How Russia's Internet Research Agency Built its Disinformation Campaign

ANDREW DAWSON AND MARTIN INNES

Abstract
In this article we analyse features of the information influence operations run by the St. Petersburg based Internet Research Agency, targeted at Europe. Informed by publicly available 'open source' data, the analysis delineates three key tactics that underpinned their disinformation campaign: account buying; 'follower fishing'; and narrative switching. Both individually and collectively these were designed to build the reach, impact and influence of the ideologically loaded messages that social media account operators authored and amplified. The particular value of the analysis is that whilst a lot of recent public and political attention has focussed upon Kremlin backed disinformation in respect of the 2016 United States presidential election, far less work has addressed their European activities.

Keywords: disinformation, Russia, Kremlin influence, Internet Research Agency

WITH HINDSIGHT, the sheer scale and scope of activities performed by the St. Petersburg based Internet Research Agency (IRA) and allied Kremlin units attempting to influence and interfere with the 2016 US presidential election process, suggests much more could have been done to interdict their efforts. For as described by two recent studies commissioned by the US Senate Permanent Select Committee on Intelligence—from Oxford University and New Knowledge—and the indictments filed by Special Counsel Mueller, the Russian backed activities were extensive, diverse and pervaded all major social media platforms. That said, doubts remain about precisely what impact they accomplished. In their recent book *Network Propaganda*, the Harvard academics Yochai Benkler, Robert Faris and Hal Roberts have cautioned that digital influencing activity does not easily translate into measurable behaviour change.[1] Thus we need to be wary of over-attributing any causal effects to even the most sophisticated disinformation campaign.

Set against this backdrop, given that digital influence engineering is now being undertaken regularly and routinely, this article highlights three issues. First, the importance of developing a better understanding of how Russian state assets have sought to use disinformation and misinformation to influence European politics. For understandable reasons, much of the public conversation to-date has focussed upon the American situation. But there is significant evidence of similar influence and interference strategies being operationalised in Europe. Understanding this arena is especially timely, given that the European parliamentary elections are scheduled for May 2019.

Second, although the Senate commissioned studies did a commendable job in documenting and describing the volume and variety of Kremlin backed influence campaigning, the amount of material involved means there is more to do in terms of distilling the IRA's disinformation playbook. Detailed 'digital forensic' investigative methods are needed to craft an evidence-based understanding of how IRA operators built their audience and influence. This is on the grounds that identifying their key tactics and techniques may enable similar disinformation campaigns to be detected in other contexts.

Finally, we discuss some of the challenges with attributing authorship and impact to disinformation communications. This reflects how, not only have the US and its allies learned about some of the methods used to seed and amplify false and misleading information online, so too have those authoring such messages. Contemporary efforts at

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).
This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

communicating disinforming narratives are increasingly sophisticated, as those involved are learning 'what works' in making messages more persuasive and in masking their origins.

Two main data sources underpin the evidence and insights reported. First, there are a small number of published accounts and stories from former workers at the Internet Research Agency describing its organisation and routines. This is supplemented by analysis of the 'FiveThirtyEight Internet Research Agency Twitter dataset'—an extensive non-anonymised corpus of tweets posted by IRA accounts. As detailed below, this includes a large number of Russian language and American facing accounts. But there were also accounts messaging in a number of other languages. Herein we focus in particular on accounts that were oriented towards Germany, as much less attention has focussed upon what these were doing.

Work at the Internet Research Agency

There are at least seven published journalistic accounts, based upon interviews with former employees at the Internet Research Agency. Collectively, these provide insights into the nature of the work it performed, including the organisation of decision making and delivery, main roles and responsibilities, and the performance indicators workers were subject to. By collating and analysing these materials, it is possible to construct an outline picture of the organisational rhythms and routines that shaped the kinds of digital behaviours presenting in the social media accounts they were operating.

The picture painted is of an organisation based around an orthodox division of labour with different departments focussing upon specific geographic regions/countries, accompanied by some platform specialisation.[2] For example, one unit focussed upon producing memes, whilst another was tasked with commenting on posts by other users. Individual operators ran multiple fake accounts: trolls were expected to make around fifty comments on news articles every day. Or, they were tasked with maintaining six Facebook pages, posting three times daily about the news, and discussing new developments in groups on Facebook twice daily, with a target of at least 500 subscribers by the end of the first month. On Twitter, operators were generally responsible for around ten accounts with up to 2,000 followers each, tweeting at least fifty times daily.[3] One source suggests they were required to make 135 comments per twelve-hour shift, working in internet forums and that they would be provided with five keywords to feature in all posts to encourage search engine pickup.[4] The latter is consistent with workers describing receiving regular 'taskings' from their managers in terms of a list of subjects/topics to focus upon.[5] Similar tasks were defined in relation to targeting comments towards outlets such as CNN, BBC and the *New York Times*.[6]

One interviewee described working in teams of three: operator one would function as 'the villain' criticising the authorities; then the others would enter a debate with him/her. One would post an image/meme in support of their argument, the other posting a link to a supportive source.[7] Other intriguing comments include a suggested pattern for developing accounts in that they are started with a politically neutral stance, which is amended later.[8] Operators wrote Twitter bots to amplify visibility and because the costs of doing so were low.[9] A few operators were ideologically committed to their work, but most were not. Workforce turnover was high and featured a lot of young people and students.[10]

These organisational arrangements certainly help make sense of some of the patterns that can be observed in the messaging data. For example, sixteen confirmed Internet Research Agency accounts all used quotations from Orwell, Shakespeare and other famous literary figures as part of the account biography. Similarly, a second group of accounts all shared fragments of the same base image as the account profile picture. There is a strong probability that these were individuals engaging cognitive shortcuts to get the job done quickly. Given that the staff were under considerable pressure to meet their performance metrics and were not necessarily deeply invested in their work, these are precisely the kinds of 'easing behaviours' found in many organisational settings. Analogous to what happens in police detective work and psychological profiling, these little 'tells' and

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

behavioural signatures can be used as clues about where suspicions should be directed.

One especially salient point though is that these social media accounts that were used for spreading disinformation were not transmitting such materials all the time. Although there was quite considerable variation, broadly speaking they seemed to operate around an 80:20 ratio. That is, most of the time these accounts were engaged in mimicking the kinds of interests and values coherent with the social identities that they were 'spoofing', and then occasionally they would message avowedly political content. This pattern of behaviour was aided by the fact that many accounts would expend a lot of time 'amplifying' messages from other users, and then only rarely 'authoring' new material themselves. Such patterns are important as they render the task of definitively attributing accounts to Kremlin direction and control challenging.

How IRA accounts built audience and influence

Spoofing personas in terms of constructing a false account profile, and then messaging around issues of interest to the thought communities associated with such digital social identities, was critical to how IRA accounts built a following to enhance their persuasive capacity and capability. Many did so over several years, but not all did. Some tried to shortcut the process of building audience and influence.

Buying followers

An alternative to the normal organic strategy and long-term investment required to grow follower numbers, is to 'buy' a following. Websites such as 'buycheapfollowerslikes.org' offer to increase a client's Twitter following by 1,000 accounts for less than $20. According to reviews, the followers have profile pictures, unique bios and are active tweeters; however they will not interact with posts, as they are bots. This is what is depicted in Figure 1, which is an account run by the IRA that simply purchased follower accounts when set up. It is not clear whether such an action was performed as part of the overarching organisational strategy, or because a worker was 'gaming' the performance measures they were subject to. In the graph, a running total of tweets are plotted on the X axis and follower count on the Y axis. The dotted line represents its followers and the solid line those accounts it is following.

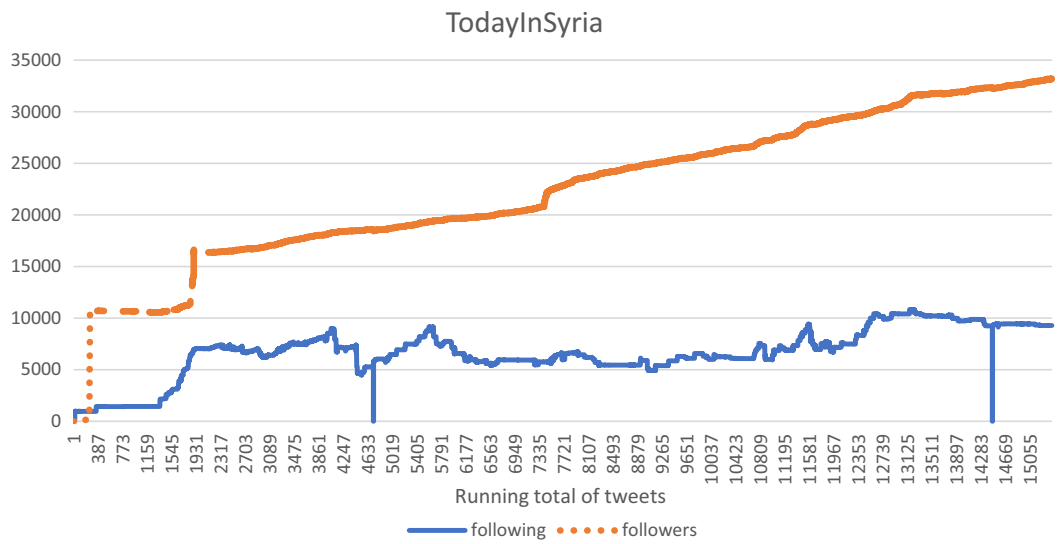

Figure 1: Example of an account purchasing followers

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

In this case, the English language account was initiated in 2015 by it acquiring 10,000 followers in a very short period of time. We have identified similar patterns of behaviour in several of the German language IRA accounts, as exemplified in Figure 2.

On 4 June 2016, this account very rapidly received 5,000 new followers. As can be seen at two later points on the graph, the follower count drops by around 1,000 accounts; this is likely due to the fake accounts being discovered and banned by Twitter. The number of followers is also unusually high: research suggests the average Twitter account has 453 followers.[11]

Follower fishing

A second pattern of behaviour designed to build audience and influence is 'follower fishing'. The logic of which is outlined by the metrics in Figure 3 below, based upon an English language account.

Around half of the most active IRA 'German' Twitter accounts engaged in prolific 'follower fishing', with thousands of accounts being followed and unfollowed regularly. The tactic works by the IRA accounts following hundreds or thousands of new accounts in a very short time frame. The aim is to get the newly added accounts to reciprocate by following the IRA account (follow-back). After a few days, the IRA operator then unfollows the accounts, increasing their 'followers per followed' ratio and with it boosting the account's implied 'authority', at least in terms of how this is assessed by platform algorithms. This tactic is commonly used by 'social media influencers', such as celebrities or marketers. Figure 4 tracks this pattern in relation to a German language account.

The solid line documents how this account followed other accounts over time. They added thousands of accounts in a very compressed time frame hoping to get 'follow-backs'. However, a high following to follower ratio indicates a low Twitter authority score, so they need frequently to stop following thousands of accounts as well. This creates a step like pattern of steep rises and sharp drops.

The longitudinal analysis to detect these kinds of behavioural patterns is time-consuming. But in an attempt to test how widespread it was, we analysed sixty-nine randomly selected IRA Twitter accounts, with different country focusses. Table 1 shows dramatic differences between the behaviour of accounts 'representing' different countries. For example, no Italian, but 86 per cent of the US accounts reviewed employed follower fishing to increase their followers and 21 per cent purchased followers.

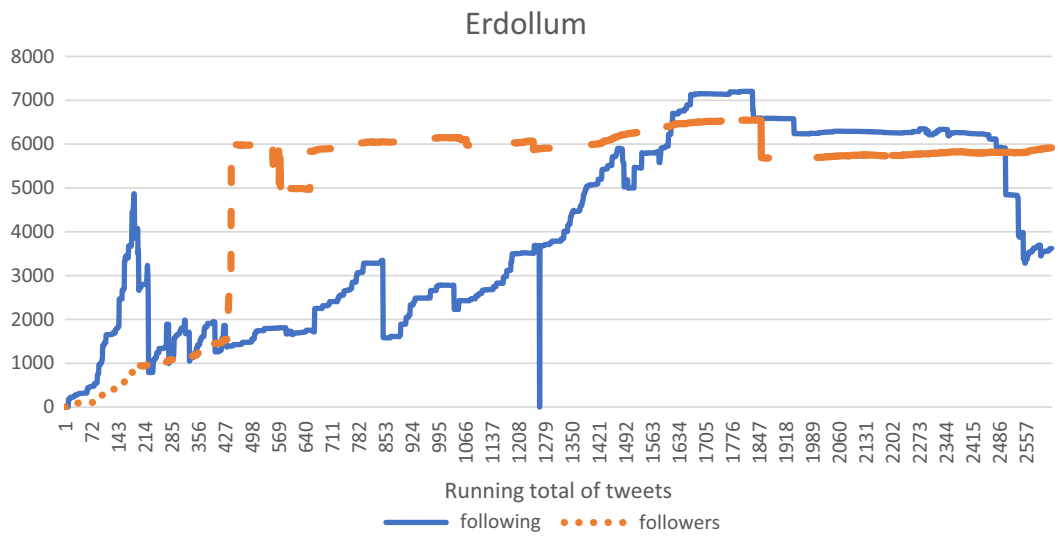

Figure 2: Example of a German account purchasing followers

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

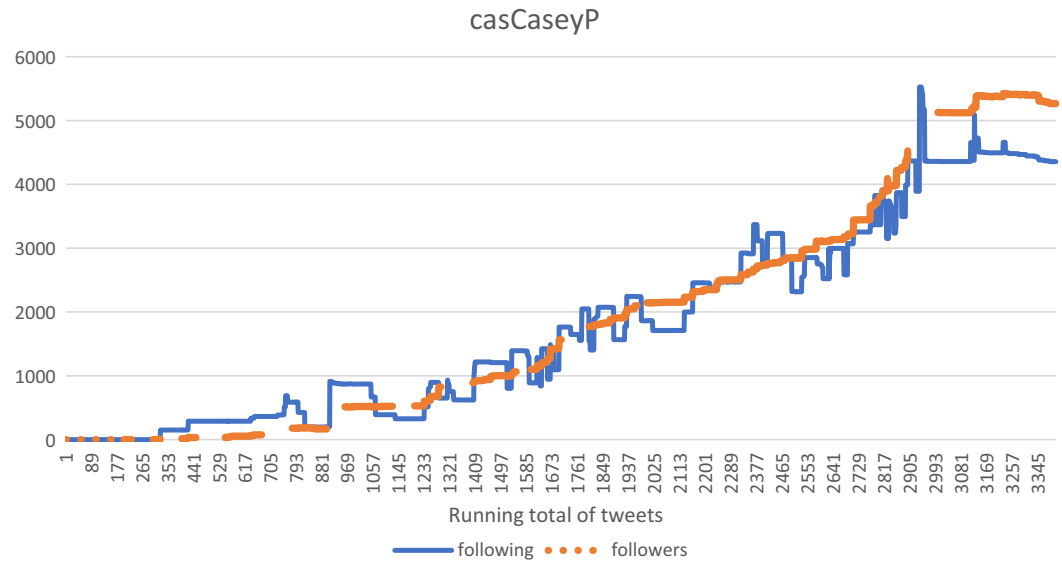

Figure 3: Basic pattern of fishing for followers

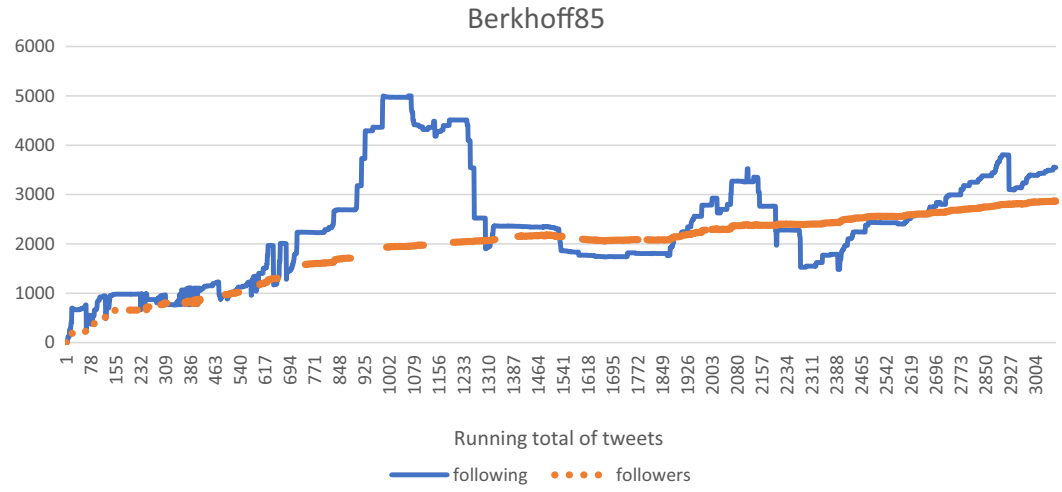

Figure 4: German example of 'follower fishing'

Within the large amount of mainstream media commentary that has attended to the activities of the IRA over the past couple of years, seventeen spoofed accounts have acquired a certain public infamy,[12] either owing to the contents of their messaging or the relatively sizeable numbers of followers they had. All of them engaged in follower fishing to build audience and influence.

Narrative switching

A third pattern of IRA account behaviour was 'narrative switching'. The operators would start by talking about fairly mundane issues, consistent with the spoofed owner's persona. However, at some point, often after an extended time period, messages became overtly political and frequently aligned with

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

Table 1: Regional summary of IRA behaviour

Region	Total Accounts	Follower Fishing	FF %	Purchased Followers	Purchased %
Ukraine	3	1	33%	2	67%
Iraq	7	1	14%	1	14%
Italy	8	0	0%	0	0%
United Kingdom	9	6	67%	2	22%
Germany	11	4	36%	1	9%
United States	14	12	86%	3	21%
Famous Accounts (Unknown/US)	17	17	100%	4	24%
Totals	**69**	**41**	**59%**	**13**	**19%**

established pro-Russian interest narratives. The IRA not only switched from banal to pro-Russian views, but also switched abruptly between different political positions according to current Russian operational priorities, or even just to create confusion. Narrative switching can also be used to collect certain followers, for example people interested in French yellow jacket protests, so that they can be targeted with messages at a later time. In some instances, these switches happened after the account was dormant for a time. However, this was not always the case.

A collection of IRA accounts were identified where there was a significant 'pause' in their messaging, lasting several months. Potentially, this might mean that they were dormant accounts that had been purchased by IRA operators. Alternatively, this break could have been used to suppress past political affiliations so the account could be 're-purposed' by the operator. Another theory suggests dormancy because IRA operational priorities had changed. For example, German accounts can only really be used to influence German opinion. As such, if IRA management or their political overseers had determined an alternative priority for their staff, then these accounts may have been less relevant, and the operators' attention directed elsewhere.

Figure 5 shows the graph for one German account displaying this pattern of behaviour. At some point during the break, 80 per cent of this account's tweets were deleted by its operator. On 14 June 2016 it began tweeting again, but with seventy-five followers instead of the eight it had previously. The tweets appear to be just news headlines from Germany and around the world, most of which are retweets.

Previously, this account had posted anti-Alternative für Deutschland (AfD) statements, such as: 'at least she is not populist stupid as the afd in #merkelmuststay': 'the people who choose the #afd are just sick # MerkelMustStay'; and, '#AfD is shit, AFD is shit #MerkelMustStay'. On 24 September, however, it suddenly started posting original pro-AfD tweets including: 'I #chooseAfD, because I remember # asylum crisis and no longer trust #Merkel!'; 'I #chooseAfD, because I want to live in the Federal Republic instead of Caliphate #Germany!'; and retweeting 'Every German #Patriot will vote #AfD tomorrow! We need a political earthquake to save #Germany! # Btw17 #NoAntifa #NoIslam'.

Possible (unsubstantiated) explanations for this switch in position are that it was a direct response to Chancellor Merkel's public statement on 14 September that the EU would not consider lifting sanctions on Russia.[13] In the September elections AfD achieved what *The Guardian* called a 'stunning success'; meanwhile Merkel's party had their worst result since World War II.[14] It should be noted that although each of the eleven accounts posted pro-AfD tweets, their numbers were small compared to the pro-Merkel tweets they had previously shared. One reason for this could be that the German authorities were said to be on the lookout for Russian interference and operators were directed by their managers to be subtler than in the past.

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

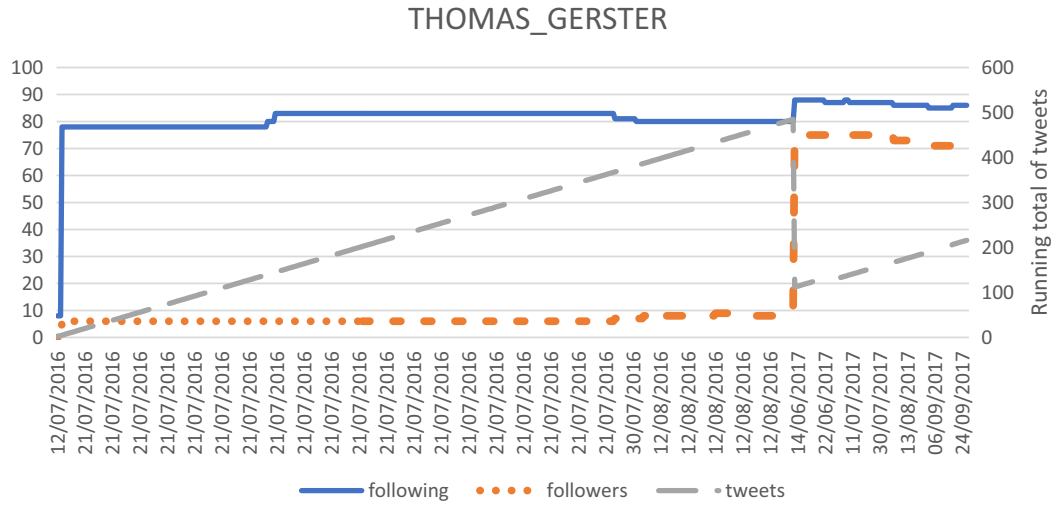

Figure 5: Example of 'narrative switching'

Synchronicity analysis

As noted previously, IRA operators were required to run multiple accounts and to generate certain volumes of activity. This provides an opportunity for attributing accounts to Kremlin direction and control by analysing temporal sequences of messaging behaviour. The method for doing this involves 'synchronicity analysis' as it looks for simultaneous patterns of messaging as a way of identifying where multiple accounts are being controlled by the same author.

The potential power and value of synchronicity analysis is demonstrated by examining the posting activities of eleven prolific IRA accounts adopting a pro-Merkel stance. On 21 July 2016, @Martin_S32 posted its first tweet of the day 'Mommy is the best #MerkelMustStay'. In total, it posted 265 tweets that day, most displaying very strong support for Angela Merkel. Initially it was assumed that this might be one of a small number of known Russian accounts adopting this stance, with others communicating more extreme right-wing messages. Further investigation revealed, however, that a series of IRA accounts were communicating messages supportive of the German Chancellor. Even more significantly, when the timings of these messages were plotted, they displayed a very similar pattern. Figure 6 plots these activity patterns on a time-line. The larger the bubble, the greater the volume of messages sent at that point in time by that account.

It can be observed that the key 'pulses' of messaging activity are very similar, but not identical. All of these accounts stopped posting tweets on 12 August and then were inactive for a minimum of six months. The inference drawn is that these accounts were probably being controlled by one author, possibly using a system such as Tweetdeck. This would be consistent with the working arrangements at the Internet Research Agency described above.

In July and August 2016, these accounts sent hundreds of pro-Merkel tweets, often using the hashtag #MerkelMustStay. As with other IRA tweets, they frequently integrated an unrelated trending hashtag in order to push their own hashtag, for example #WorldElephantDay. These posts came during a period when Angela Merkel was under intense political pressure to step down as Chancellor, with Reuters noting that in January, 40 per cent of Germans thought she should resign over her refugee policy.[15] This would be consistent with the Russian state's known modus operandi for seeking to leverage political weakness to amplify social and political tensions.

Germany was subject to a series of terrorist attacks between 18 July and 26 July 2016,

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

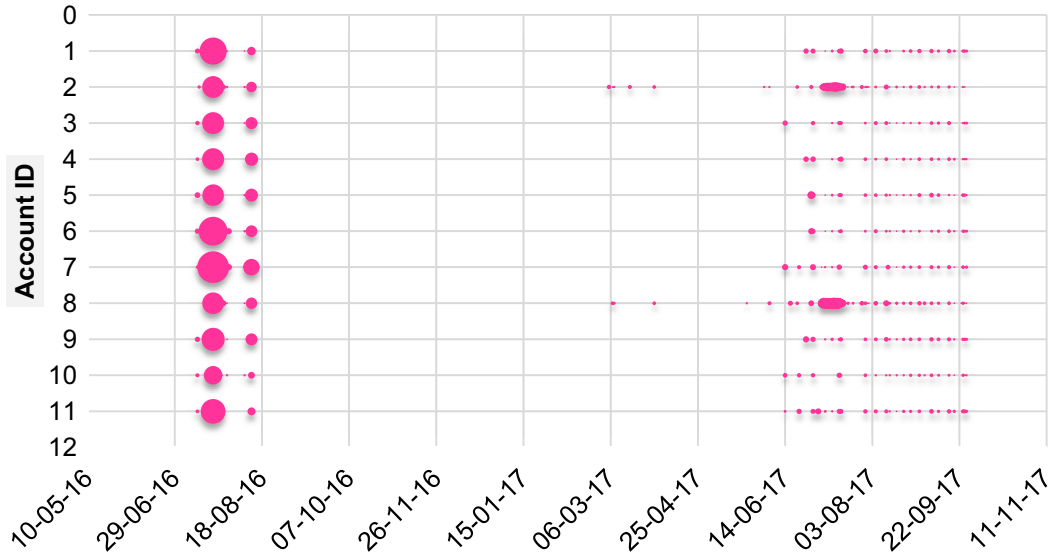

Figure 6: Pro-Merkel accounts schedule

in which fifteen people died. The so-called Islamic State claimed responsibility for two of the attacks and three of the attackers were asylum seekers.[16] The Nice terror attack also occurred in July, sending shockwaves around Europe. Despite this sequence of events, these accounts were very supportive of the Merkel government's refugee policy: 'Lady #Merkel, Stick to your line! "The #refugees" are not dangerous mass but people! # MerkelMustStay'; and 'The refugee policy of Mrs. Merkel shows that she is compassionate! #MerkelMustStay'.

Consistent with this line, all of the accounts disparaged the anti-immigration AfD, with multiple variations of '#AfD is shit, AfD is shit #MerkelMustStay' being posted during a time when polls were suggesting AfD was enjoying some mainstream support (35 per cent CDU to 12 per cent AfD).[17] The media has typically blamed Russia for supporting populist/anti-immigrant parties, but at a point where Merkel (and EU unity) was politically weakened, Russian controlled accounts were messaging support for her domestically. There were significant similarities between the content of tweets being posted by these accounts. Some were copied verbatim, and others had single word differences, usually a hashtag. Combined with the timings of the tweets, this points to the likelihood of a single person or team operating all of these accounts in a co-ordinated strategic fashion.

Synchronicity analysis revealed this group comprised forty-five accounts, thirty-four more than we had previously discovered. It also revealed another German team of twenty-five accounts operating in a very different manner, obsessed with Brexit, with three of their top five hashtags directly related to the Brexit vote. These posted a variety of messages that promoted the idea of leaving the EU such as: '#Brexit will only have small consequences! You cannot act in the EU #BritainInOut #GoodbyeUK #RemainINEU #EUref' and 'Do not let yourself be manipulated with fear. #Brexit #BrexitOrNot #GoodbyeUK #BritainInOut'. Confusingly, these same accounts also posted anti-UK messages in apparent offence that the British public had chosen to leave, tweeting '#britaininout #goodbyeUK Let them drown on their island now' and '#britaininout #goodbyeUK We do not need snobs'.

In direct opposition to the pro-Merkel accounts, the latter group invoked anti-refugee sentiments: '#britaininout #goodbyeUK You flee like #Refugees' and '#britaininout #goodbyeUK Take refugees with you!'. They

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

also blamed Merkel's migration policy for increasing terror in Europe 'Thank you, Mrs Merkel, that citizens now have to be afraid of terror in Europe. #stopptTerror' and spouted populist rhetoric 'Why can not our warships send these #migrants back immediately? #stopptTerror'. The Russians were amplifying both sides of the political argument simultaneously, trying to increase the social fissures associated with them.

When the high profile (infamous) Internet Research Agency accounts, were tested in this way only two (@southlonestar and @southlonestar2) could be linked through synchronicity analysis (the latter appears to have been set up as a 'backup' in case Twitter suspended @southlonestar). One possible implication of this is that if an account achieved a certain scale of influence, then operators focussed on running that one persona. Alternatively, it may simply be an artefact of higher skill operators being in charge of these accounts.

Rather than just retrospective linkage, synchronicity analysis has two potential uses going forward. First, if there is an identified Kremlin controlled account, then treating temporal pulses of messaging activity as a behavioural signature might enable identification of other 'accounts of interest'. Equally possible is that, with a number of accounts, the presence of similar pulsing sequences can be interpreted as a potential indicator of a common controller.

To test the potential of these methods we applied them to all 2,848 Twitter accounts featuring in the full Twitter dataset. The results are represented graphically in Figure 7 where the nodes represent IRA Twitter accounts, shaded by clusters. Some clusters have had their shapes changed to make them easier to differentiate.

Representing the data in this way, the closeness in proximity between two connected accounts indicates how similar their tweeting activity is. Thus, the large cluster in the centre of the graphic (box A) represents 449 accounts that have their region predominantly set to Russia and tweet primarily in Russian. This is significant in that it reflects the pre-eminent strategic objective of the Russian state, in terms of the perceived importance of managing domestic public opinion and in the 'near abroad'. This provides an important corrective to much of the public debate that has taken place in the West about Kremlin disinformation campaigns, which has worried predominantly about impacts in these contexts. But this focus neglects just how much of the IRA's effort was directed towards influencing the views and perceptions of Russian speakers.

In addition to the main cluster, the linked accounts in the top right-hand corner and constituting the second largest group (box B), look to be those associated with the IRA's American department. Intriguingly, in terms of their temporal activity profiles and message contents, these could be loosely connected to a much smaller group of Russian facing accounts. The latter were probably engaged in covering similar topics, but for a different audience.

Around the edges of the diagram, are a large number of smaller 'satellite' clusters. The accounts here can often be distinguished on the basis of them using different languages, or focussing upon particular social identity politics (such as Black Lives Matter). Box C shows a cluster of forty-five German accounts, which include the pro-Merkel accounts we talked about earlier. In total, 2,031 or 71 per cent of the IRA Twitter accounts in the dataset could be linked to at least one other, comprising 119 separate clusters. This affords a clear sense of how multiple accounts were being employed by IRA operators to push key messages in a co-ordinated fashion.

The attribution challenge

Detailed forensic analysis methodologies of the kind outlined above are necessary for establishing an evidence base for detecting current and future activities of a similar nature. This is important given the increasing difficulties associated with confidently attributing accounts involved in communicating disinformation to Kremlin direction and control, as they have become increasingly sophisticated. Not all disinformation comes from overseas; much of it is authored by citizens resident in Western countries. When such sources are mis-attributed, it is especially problematic, as it negatively impacts public confidence in the authorities involved and can be used as propaganda against them.

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

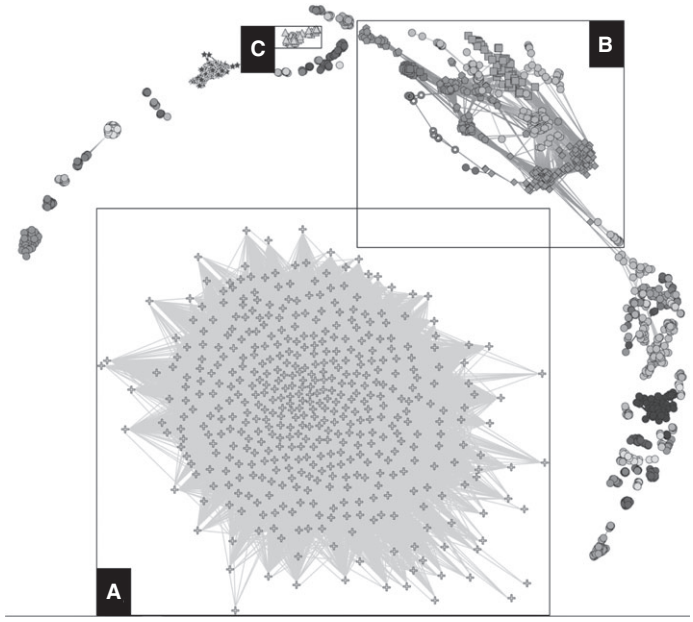

Figure 7: Network graph of synchronicity analysis on all IRA accounts

Such challenges have been exacerbated by a general recalcitrance on the part of the principal social media platforms to admit proactively that malign actors are operating on their systems. Whilst they have responded to these issues when pushed by governments, their responses in terms of increasing restrictions to application programming interface (API) access and related interventions have, somewhat ironically, also made it harder for independent researchers to assist in detecting and attributing disinforming communications to Kremlin backed accounts. There is a danger that the platform providers are manoeuvring into an arrangement where only they are positioned routinely to detect bad actors.

Further challenges to the work of attributing disinformation has resulted from the strategy pursued when a suspected Kremlin backed account (or accounts) are detected. Typically, steps are taken either to 'take down' the account from the platform, or to 'expose' its presence through publicising its suspicious activities. The issue is that such approaches are of limited effectiveness in altering the dynamics of the disinformation ecosystem. Moreover, this has enabled the IRA and other Kremlin backed units to learn how they are being detected and to adapt their methods accordingly, the consequence being that some of their approaches have become more sophisticated and harder to detect. Far more impactive, therefore, in terms of leveraging disruption on the capacity and capability to spread disinformation, is a strategy that seeks to build an understanding of a disinformation network over time, and implements interventions against multiple nodes simultaneously. This is how police investigators have learned to do disruptions of criminal networks in offline spaces to maximise impact.

Conclusion

In his coruscating account of life in Russia and the state's normalised use of 'soft facts' to convey multiple and shifting 'truths' to its citizens, Peter Pomerantsev, articulates how the aggregating effect is a profound suspension of belief.[18] Unlike classic propaganda, the design is not intended to seduce people to invest in a particular 'truth', but rather to render them in a state of profound and radical doubt about what to believe—a state of epistemic anarchy.

One of the most striking aspects of the growing number of analyses of the IRA's

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

activity, especially around the 2016 US presidential election, is just how extensive and varied it was. This, notwithstanding, it is equally vital to recognise that similar efforts have been deployed across a number of other situations and settings. With this in mind, what is required now is a series of detailed and forensic analyses, of the kind outlined herein, to distil the key operational tactics and techniques that were being used. If this can be accomplished, then it enhances capacity and capability to detect similar attempts going forward, and to constrain their efficacy.

The particular value of the behavioural models discussed is that they document fairly unusual patterns of activity that function as 'signatures' or 'tells' that an account is possibly being run by an operator with specific intents. The potential is one that is similar to how police detectives use behavioural signatures to profile repeat offenders: their digital equivalents can be used to detect malign influencers online. A benefit of the kinds of diagnostic data used to ascertain these behaviours is that they are largely language agnostic and do not rely upon an ability to read and interpret the contents of what is being communicated.

At this precise moment, it is difficult to know how worried we should collectively be about disinformation communication. There are indications that despite the efforts of governments, intelligence agencies and platform providers, misinformation and disinformation is becoming an endemic feature of the modern media ecosystem. And whilst there is certainly something objectionable about attempted behaviour modification in respect of democratic processes and outcomes, there is actually remarkably little robust evidence that such disinforming communications have a discernible measurable impact upon how the majority of people think, feel or act. Messaging of this kind may be better at 'channelling' peoples' pre-existing values and opinions than it is in changing them. Perhaps then it is more appropriate to argue that disinformation has more impact in shaping the issues we collectively think about, than what we individually think. That is, its pernicious influence resides in framing and agenda setting what troubles come to be defined as key public policy problems.

Notes

1 H. Benkler et al., *Network Propaganda: Manipulation, Disinformation and Radicalization in American Politics*, New York, Oxford University Press, 2018.
2 *RBC Magazine*, 'Investigation of RBC: how the "factory of trolls" worked in the elections in the United States', 17 October 2017; https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1; Radio Free Europe, 'One professional Russian troll tells all', 25 March 2015; https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html (both accessed 9 April 2019).
3 The Higher Learning, 'Russia has a troll army that is trying to mold public opinion on internet news sites', 4 June 2014; http://thehigherlearning.com/2014/06/04/russia-has-a-troll-army-that-is-trying-to-mold-public-opinion-on-internet-news-sites/ (accessed 9 April 2019).
4 Radio Free Europe, 'One professional Russian'.
5 Yahoo!, 'Trolling for Putin: Russia's information war explained', 5 April 2015; https://www.yahoo.com/news/trolling-putin-russias-information-war-explained-063716887.html (accessed 9 April 2019).
6 Radio Free Europe, 'One professional Russian'.
7 Ibid.
8 BuzzFeed, 'Documents show how Russia's troll army hit America', 2 June 2014; https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america (accessed 9 April 2019); Radio Free Europe, 'One professional Russian'.
9 *RBC Magazine*, 'Investigation of RBC'.
10 Yahoo!, 'Trolling for Putin'.
11 KickFactory, 'The average Twitter user now has 707 followers', 23 June 2016; https://kickfactory.com/blog/average-twitter-followers-updated-2016/ (accessed 9 April 2019).
12 IRA accounts tested: TEN_GOP, Blackmatterus, Blacknewsoutlet, Blacktolive, Bleepthepolice, Crystal1johnson, Jeblary2016, Jenn_abrams, Lgbtunitedcom, Muslims_in_usa, Pamela_moore13, Southlonestar, Thefoundingson, Tpartynews, Trayneshacole, Usa_gunslinger, Wokeluisa.
13 Yahoo!, 'EU firm on Russia sanctions over Ukraine: Merkel', 14 September 2018; https://sg.news.yahoo.com/eu-firm-russia-sanctions-over-ukraine-merkel-153248229.html (accessed 9 April 2019).
14 C. Mudde, 'What the stunning success of AfD means for Germany and Europe', *The Guardian*, 24 September 2014; https://www.theguardian.com/commentisfree/2017/sep/24/germany-elections-afd-europe-immigration-merkel-radical-right (accessed 9 April 2019).

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).

15 Reuters, 'Forty percent of Germans say Merkel should resign over refugee policy: poll', 29 January 2016; https://uk.reuters.com/article/us-europe-migrants-germany-merkel-idUKKCN0V70KM (accessed 9 April 2019).
16 Reuters, 'Germany's far-right AfD claws back some support after attacks', 31 July 2016; https://www.reuters.com/article/us-germany-afd-idUSKCN10B0FR?feedType=RSS&feedName=worldNews (accessed 9 April 2019).
17 Ibid.
18 P. Pomerantsev, *Nothing is True and Everything is Possible: The Surreal Heart of the New Russia*, London, Faber & Faber, 2014.

© 2019 The Authors. *The Political Quarterly* published by John Wiley & Sons Ltd on behalf of Political Quarterly Publishing Co (PQPC).