide vests (plastic bottles covered in black tape wrapped around their bodies) and armed with large knives, which they used on an apparently random basis to kill six more people near Borough Market and in the vicinity of Borough High Street. Armed police arrived within eight minutes of receiving the emergency call and shot them dead.

Khuram Butt was a live SOI (Subject of Interest) under active investigation at the time of his attack.<sup>31</sup> He was a prominent member of the al-Muhajiroun network of extremists that has been the centre of the UK’s violent Islamist terrorist threat for the past two decades. He had also been repeatedly subject to investigations and even featured in a widely viewed documentary ‘The Jihadis Next Door’ which followed a number of prominent al-Muhajiroun members. The other two attackers were less well known to British investigators. However, it

was revealed that Zaghba had been previously flagged to British authorities through a European intelligence sharing system as someone of concern to Italian authorities

### 5.4 FINSBURY PARK

The final case study that features in this report concerns the vehicle-based attack on a crowd of worshippers who had just exited Finsbury Park Mosque on the night of 19 June 2017. The attacker drove a Citroen Relay van (hired in South Wales some days previously) into a crowd of worshippers outside Finsbury Park Islamic Centre in London. Makram Ali was struck by the vehicle and died soon afterwards. 10 other people were treated for injuries.

Subsequent background investigations of the assailant revealed that 47-year-old Darren Osborne had a “dysfunctional” background and history of violence, having served two years in prison for assault and suffered from depression, and alcohol and drug abuse.<sup>32</sup> In the immediate aftermath of the attack, police officers found various items in the van, including a hand-written note from Osborne containing a monologue of his extremist views. An investigation was immediately launched by the Metropolitan Police’s Counter Terrorism Command and Osborne was charged four days later on 23 June 2017. Police analysis of Osborne’s electronic devices showed an increasing interest in far-right material in the weeks leading up to his attack. His internet search history shows he viewed content from the English Defence League, Britain First, Tommy Robinson, Jayda Fransen, Paul Golding, and InfoWars.

It was identified in *Figure 1* that the volume of social reaction generated by these four attacks differed markedly. The Manchester Arena attack triggered far greater levels of communication than the other three, and the Finsbury Park incident the least. The line of reasoning being that not all attacks are the same in terms of their capacity to leverage public concern and reaction. This can be elaborated by looking at other indicators of impact. One such is levels of reported hate crime. In *Figure 2* are depicted the levels of hate crime

<sup>31</sup> David Anderson Q.C., *Attacks in London and Manchester: Independent Assessment of MI5 and Police Internal Reviews*, 2017. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/664682/Attacks\\_in\\_London\\_and\\_Manchester\\_Open\\_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf) [accessed 21/10/18]

<sup>32</sup> Lizzie Dearden, 2018, *Darren Osborne: how Finsbury Park terror attack became ‘obsessed’ with Muslims in less than a month*, *The Independent*, 2 February, Available at: <https://www.independent.co.uk/news/uk/crime/darren-osborne-finsbury-park-attack-who-is-tommy-robinson-muslim-internet-britain-first-a8190316.html> [accessed 21/10/18]

## FOUR ATTACKS IN 2017

### SOFT FACTS AND DIGITAL BEHAVIOURAL INFLUENCING AFTER THE 2017 TERROR ATTACKS

for England and Wales for the three weeks following each of the attacks, compared with the same period the previous year.

Introducing these data as an indicator of the kinds of secondary impacts attributable to terror events suggests some intriguing empirical properties:

- Not all terror events generate the same patterns of responses, at least as measured by recorded hate crimes. In the case of the Westminster attack there was a period of escalation followed by decline. Whereas for Manchester Arena and London Bridge there was a rapid spike in offending, pursued by a period of tailing off.
- That there was no aggregate increase in hate crime following the Finsbury Park incident potentially suggests that the perceived identity and motive of the attacker is important in shaping any responses.
- Most saliently given the interests of this report, there is a loosely coupled association between the volumes of social media communication in *Figure 1* and rates of hate crime. The incident seeing the most reaction online (Manchester) also triggered the greatest number of hate crimes, whilst the

Finsbury Park attack generated little response either in terms of secondary violence or on social media.

Of course, there is insufficient data available to this study to validate such claims and robustly test their reliability. It is also the case that we are dealing with an unusual sequence of events, with four incidents happening in rapid succession to each other. That said, these may be fruitful development opportunities for future research.



Figure 2: Percentage change in hate crimes in England and Wales following the 2017 terror attacks compared with the same period in 2016. Source: Authors' own compilation from National Police Chief's Council Data.

## 6. A CONCEPTUAL MODEL OF INFLUENCE

As was outlined in the preceding sections, in analysing some of the social media communications data emanating from the social reactions to these four attack events, the principal interest of this report is in understanding how and why a range of soft facts influenced the ways the events were publicly defined and understood. This requires an overarching theoretical model of disinformation communication able to encompass and disinter the specific methods that are used to construct and convey soft fact materials.

Informed by the empirical data and patterns of communication behaviour observed across the four post-event attack situations, *Figure 3* has been designed to represent some key features of how a variety of soft

facts are deployed and achieve traction. The bell curve line depicts the distribution of public opinion, with mainstream values and views depicted by the largest section in the centre. The blue arrow represents the mainstream audience to which most orthodox strategic communications interventions are targeted to. However, our data shows that soft facts are more often directed to seek to influence segments of the audience that diverge from the mainstream in their views, opinions, and behaviour.

There are a number of key features of this schematic that are worth highlighting:

- Soft facts tend to gain traction at the more extreme ends of the spectrum of public opinion.
- In so doing, they tend to amplify pre-existing concerns and prejudices within established interest groups and thought communities. People are content to consume soft facts that support their already established values and inclinations, while actively rejecting others.

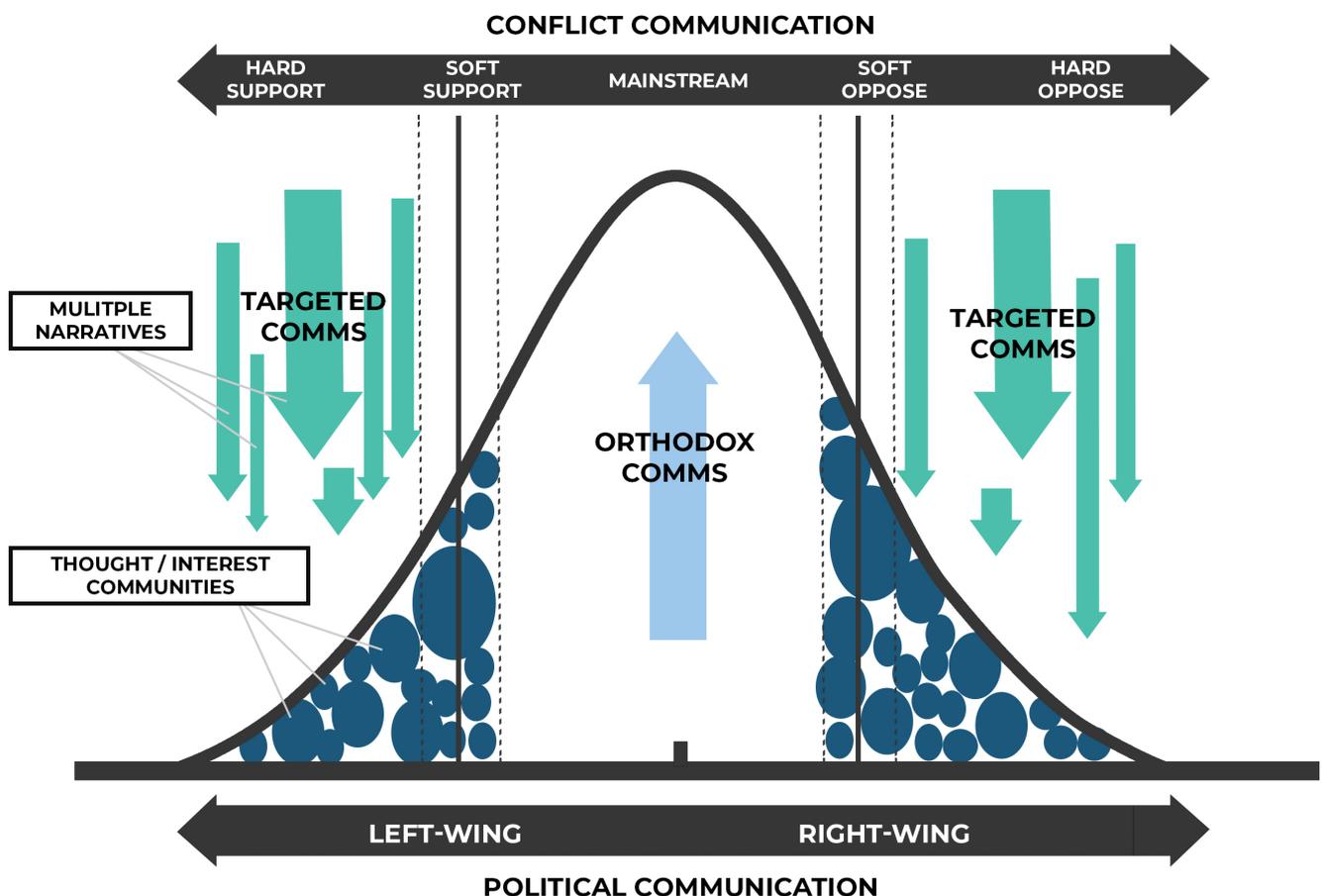


Figure 3: A Conceptual Model of Soft Fact Communication

## A CONCEPTUAL MODEL OF INFLUENCE

### SOFT FACTS AND DIGITAL BEHAVIOURAL INFLUENCING AFTER THE 2017 TERROR ATTACKS

- As depicted in the dark blue ‘bubbles’ at either end of the opinion spectrum, it is misleading to think of these as cohesive groups. Rather, these comprise diverse constellations of values and groupings that possess family resemblances, but for whom small differences are often quite important.
- Certainly, in post-attack situations there tends to be multiple soft facts of different kinds (as illustrated by the multiple green arrows) each of which will play to specific audience segments.
- Importantly, in terms of the dynamics of social reaction, it is frequently the case that soft facts that elicit a response at one end of the ideological spectrum will also generate a counter-response or ‘reactance’ amongst members of groups positioned at the opposite end of ideological spectrum.

The key tenets of this conceptual modelling apply equally well to contemporary political contests as they do to conflict situations. This is visualised by the two arrow bars at the top and bottom of *Figure 3*. The top one attends to conflict communications; the key focus of this analysis. Whereas the bottom horizontal arrow displays how the modelling applies to more standard political communications.

In summary, this model and its component parts provides a framing device for discussing some of the specific ways that soft facts are constructed and used to influence particular audience segments.

## 7. TECHNIQUES OF DISINFORMATION

Consistent with the tenets of a digital behavioural analytics method, and framed by the theoretical model of communicative influence outlined in the preceding section, we now move on to the processes of how soft facts are constructed and communicated, and how they influence people's understandings, perceptions and values. In so doing, we define eight 'techniques of disinformation'. The adoption of this label contains a direct allusion to the work of Sykes and Matza (1957) and their 'techniques of neutralization'.<sup>33</sup> These were designed to capture how people engaging in deviant conduct loosen the moral constraints they are subject to in ways that do not taint their sense of social and self-identity. Of course, in a social environment suffused with social media communications, the ways people build and sustain their social status and reputations has changed significantly. As such, there is a considerable degree of crossover between the social dynamics described by the authors over 50 years ago and the eight techniques of influence described below. Moreover, there is a similar imperative in terms of understanding how misinformation and disinformation work.



Figure 4: Disinformation Tweet from Manchester Arena

### 7.1 SEEDING

Looking across the empirical data collected on the four attacks, in tandem with previous studies, it seems that information that circulates on social and mainstream media in the immediate wake of a terror event are often inaccurate and misleading. This is not always intentional, resulting instead from a 'media logic' that privileges speed of communication over accuracy and validation.<sup>34</sup> Thus constituting misinformation rather than disinformation. The key analytic point to be made is however, in 'seeding doubt' about what has actually transpired, misinformation creates the conditions for the communication of more deliberately framed disinformation.

During the early reactions to the Manchester attack, there were multiple instances of doubt 'seeding'. For instance, soon after the initial reports began circulating, pictures from the scene were being attached to Twitter messages and posts to Facebook. However, several response messages were then sent claiming the images were a hoax, and related to a police training exercise at the Manchester Arena earlier that year:

*If you see people sharing this image re Manchester it's already been debunked as being from a training exercise video*

Source: Twitter, 22 May 2018; 23:39; retweets 240

Relatedly, Andre Walker (a New York Observer Columnist), posted the image and text in *Figure 4*, receiving 282 retweets and 364 'likes'. Several other users adopted similar lines doubting that an explosion had occurred.

More detailed images from the scene quickly followed. This led many previous 'doubters' to revise their positions, but not all did. In the days and weeks following the attack, messages from a relatively small number of users continued claiming that it was an elaborately staged deception. More generally, the use of visual images to try and validate claims to veracity is an important element of how digital persuasion is being performed (see section on 'truthing' on page 27).

33 Gresham M. Sykes and David Matza, 'Techniques of Neutralization: A Theory of Delinquency,' *American Sociological Review*, 22, 6 (1957), 664-670.  
34 David L. Altheide, *Terrorism and the politics of fear* (Lanham, MD: AltaMira Press, 2006).

A second episode further illuminates the blending together of these key themes of uncertainty and misinformation, and how they create a space in which disinforming communication can acquire traction. It involves the misidentification of Abu Izzadeen as a suspect for the Westminster attack.

The rumour about the relatively high profile Islamist preacher Izzadeen first appeared via an unverified Twitter account ‘News Executive’, which was positioned as an online source for breaking news stories:

*BREAKING UPDATE: Reports name the Westminster terrorist suspect as hate preacher Abu Izzadeen (Trevor Brooks) from Clapton in Hackney*

Source: Twitter; @News\_Executive; 22 March 2017; 17:59.

Ultimately this message triggered a chain of events that caused a wider section of the public to doubt the integrity and credibility of a number of key institutions, including the police and media.

Subsequent Twitter and Facebook communications would use images of the suspect at the scene, alongside a media photo of Izzadeen, to highlight the admitted visual similarities between the individuals concerned. However, approximately two and six minutes later, two foreign news outlets – *La Stampa* (Italian) and *Dreuz* (French), also named Abu Izzadeen as the attacker. Intriguingly, from a disinformation perspective, both articles were modified the following day to claim that Channel 4 and other British mainstream media were responsible for misidentifying the Westminster terrorist, effectively attributing the ‘fake news’ to other sources. Fourteen minutes after News Executive’s message, Abu Izzadeen’s Wikipedia page was edited to claim that he was responsible for the Westminster terrorist attack. Wikipedia provides an audit trail for all previous editions and changes, revealing Izzadeen’s Wikipedia page was edited 84 times on the day of the attack.

Channel 4 News commenced their evening television broadcast at 7pm with the main presenter, on location at Westminster, naming Izzadeen as a suspect. Thirteen minutes later, Rym Momtaz (an ABC producer) tweeted

that she had contacted Izzadeen’s solicitor who had confirmed Izzadeen was still serving a prison sentence for breaching an anti-terror order and could not have been the attacker. About 20 minutes after Channel 4 News, two UK-based news outlets – *The Independent* and *IBTimes* – published two online articles reporting Abu Izzadeen as the attacker. Similarly to *La Stampa* and *Dreuz*, both UK articles were subsequently amended (or deleted). Despite this, their previous stories and approximate time of posting can still be discerned through detailed analysis of Twitter.

About 35 minutes into the one-hour programme, Channel 4 News’s Senior Home Affairs Correspondent, Simon Israel, started to voice doubt about the information he had previously provided on air: “Yes, I appeared quite certain earlier in the programme, but there appears to be some doubt now.” At 7.54pm (the end of the programme), the presenter revealed that Channel 4 News had been contacted by Izzadeen’s brother stating he is still in prison, confirming the accuracy of Momtaz’s information. At about 8.50pm, both Simon Israel and Ben de Pear (Channel 4 News Editor) tweeted apologies for the mistake on the basis that ‘this was a fast-moving story’ where conflicting information was coming to light:

*The source I trusted, but ultimately I made a mistake. This time got it wrong. Abu Izzadeen is in prison.*

Source: Twitter; Simon Israel; 22 March 2017; 20:50

Despite this full retraction, the soft fact claiming that Izzadeen was involved continued to circulate on social media for several days afterwards. In particular, it was shared and retweeted in high volumes by senior figures in the far-right Britain First group, and by prominent alt-right accounts in the United States, and their affiliates. In terms of its usage by these other groups, it provided an opportunity to engage in ‘emulsification’, blending the current crisis event with a wider set of issues they wanted to promote. (See section on ‘*emulsification*’ on page 24.)

This episode served to empirically evidence three important notions:

- First, is the symbiotic relationship between social and mainstream media in the construction and communication of misinformation. This research negates the idea that the communication of rumours and conspiracies is a particular pathology of social media platforms.
- Second is the retroactive altering of history by mainstream media outlets who sought to edit discrediting information from their timelines. By concealing previous communication they have themselves engaged in disinformation.
- More broadly, the empirical detail of this case study conveys the messy, contingent and complex nature of disinformation as an ‘artefact’, subject to multiple edits, rewrites and revisions as it travels through the media ecosystem.

The key point about ‘seeding doubt’ as a technique of disinformation is that it is not designed to convince members of the audience to believe a particular interpretation or set of facts. Rather, it is about persuading and influencing people so that they do not know which information sources to trust and what to believe.

---

## 7.2 DENIAL OF CREDIBILITY

In their original five techniques of neutralization, Sykes and Matza framed three as involving acts of denial (denial of responsibility, injury, and of the existence of victims).<sup>35</sup> Their perspective was an explicit influence upon Cohen’s (2005) work on the politics of denial, where he distinguished between its literal, interpretive and implicatory forms. In the context of disinformation, one particular form of denial was detected in the aftermath of four terror attacks. ‘Denial of credibility’ involves attacking the source of a piece of information using different techniques that are analogous to those discussed by Sykes and Matza.

Examining the empirical social media data tracking reactions to each of the four attacks, it was revealed that in each case there were a small number of accounts claiming, for different reasons, that it was a hoax. Typically, these accounts engaged in detailed dissections of particular aspects of the incident to

attack the credibility of those involved in the event, and of the media institutions colluding in the conspiracy by reporting the events.

Oftentimes this could be quite grotesque. For instance, following the Westminster attack a picture was circulated across multiple social media platforms of a victim’s body lying under a red London bus, with the head obscured and the legs protruding from under the wheels. The force of the collision and weight of the vehicle, made the corpse look akin to a mannequin, with comments such as the following accompanying the picture: “The person is not injured or run over. It’s just for shock effect, nothing else, meant to manipulate public consciousness”. Thus in this instance, a denial of credibility was being used against ‘the evidence’ that other social media users were sharing (possibly not in the best taste) to confirm what was happening.

More often, attempts to deny credibility were directed towards individuals and/or institutions. Following the Westminster Bridge attack, Mark Rowley (national lead for Counter Terrorism Policing and Acting Deputy Commissioner for the Metropolitan Police), made two statements informing the public about what had happened and developments in the police investigation. In his evening press conference, he stated:

*[...] we must recognise now that our Muslim communities will feel anxious at this time given the past behaviour of the extreme right wing and we will continue to work with all community leaders in the coming days.*

This comment, highlighting a potential for extreme right-wing violence, which constituted a small fraction of an otherwise lengthy, informative and reassuring statement, was significant. It was the first time such a pre-emptive statement had been made by police in this manner, reflecting learning gleaned from previous terror attacks.<sup>36</sup> It also triggered intense and aggressive negative reactions from supporters of far-right ideologies. These reactions escalated into the construction and dissemination of a meme, shared and reposted extensively by several high profile far-right groups and personalities, for example Tommy Robinson and the British National Party. It contained Rowley’s image on the left, an extract of his ‘far-right

---

<sup>35</sup> Sykes and Matza, *Techniques of Neutralization*, 664-670.

<sup>36</sup> Innes, M. et al., *Ten ‘Rs’ of social reaction*, 1-21.

concerns' quote on the right, and an alternative 'truth claim' at the bottom:

*No mention of the concerns of the English community feeling anxious concerning Muslim terrorism and prime example of the liberalism that is killing England.*

The clear suggestion being that the police and other 'elite' groups in society do not understand the concerns of 'ordinary' people. Other variants of this included:

*Typical liberal nonsense! How about the British community's [sic] under threat from Islamic terrorists? Stop appeasing and start acting.*

**Source: Twitter; 24 March 2017; 12:24; retweets 132.**

*Fuck them and fuck you Mr Rowley! What about us ..... THE BRITS? The people you promised to protect and serve!!*

**Source: Twitter; 24 March 2017; 09:44; retweet 0**

Albeit, adopting slightly different vectors of attack, collectively these kinds of reactions were intended to try and disrupt the authority and credibility of Rowley as a credible messenger. In so doing, they utilised several verbal formulations analogous to Sykes and Matza's methods of neutralization, including 'denying the victim', 'condemning the condemners' and 'appealing to higher loyalties'.

It is not clear how much impact was achieved by these kinds of attempts to undermine the credibility of figures like an Assistant Police Commissioner. More generally however, their very presence signals some of the ways that high intensity and intemperate rhetoric are used to underpin disinformation and thus shape the tenor and tone of online interactions around contentious issues. It is suspected that such processes help to suppress alternative narratives and viewpoints being introduced into the digital conversations, as some users do not want to engage in a conflictual situation

For the purposes of the present article and reflecting its particular interests, herein we cast 'denial of credibility' as a 'master concept', comprising several specific techniques of disinformation. What binds these together is that they are all directed towards attacking and undermining the perceived validity and reliability of sources of communication that are disputed. As with some other techniques described here, they will not succeed in influencing large segments of the audience, but they do influence the views of some.

### 7.3 EVENT GHOSTING

'Event ghosting' involves manufacturing/inventing aspects of an event that did not really happen. By inserting these invented details into a wider narrative to augment it, the meaning is 'turned' or changed in some way. It is an important technique of disinformation as these illusory 'digital apparitions' can exert considerable influence upon public understandings of the wider event, and can continue to do so even after having been debunked.

One particular episode following the Manchester Arena attack exemplifies several key features of event ghosting as a mode of communicating soft facts. It concerns the activities of a woman who, after the attack, claimed to have taken a number of children separated from their parents to a local hotel, where she was keeping them safe.

At the time, and for a period afterwards, this story was communicated widely on the main social media channels, including a contact number for worried parents to phone. It was also picked up by a number of press and broadcast media outlets who publicized it further. The main protagonist was a real person and she publicized her genuine mobile telephone number on the night of the attack. However, she did not shelter any unaccompanied children in a hotel. It never happened.

Whilst it is difficult to remotely define the individual's motives and intents, it is possible to identify the presence of a series of influencing techniques used to construct a persuasive and plausible narrative that could be widely shared.

At around 12.30am four messages were posted in quick succession on the individual's personal Facebook page:

*Bomb gone off Manchester git loads with kids with us please pass on we taking them to premier inn bomb at Victoria station.*

**Source: Facebook; 23 May 2017; 00:30 approximate time.**

In the emotionally charged post-terror environment these messages generated a huge response from the public who quickly and rapidly shared Facebook screenshots on Twitter. There was a spike in Twitter traffic around this time concerned with missing children (see Figure 5).

*#Manchester There are over 60 children without guardians at Holiday Inn if you're missing or can't get hold a loved one ring 07896711298 RT.*

**Source: Twitter; 23 May 2017; 00:21; retweets 17.6K**

As indicated above, even though late at night, in less than two hours, the above message had been retweeted over 17,500 times. This pattern of behaviour captures some of the 'fuzzy' boundaries that exist between misinformation and disinformation in online environments, and hence why adopting a concept such as 'soft fact' might be preferable.

For what can be observed in this particular episode is how the originator of the message was engaged in disinformation communication, however, the thousands of people that shared and reposted her message were doing so mistakenly believing it was genuine.

Their misinformation communications significantly amplified the reach of the disinformation. Other case studies reported herein, demonstrate that this coupling can sometimes be reversed with misinformation creating an environment conducive to disinformation.

One reason for these high levels of online mobilization may be that it helped onlookers online to feel they were making a positive contribution when confronted with a quite horrific scenario in Manchester. But also, by placing herself at the scene, the woman claimed 'epistemic authority' and appeared to be engaging in

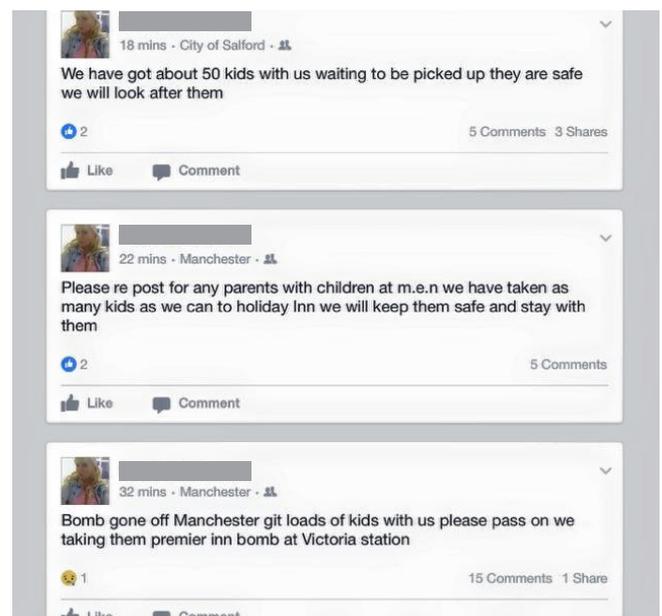


Figure 5: Series of Posts to Facebook

important pro-social action (looking after lost children) in the absence of any specific official advice. This was supported by her back story that positioned her as a mother and grandmother herself.

Within an hour of posting to Facebook, the social media audience were lauding her with praise and calling for her to be rewarded for her actions:

*Can we give praise to this lady "[xxxx]" who is looking after missing children, when evil strikes the people hit back #Manchester*

Source: Twitter; 23 May 2017; 00:43

She was labelled the ‘Angel of Manchester’, an identity that the *Daily Mail* newspaper used in an article seven months later about her being deserving of a nomination for New Year Honours list.<sup>37</sup> This was even though none of it happened; it was an invented story.

The Holiday Inn issued a statement the following morning at 9.19am confirming they did not have any missing children at the hotel. A police statement later that afternoon (3.49pm) reiterated ‘we DO NOT believe there are any accompanied children in any of the hotels in Manchester because of the explosion last night’. The woman was interviewed by the BBC Newsnight programme the following day where she recounted her narrative of events<sup>38</sup> and looked visibly shaken when talking about the hundreds of calls and pictures sent to her phone from worried parents saying, ‘it’s got mistaken that I’m the helpline’. She was not the only individual to ‘ghost’ false missing children appeals. In the dataset, 28 separate claims of this kind that were subsequently debunked, were identified following the Manchester Arena attack.

A different instance of event ghosting was identified immediately following the explosion in Manchester. It involved a Facebook post claiming that there was a gunman outside Oldham hospital. The message was imbued with urgency, written in capital letters and instructing people to avoid the area:

*DO NOT COME OLDHAM HOSPITAL IM CURRENTLY LOCKED INSIDE...MAN OUTSIDE WITH GUN.*

We do not have an exact time for the original post, but we do have the screenshot of a message the author sent to a friend at 12.22am. This initial post was retweeted by at least 368 Twitter accounts, many of which used a screen grab of the Facebook post referred to above presenting it as a form of proof or evidence. At 12.50am, Oldham Council tweeted saying they have no information that there is a gunman at the hospital. However, this communication did not dispel the rumour as new messages about ‘the gunman’ continued to be sent for over half an hour after this rebuttal.

This episode is especially important in demonstrating how disinformation communications can have serious and consequential effects. In the aftermath of the bombing, wracked with uncertainty about what was actually happening, the messages circulating on social media that there may be still attackers active in the area, caused a decision to be taken to keep the ambulances and fire crews at the outer scene cordon for their own protection. This meant that they were not able to get to the victims near the bomb site who were critically injured and administer first aid.

These two examples used to illuminate the essence of event ghosting as a technique of disinformation were particularly explicit and egregious. A number of other more subtle and nuanced examples were present in the dataset, in terms of specific soft fact occurrences and details being inserted and/or manipulated. The purpose being to alter the wider understandings of and meaning attributed to the event in question.

## 7.4 EMULSIFYING

Emulsifying involves blending two distinct sets of ingredients together to create a new concoction. In terms of disinformation communication this technique can be utilized to accomplish two ends: (1) to connect a current crisis event to wider issues or previous occurrences, thereby wrapping them into a broader narrative of

37 Rory Tingle, *Anger as heroes of Grenfell Tower fire, Manchester Arena bombing and London Bridge terror attack are snubbed in New Year honours list amid cronyism row as Theresa May hands out TWO FIFTHS of gongs to fellow MPs, 2017*, <http://www.dailymail.co.uk/news/article-5222091/Heroes-Grenfell-Tower-miss-New-Year-honours.html>

38 In this narrative, the lady talks about two children and shouting out to other children, with no mention of the ‘50 children’ in her message that she said she would ‘look after’.

grievance; and (2) complexifying the overall picture so that it is harder for public audiences to comprehend the causes and consequences of problematic and troubling events.

In the aftermath of terror attacks, there is now an almost ritualized quality to some of the key statements that are made. In the hours after the violence, police will tend to issue quite factual statements to update the public. Political leaders also perceive a need to communicate with the public, pivoting around a set of tropes promoting social resilience – ‘we will not give in to terror’. Looking across the four attacks we can observe how these kinds of political communications can become engaged in processes of emulsification.

Following the well-rehearsed rhythms alluded to above, the Mayor of London, Sadiq Khan, issued a public statement after the Westminster attack:

*My statement on the incident near Parliament Square this afternoon. Please visit <http://news.met.police.uk> for the latest information. [attached link]<sup>39</sup>*

**Source: Twitter; 22 March 2017; retweets 2566; likes 2653; comments 668**

Several thousand people ‘liked’ the post, but almost all of the 668 comments were highly negative, and many aggressive. There is an important difference between the ‘low energy’ action of ‘liking’ a message and the ‘high energy’ required to compose and write down your opinion, making comments highly important empirical data.

After each of the series of attacks that took place in 2017, the Mayor issued not dissimilar messages. One widely cited message, stating that terror attacks are ‘part and parcel of living in a major city,’ triggered heated opprobrium. Notably, event President Donald Trump reflected on this:

*At least 7 dead and 48 wounded in terror attack and Mayor of London says there is "no reason to be alarmed!"*

**Source: Twitter; 22 March 2017; retweets 2566; likes 2653; comments 668**

Following on from which, a small series of social media campaigns were observed that sought to connect the series of terror attacks with a range of other social problems, especially immigration and refugee numbers. This pattern persisted, for example, when the Grenfell Tower tragedy happened in 2017. Several messages questioned whether this was also ‘part and parcel’ of living in a global city, thereby linking terrorism to other failures of social policy.

It is hard to be definitive about how emulsification works at this stage based upon the data available, and it may be that it is contextually sensitive. One plausible hypothesis is that by intertwining different subjects and narratives, the cognitive load placed upon audience members to follow the complexities of what is actually going on is increased, such that many are just rendered confused about how to infer causes and consequences for what has happened. Alternatively, it may be that merging separate events establishes an archetype that induces people to infer that they are of a ‘kind’, such that a common set of causes and consequences can be imputed. This latter model involves reducing the

INCIDENT	NUMBER OF ORIGINAL MESSAGES FROM IRA ACCOUNTS	NUMBER OF REPOSTS
Westminster	35	35662
Manchester	293	55581
London Bridge	140	57322
Finsbury Park	7	4871

Table 1: Summary of Internet Research Agency Messages by Incident

cognitive load through processes of simplification, by stripping out layers of context and detail.<sup>40</sup>

## 7.5 INFILTRATING AND INCITING

Political and public discussions of disinformation over the past two years have pivoted, to a significant degree, around the involvement of actors connected to the Kremlin and the Russian State. Multiple politicians, think tanks and investigative journalists have documented activities deliberately intended to disrupt democratic processes and institutions.<sup>41</sup> Related to which, the head of the UK's new National Cyber Security Centre has also publicly stated that attacks have been committed against elements of the UK's critical national infrastructure, including utility companies and financial institutions. Whilst processing the data on the four terror attacks, the team detected a number of the Russian-linked social media accounts, previously identified by Russian journalists and the US Senate, seeking to amplify the impacts of terrorist violence.

In total, 47 accounts connected with the St Petersburg based Internet Research Agency (IRA) were identified in the current dataset. Eight of these accounts were especially active, posting at least 475 Twitter messages across the four attacks, which were reposted in excess of 153,000 times (see Table 1):

Following the Manchester and London Bridge attacks, at least one IRA account was sending inflammatory messages within 15 minutes:

*Another day, another Muslim terrorist attack. RETWEET if you think that Islam needs to be banned RIGHT NOW! Manches...*

Source Twitter; 22 May 2017, 22:22

From an account presenting with a right-wing, anti-Islam stance, this one message sent within an hour

of the Manchester attack, was retweeted 3,606 times. Responding rapidly to 'frame' the definition of the situation in this manner acts to subtly shape how and what some people think. There is an 'early mover advantage' to be accrued from getting in at the inception of an incident to try and sow seeds of antagonism and anxiety. The Russian-linked accounts, whose primary purpose we surmise was to communicate disinformation, were organized around a twin-track strategy of infiltrating established online thought communities on both ends of the ideological spectrum, and then seeking to incite and inflame their emotions, to make their views a bit more extreme.

## 7.6 SPOOFING

From the evidence available, it is clear that the infiltrate and incite strategy engages several more tactical techniques of disinformation. The first of these we label 'spoofing' appropriating Mackenzie's (2018) term for attempts to 'trick' algorithms in high frequency financial trading markets to leverage competitive advantage and profit.<sup>42</sup> Albeit focussed on machines



Figure 6: Spoofed Internet Research Agency Profile

<sup>40</sup> Tali Sharot, *The Influential Mind* (New York: Little Brown, 2017).

<sup>41</sup> See for example: US Senate Intelligence Committee, *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*, 2018, <https://democrats-intelligence.house.gov/social-media-content/> [accessed 02/10/18]; Digital, Culture, Media and Sport Select Committee, 'Disinformation and Fake News: Interim Report' (London: HMSO, 2018).

<sup>42</sup> Donald MacKenzie, 'Material signals: A historical sociology of high frequency trading,' *American Journal of Sociology*, 123, 6 (2018), 1635–83.

rather than humans, aspects of his analysis are redolent of Goffman's detailed dissections of how people, in their co-present encounters and interactions with each other, seek to deceive, misrepresent or mask aspects of their identities and/or motives.<sup>43</sup>

Spoofing as a technique of disinformation steers attention to the ways the operators of fake accounts are able to construct false digital identities. They employ these to ingratiate themselves within a digital community of individuals, seemingly possessing similar identity characteristics and/or interests to the wider group. Part of how this is done involves clear analogies with what Goffman termed 'identity kits', or the props and materials we use to symbolically display and represent a particular form of social status and positioning.<sup>44</sup>

For example, a number of the Russian-linked accounts were constructed around avowedly politically right-wing, Southern state, President Trump supporting, presentations of self. The avatars selected to accompany these accounts were stereotypical depictions of this, featuring white males sporting Stetson hats (*see Figure 6*).

@SouthLoneStar was active in communicating around a number of the episodes that have been discussed previously. For instance, in respect of the misidentification of the suspect for the Westminster attack, the account tweeted:

*UPDATE: London terrorist identified as Islamic cleric Abu Izzadeen who was sentenced to jail in January for hate p... <https://t.co/Zw9uNpzB7H>*

**Source: Twitter; retweets 833**

A critical feature of the infiltrate and incite strategy in general, and its deployment of identity spoofing as a specific tactic, was that the Russian-linked accounts adopted a range of different personas, positioned across the ideological spectrum. This included, for example, spoofing members of the Black Lives Matter movement.

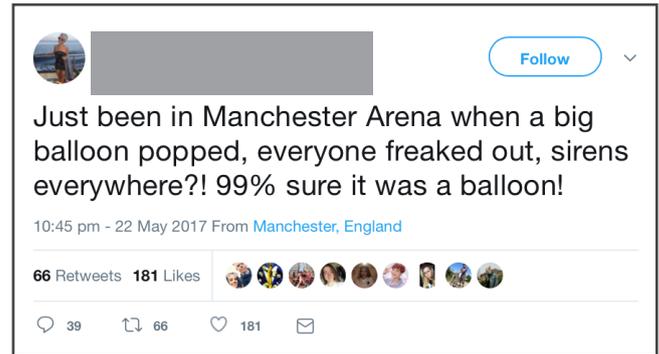


Figure 7: Misinformation from Manchester Arena

The quality of mimicry and imitation was often quite convincing, allowing the operators to build up thousands of followers in some cases. This meant that around contentious and highly charged social and political issues, these accounts were interfering in and influencing the views of multiple different digital thought communities simultaneously.

## 7.7 TRUTHING

The performance of spoofed digital identities is frequently accompanied by two other techniques of disinformation: truthing and social proofing. A key feature of several of the exemplars of the techniques of disinformation detailed above has been the use of visual images by messengers to try and persuade their audiences about the ultimate 'truth' of the claims they are seeking to mount. Photographs and videos possess an almost inherent particular persuasive potency, albeit there is increasing awareness of how these too can be manipulated and faked. Another form of truthing involves presenting an argument in highly detailed and technical language, that deliberately imitates the aura of digital forensics and crime investigation. A third variant, concerns the illegitimate manipulation of statistical data.

Perhaps the most common manifestation of truthing as a technique of disinformation though, derives from people claiming and being attributed 'epistemic authority' by virtue of them being at the scene, when they were not. Epistemic authority involves being seen as the possessor of credible and validated knowledge. The message reproduced in *Figure 7* exemplifies this.

43 Erving Goffman, *Interaction ritual: Essays in face to face behaviour* (New York, NY: Pantheon, 1967). Erving Goffman, 'The interaction order,' *American Sociological Review*, 48, 1 (1983), 1–17. doi: 10.2307/2095141

44 Goffman, *Asylums*.

This individual sought to debunk some of the other messages circulating at this point in time, which were suggesting that a bomb had exploded at Manchester Arena. As can be observed, the author of this tweet sought to validate her interpretation by reference to her 'being in Manchester'. Unfortunately, in so doing this individual was involved in spreading misinformation. In and of themselves, such misinforming messages are of limited consequence, as they tend to be corrected by other communications that rapidly provide more accurate situational awareness. However, they are pertinent to understanding the dynamics of digital disinformation because of how they tend to be latched onto by other users with more conspiratorial viewpoints. Such messages that provide alternative interpretations of what has happened are frequently co-opted and drawn upon by thought communities that seek to derive more deeply conspiratorial narratives.

When conspiratorial interpretations are communicated they are regularly accompanied by phrases asserting that what is captured is a hidden truth about what has really occurred. Something that has been masked by surface appearances. What is striking about a number of the case studies considered above, and especially those involving Russian-linked actors, is how there can be multiple narratives about what has happened in circulation simultaneously. Each of which is using different materials and interpretations of these materials to buttress their apparent validity and reliability.

## 7.8 SOCIAL PROOFING

In their study of political mobilization, Margetts et al. (2016) evidence how the number of followers and 'likes' that attach themselves to particular messages and users, influences how others interact with those materials.<sup>45</sup> This can be labelled 'social proofing', in that it seeks to exploit a cognitive bias in terms of individual attention being shaped of the actions by other members of a social group.<sup>46</sup>

To illustrate the workings of social proofing we will draw upon a rather different empirical example from after the London Bridge attack. It is especially pertinent because of how it also illuminates the ways

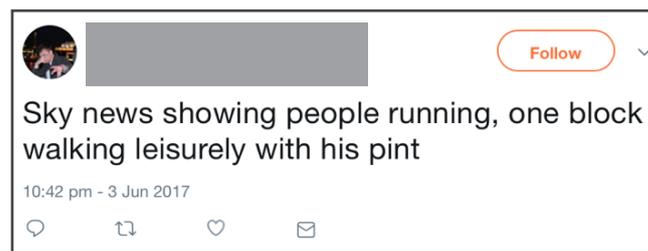


Figure 8: Triggering the Interest in 'Pint Man'

social media can play a role in fostering community resilience, as well as amplifying the sense of harm and risk, in the post-attack window.

As an episode it commenced when, amid the chaos that ensued in the aftermath of the London Bridge attack, the image of a man running whilst holding a pint of beer was broadcast on live TV. Several eagle-eyed viewers picked up on this and shortly after the footage aired, tweets began appearing. One single tweet received over 110k 'likes'. Responding to the reaction on social media, mainstream media outlets picked up on the story, sharing reports via their own websites and social media pages. One such Facebook post received over 200,000 reactions and 12,000 comments.

This scale of reaction cascaded over time, with social media users responding to the communicative actions



Figure 9: Example of Reaction to the 'Pint Man' Meme

<sup>45</sup> Helen Margetts, Peter John, Scott Hale, and Taha Yasseri, *Political turbulence: How social media shape collective action* (Princeton: Princeton University Press, 2016).

<sup>46</sup> Robert B. Cialdini, *Influence: Science and practice* (New York: William Morrow, 2009).

of others. Although it is difficult to identify precisely how this process started, we think it originated with the message in *Figure 8*.

The original image was broadcast at around 10.42pm on *Sky News*. By around an hour later a large number of messages were being shared and reposted including the image of the man, and these were generating a large number of reactions from other users. For example, the message in *Figure 9* was retweeted in excess of 37,600 times and received 117,000+ 'likes'.

Among the most popular posts was an article by *LADbible* which received 207,893 reactions, 33,987 shares, and 12,083 comments. Other popular media articles included the *HuffPost* (13,182 reactions, 1,361 shares, 470 comments), *The Guardian* (10,630 reactions, 1,740 shares, 252 comments) and *Business Insider* (6,073 reactions, 2,811 shares, 653 comments). Driven by individual users collectively reacting to the initial story, but equally by the behaviour of people in their networks, 'pint man' became a meme. The original image was shared repeatedly, with variants of it and a range of textual accompaniments used to convey a variety of meanings. It worked as a visual symbol of resilience and Britishness – even in an emergency, you don't leave or spill your pint of beer.

Evidence from social psychology strongly suggests that individual behaviour can be strongly influenced by those around us. In terms of the 'pint man' meme, and other memes identified in the dataset, these processes of reaction were in part driven by users being able to observe others from their social networks engaging with particular stories and subplots. In the process this draws others in to participate in similar ways, facilitated by some of the affordances and logics designed into social media technologies.

Memes emerge as powerful mechanisms of communication in terms of enabling both hard and soft facts to spread and travel. As indicated by the figures for the volumes of shares and likes in the 'pint man' example, mimetic forms of messaging can engage large numbers of people. The 'pint man' case was deliberately selected because of how it exemplifies these social proofing dynamics, whereby the reactions of social media users are shaped by the actions of others in their network. It is also useful in conveying some of the complexities associated with processes of social reaction in the aftermath of terror events.

For although most of the empirical examples cited in the preceding sections, and indeed in the dataset as a whole, are concerned with how social media is involved in amplifying the sense of risk and threat, not all such messaging is so inclined. There are communicative actions that function, in some sense, to manage and mitigate the sense of public harm induced by the violence.

Creating an illusion of social support for a viewpoint or idea, in order that this might persuade others to take it on, also provides some insight into how and why bots can be deployed as part of a disinformation campaign. As automated forms of algorithmically driven communication, bots can be used to artificially amplify the visibility of a message in the expectation that increased exposure will cause more people to align with it. Albeit, the empirical validity of such a supposition is not established.

## 8. CONCLUSION

The main aim of this report has been to document and describe how and why misinformation and disinformation arises in the aftermaths of terror attacks, and the consequences it has for the harms induced by such events. As such it makes a contribution both to our understandings of how disinformation operates, and to knowledge about processes of social reaction to terrorism. Set against a backdrop of increasing public and political consternation about the ways social media platforms are being engaged in undermining democratic institutions, values and processes, adopting this specific focus has generated several significant insights:

- It has refined the concept of soft fact in such a way as to draw together a range of informational forms with family resemblances to each other, where previously they have tended to be treated separately. This is important given the dynamics of the contemporary information environment where rumours, conspiracy theories and propaganda of various kinds overlap and are interspersed with each other, seemingly creating the conditions for each other to thrive.
- Empirically, the analysis suggests that the minutes, hours and days following an attack are especially susceptible to being shaped by soft facts, given the emotional intensity of much communication during these periods and the high degrees of uncertainty about what has actually happened.
- An important and unanticipated finding from the research was the detection of Russian-linked media and social media assets, operating to amplify the harms of the four attacks under study. The analysis highlighted how these accounts, infiltrated established online thought communities, seeking to incite their affiliates by posting provocative and emotionally charged messages. Identification of this geopolitical dimension has important implications for the future management of strategic communications following terror events.
- Arguably the key contribution of the report is in distilling and delineating the eight ‘techniques

of disinformation’ to illuminate some of the key methods via which soft facts are constructed and communicated in a post-attack situation. Future work could enhance and extend the usefulness of these concepts by attending to their representational and rhetorical construction.

Taken together, the evidence and insights related to these contributions provide the key components for a digital behavioural analytics that can be applied to the task of understanding the operations of digital influence engineering. The latter concept is concerned with understanding how features of specific messages and the wider information environment are being designed with the intent that they should both overtly and covertly shape the thoughts, feelings and actions of different audience segments. Elements of the analysis have also documented how new collective participatory communicative actions, such as memes, can perform as important instruments of influence at moments of crisis and emergency.

An ancillary contribution of the study is in pointing towards how comparative case study research designs could be utilised in developing the research agenda on social reactions to terrorism. Although there has been a recent growth in the number of studies attending to the aftermath of terror events, these have been predicated upon case studies of individual incidents. In contrast to which, the approach adopted herein, starts to outline the benefits derivable from conducting systematic comparisons across multiple events. For what this affords is an ability to see patterns, in terms of recurring features that are common to all such situations and settings. Thus providing the basis for more nuanced and sophisticated policy and practice development.

The implications for policy and practice are twofold. The findings speak to the specific and focused requirements associated with the post-event management of terror attacks. But in addition, they are also relevant to the growing public and political consternation about the corrosive effects of a ‘post-truth’ social order.<sup>47</sup> In relation to the former of these concerns, there has been a general neglect of the post-attack window at the expense of preventative efforts designed to impede and interdict the onset of processes of violent radicalisation. What the evidence and insights reported above do is

<sup>47</sup> Michiko Kakutani, *The Death of Truth* (London: Harper Collins, 2018); Kavanagh, J. and Rich, M. (2018) *Truth Decay*. Santa Monica, Ca.: RAND Corporation.

set out how, within the post-attack situation soft facts can be highly influential, often amplifying the harm induced by the original violence. Rumours, conspiracy theories and propaganda do this by shaping public interpretations and understandings of the causes and consequences of the incident.

Equally important however, is to elucidate how the kinds of techniques of disinformation distilled by the analysis, and their involvement in the conduct of digital influence engineering, are also present across a range of other situations and settings. In effect, by conducting a focused empirical study of how misinforming and disinforming communications are engaged in shaping public reactions to a specific species of social problem, it is possible to illuminate features of the contemporary information environment that are of wider relevance and applicability.

Cast in such terms, it appears that devising strategies and tactics for managing and mitigating the deployment of soft facts as part of digital influence engineering campaigns is likely to become an increasingly important consideration for all those involved in managing security risks and threats. Albeit it was not the principal focus of this work, as part of the scanning and assessment work conducted, there are indicators that disinformation campaigns are becoming more mainstream, featuring as part of the reaction processes for a variety of different security events. As such, the techniques of disinformation that are the principal finding of this analysis are an increasingly important and influential feature of how contemporary social reality is being ordered and organised.

## READ MORE

This is the full report from the *Soft Facts And Digital Behavioural Influencing* project, funded by CREST.

An Executive Summary of this report can be found at [crestresearch.ac.uk/resources/soft-facts-summary](http://crestresearch.ac.uk/resources/soft-facts-summary)



A Policy Brief is also available from this project, which details how the systematic use of fake social media accounts, linked to Russia, amplifies the public impact of four terrorist attacks that took place in the UK in 2017.

You can download, read and share the four-page brief at [crestresearch.ac.uk/resources/russian-influence-uk-terrorist-attacks/](http://crestresearch.ac.uk/resources/russian-influence-uk-terrorist-attacks/)



For further reading on this topic, see Martin Innes' article *Russian Influence And Interference On Twitter Following The 2017 UK Terrorist Attacks* in *CREST Security Review*, Issue 7: Transitions.

To see all CREST outputs from this project go to [crestresearch.ac.uk/projects/soft-facts-digital-behavioural-influencing/](http://crestresearch.ac.uk/projects/soft-facts-digital-behavioural-influencing/)

For more information on CREST  
and other CREST resources, visit  
[www.crestresearch.ac.uk](http://www.crestresearch.ac.uk)



CREST

CENTRE FOR RESEARCH AND  
EVIDENCE ON SECURITY THREATS