

MARTIN INNES

# RUSSIAN INFLUENCE AND INTERFERENCE ON TWITTER FOLLOWING THE 2017 UK TERROR ATTACKS

Following the UK terror attacks in 2017, there was a significant level of influence and interference by Russian-linked social media accounts, trying to engineer division in the UK.

This was the finding from a CREST-funded report by researchers at the Cardiff University Crime and Security Research Institute. As part of our project looking into soft facts and digital influencing, the team gathered data from across four terrorist attacks in 2017 (the Westminster, Manchester Arena, London Bridge and Finsbury Park attacks). We collected a dataset containing approximately 30 million datapoints from various social media platforms. Whilst processing these data, we detected some anomalies, which upon further investigation have been revealed to be associated with fake accounts.

By comparing these accounts with open-access datasets on Russian-linked accounts we were able to show that 47 accounts were Russian-linked. We also identified other accounts with similar identifying features, which had not at that time been confirmed to be Russian.

Terrorist violence is fundamentally designed to 'terrorise, mobilise and polarise' its audiences. The impacts of these events are increasingly shaped by social media, and reflect the speed and scale with which such platforms can make information

travel. With this in mind, our evidence suggests that a systematic strategic political communications campaign has been directed at the UK, designed to amplify the public harms of terrorist attacks.

Many of the accounts described themselves as 'breaking news' sites. Following the Manchester and London Bridge attacks, at least one account was sending inflammatory messages within 15 minutes. This is significant because, in influence terms, responding rapidly to 'frame' how an event should be defined is important in being able to subtly shape how and what people subsequently think about it. 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.

Eight out of the forty-seven accounts were especially active, posting at least 475 Twitter messages across the four attacks, which were reposted in excess of 153,000 times. Rather than generic news accounts, these accounts were based on personal, highly opinionated and ideologically driven identities. Messages from these accounts were reposted in excess of 153,000 times.

Some of these eight, personal, accounts had a large number of followers. To take three as an example: @TEN\_GOP (the right-wing, anti-Islam account mentioned above) had circa 127,000 followers on the 26 June 2017; @CrystalJonson (adopting a civil rights stance) had nearly 46,000 followers; and @SouthLoneStar (another with a right-wing stance) had almost 54,000.

What's also striking from just those examples, is the range of ideological standpoints these accounts took. The use of these accounts as 'sock puppets' allowed for interventions to be made on both sides of polarised debates, amplifying their message and ramping up the level of discord and disagreement within public online debate.

An example of these contrasting positions was in regard to the infamous image of a Muslim woman on Westminster Bridge walking past a victim being treated, apparently ignoring them. This became an internet meme propagated by multiple far-right groups and individuals, with about 7,000 variations of it according to our dataset. In response to which the far right aligned @Ten\_GOP tweeted: She is being judged for her own actions & lack of sympathy. Would you just walk by? Or offer help? Whereas, @CrystalJohnson's narrative was: so this is how a world with glasses of hate look like - poor woman, being judged only by her clothes.

While most attention around terror attacks is quite rightly focused on the planning, motivations and behaviours of terrorists, the downstream consequences have often been neglected. There is potential for better managing and mitigating the harms associated successful attacks.

The hostile intervention after the attacks we looked at suggests that we should focus upon rapidly establishing what counter-measures are effective in offsetting the impact of 'soft facts' propagated by overseas interests, as they seek to do the work of terrorist organisations by amplifying the capacity and capability of violent acts to mobilise and polarise citizens.

*Professor Martin Innes is Director of the Crime and Security Research Institute at Cardiff University. This research was funded via CREST as part of a project focused on how 'soft facts' (rumours / fake news / conspiracy theories / propaganda) influence the aftermath of terrorist attacks. For more information and to download the report this article is based on, visit the project page at <https://crestresearch.ac.uk/projects/soft-facts-digital-behavioural-influencing/>*