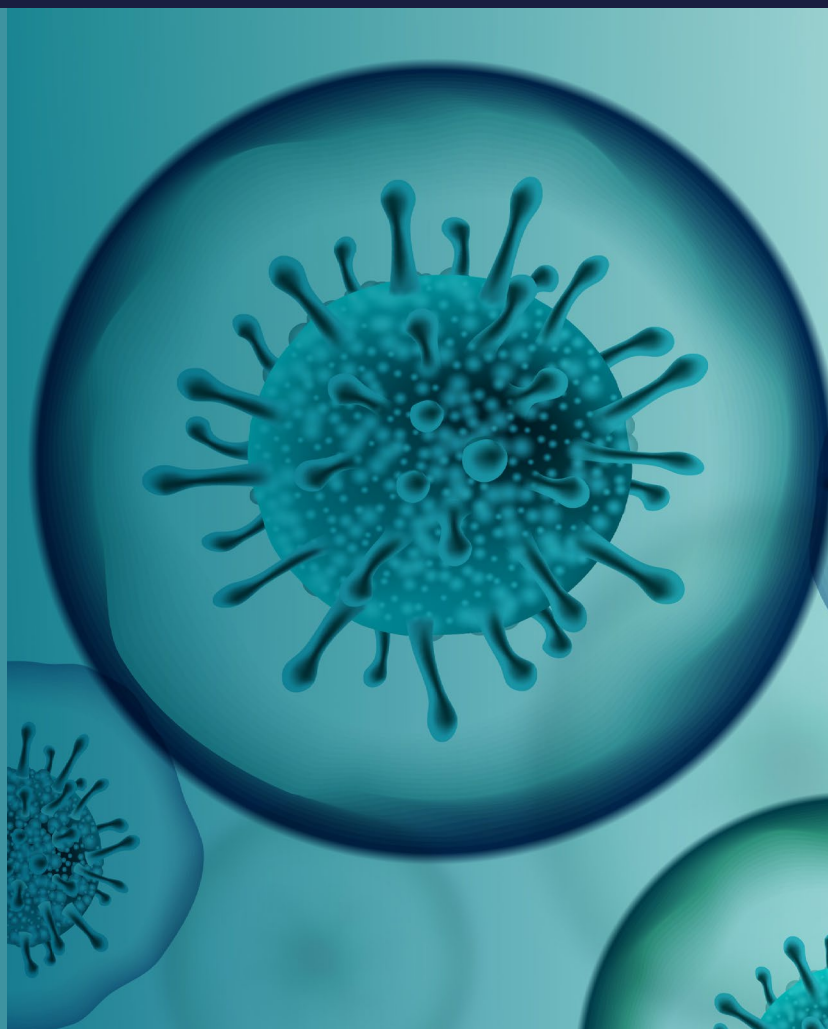
OSCAR
OPEN SOURCE COMMUNICATIONS, ANALYTICS RESEARCH

‘Perception Infections’: Tactics and Techniques of a Russian Information, Influence and Interference Operations (IIIO) Methodology

2020



EXECUTIVE SUMMARY

This report analyses the operational tactics associated with a methodology used by hostile state actors to manipulate public perceptions and political agendas. Analogous to a biologically based viral infection, it works by infiltrating the information system in a way that is difficult to detect, and then hi-jacks the system's established logics and mechanisms to spread and distribute the disinformation or malinformation that has been introduced. We define this as a 'perception infection methodology'.

Perception infections utilise a different logic and practices to the more 'organic' disinformation campaigns associated with the Internet Research Agency (IRA) that have been the predominant focus of public and political debates to date. **There are five defining techniques engaged by perception infection methodology:**

One to Many

- a defined unit of information, often based around 'hacked' or 'leaked' documents, is used to manipulate the perceptions of a larger audience, influencing their definitions of the situation and the collective ordering of reality. This contrasts with known IRA disinformation campaigns that have used multiple 'spoofed' accounts, and an array of narratives, images and memes, across a variety of topics.

Obscure the Origins

– perception infections work through a series of transmission events to obfuscate the real source of the material. This can be assisted by 'hacking' known human cognitive, emotional and behavioural biases so attention focuses upon what is being communicated, rather than worrying about source provenance.

Digital Typhoid Marys

– a key focus of this approach is to target efforts to persuade established influencers to engage with the content and act as 'carriers' in terms of getting it into the media stream. By having influencers and authority figures repeat and reproduce the message, they lend it credence and help to obscure its origins.

Hack Media Logic

– the process of 'laundering' the story so it comes to be believed by at least some audience segments functions by exploiting vulnerabilities in the logics and practices of contemporary media ecosystems. These are 'hi-jacked' to diffuse and replicate the information.

Kernel of Truth

– perception infections can pivot around both genuine and forged documents and information, but they are effective when they have surface plausibility. Thus, analogous with other forms of viral contagion, such attacks typically focus upon established weak points in the 'host' social and cultural system. For example, this might exploit distrust in politicians, or attempt to de-stabilise political relations between two nation states.

This conceptual model is developed initially through careful analysis of data from the US-UK Brexit trade deal leak publicised by Jeremy Corbyn just prior to the 2019 General Election. It is then tested for 'fit' against material derived from 61 Reddit accounts that were suspended for links to the above operation and engaging in inauthentic co-ordinated behaviour. Based upon this analysis we have identified a hitherto undetected operation smearing senior, high-profile Polish politician Jaroslaw Kaczynski (former Prime Minister and brother of former President) in 2016. The components of the model are then further applied to an additional two case studies: (1) The 'hack' of the Democratic Party servers in the US in 2016; (2) The campaign run around material leaked or hacked about the UK Integrity Initiative.

Taken together, these case studies demonstrate how the methodology of perception infections can be understood as involving implanting a particular unit of (dis)information within a media ecosystem, then encouraging it to be spread by carriers through a series of transmission events, intended to influence the views and interpretations of audience members. **By analysing several empirical case studies, it is possible to see how these precepts are operationalised in practice in relation to the contemporary information environment:**

- Initial publication occurs in a relatively obscure outlet, with the material presented as deriving from a leak/hack. The documents are sometimes genuine, but more often forged.
- Attempts are made to draw the attention of established 'influencers' to the material, especially where their interests are aligned with the subject matter. The intent being to have the influential individual repeat the content of the material, lending it credence and plausibility, thereby obscuring and obfuscating its real provenance.
- Functioning akin to 'digital Typhoid Mary' figures, these influencers significantly extend the volume of reach and engagement with the implanted material through a sequence of transmission events.

Importantly, there are significant historical precedents for this approach in terms of established KGB 'active measures' techniques. Accordingly, we infer that the contemporary usages of similar patterns of behaviour may be associated with the activities of the main Russian state intelligence agencies, rather than organisations like the Internet Research Agency.

In foregrounding the principles and logics of perception infection methodologies, the analysis reported contributes to developing a more comprehensive understanding of the variety of ways in which Russian state actors are engaging in forms of digital influence engineering. For example, it is noted that their activities do not always pivot around disinformation, but can more subtly distort factual information also. Accordingly, the analysis develops a taxonomy of six different modes for conducting 'Information, Influence and Interference Operations' engaged by actors aligned with the Kremlin.

01 **'Pure' or 'classic' disinformation campaigns** where communication pivots around the transmission of purposively and deliberately false information, often relating to both the message and messenger. Thus, disinformation combines both an intent and action designed to deceive.

02 **Misinformation into disinformation pathway** is where unintentionally misleading material is deliberately amplified to induce negative consequences.

03 **Disinformation into misinformation pathway** is an ideal scenario for hostile state actors, in that others amplify a false message sincerely believing it to be true or accurate.

04 **Information – Influence Operations** seek to shape the ordering of reality through perceptual management and manipulation. This can involve distortion of factually accurate information, as opposed to outright disinformation.

05 **Information – Interference Operations** involve physical 'real world' interventions, as opposed to psychological mechanisms.

06 **Information, Influence and Interference Operations** are the most complex version, and involve both psychological and physical interventions to shape public perceptions and political agendas.

INTRODUCTION

Disinformation campaigns and allied digital influence engineering strategies are designed and delivered to influence public perceptions of a range of contentious social problems and political issues. This report illuminates a repertoire of tactics and techniques that together constitute a defined Russian IIIO methodology that works by infiltrating specific messages and material into the media ecosystem. The spread and diffusion of the unit of (dis)information is accomplished by harnessing and exploiting the ecosystem's standard processes and procedures. By obscuring and obfuscating the origins of these messages, the credibility of the content is enhanced and rendered more plausible. This frequently involves persuading targeted influencers and other 'authority' figures' to repeat and reproduce the content, enabling far greater audience attention to it. We label this a 'perception infection'.

Adopting this focus is significant because such targeted tactics have been relatively neglected compared with the attention directed towards the more 'organic' forms of disinformation employed by the Internet Research Agency (IRA) in the lead-up to the 2016 US Presidential election. Perception infections are rather different from known IRA tactics, in terms of how and why they work. Just as with a viral infection, they involve getting the harmful material inside the 'host' media ecosystem, and then hi-jacking its processes and mechanisms to distribute it. Importantly, perception infections work with a single unit of (dis)information to manipulate public perceptions and attention, whereas orthodox IRA disinformation campaigns employed multiple narratives, images and memes.

Based upon detailed analysis of a series of empirical case studies (see below), five defining techniques of perception infection methodology can be distilled:

01 **One to Many** – a particular unit of information, often based around 'hacked' or 'leaked' documents, is used to manipulate the perceptions of a larger audience, influencing their definitions of the situation and the collective ordering of reality. This contrasts with known IRA disinformation campaigns that have used multiple 'spoofed' accounts, and an array of narratives, images and memes, across a variety of topics.

02 **Obscure the Origins** – perception infections work through a series of transmission events to obfuscate the real source of the material. This can be assisted by 'hacking' known human cognitive, emotional and behavioural biases so attention focuses upon what is being communicated, rather than worrying about source provenance.

03 **Digital Typhoid Marys** – a key focus of this approach is to target efforts to persuade established influencers to engage with the content and act as 'carriers' in terms of getting it into the media stream. By having influencers and authority figures repeat and reproduce the message, they lend it credence and help to obscure its origins.

04 **Hack Media Logic** – the process of 'laundering' the story so it comes to be believed by at least some audience segments, functions by exploiting vulnerabilities in the logics and practices of contemporary media ecosystems. These are 'hi-jacked' to diffuse and spread the information.

05 **Kernel of Truth** – perception infections can pivot around both genuine and forged documents and information, but they are effective when they have surface plausibility. Thus, analogous with other forms of viral contagion, such attacks typically focus upon established weak points in the 'host' social and cultural system. For example, this might exploit distrust in politicians, or attempt to de-stabilise political relations between two nation states.

Framed in this way, there are clear analogies with known Soviet era 'active measures' techniques. Updated for the information age, our assessment is that they are probably being operationalised by Russian state intelligence, rather than the Internet Research Agency and similar. Accordingly, the empirical case based discussions are informed by reference to some historical context on the use of similar processes by the KGB pre-internet. This is important for understanding how the tactics discussed herein are positioned in a tradition of distortion and deception.

The empirical analysis commences with a case study of the NHS Brexit document hack/leak that occurred in the lead-up to the 2019 UK General Election. This is on the grounds that it was this event that alerted us to the key features of the methodology that is the principal focus of this report and demonstrates how the tactics described have been successfully mobilised.

Having briefly established the principal tactics and techniques associated with this operational methodology, the analysis applies these to other data that has been identified in the wake of the NHS-Brexit trade deal leaks. This evidences a clear pattern, suggestive that use of this IIIO methodology has probably been more widespread than has been appreciated to date. The report concludes by drawing upon the empirical materials to construct a taxonomy of the different strategic methodologies to communicate disinforming, distorting and deceptive materials in order to shape public perceptions and political agendas.

HISTORICAL RESONANCES

Disinformation is a concept with its roots in Soviet era active measures, as is the notion of an 'information operation'. Although disinformation has become something of a 'catch all' term recently, if used with conceptual precision, it refers to a specific mode of communication involving the deliberate and co-ordinated transmission of misleading information. This is different from its conceptual cousin of 'misinformation', where the intent to mislead is missing, albeit the outcome can be similar.

The principles of how and why transmitting false information to influence peoples' understandings of social reality works have long been established, as exemplified by the following quotation from Ladislav Bittman, deputy chief of the Czechoslovak intelligence service's disinformation department from 1964 to 1966:

> *"every disinformation message must at least partially correspond to reality or generally accepted views."*[1]

In a subsequent passage he elaborates:

> *"Soviet bloc propagandistic disinformation is systematically polluting international relations with massive dosages of distorted or totally false messages to influence public opinion. The messages usually play upon existing political conflicts and cultural prejudices…"*[2]

The operationalisation of these principles is adroitly described in Boghardt's (2009) detailed account of how the KGB implanted a story that the US government was responsible for the AIDS epidemic in the early 1980s.[3] Dubbed 'Operation Infektion', it started by seeding an anonymous letter in 1983 in an obscure newspaper in India called the Patriot. This letter included a claim that an American scientist and anthropologist had attributed the AIDS virus to a Pentagon programme experimenting with new biological weapons, citing a number of well known American media sources.

Initially there was no reaction to the contents of the letter. As Boghardt describes, it lay dormant for three years until in 1985, Literaturnaya Gazeta, one of the KGB's prime conduits in the Soviet press for propaganda and disinformation, published an article by Valentin Zapevalov, titled "Panic in the West or What Is Hiding behind the Sensation Surrounding AIDS." Following on from which, the story was taken on, developed and propagated by a retired East German bio-physicist Professor Jakob Segal. According to Boghardt's research, Segal was known to the KGB and East Germany's Ministry for State Security (colloquially known as the Stasi), and for a period of several years he played a critical role in 'mainstreaming' it, such that it became accepted as 'true' in some thought communities.

The success in insinuating this narrative into the media stream, exemplifies how such propaganda techniques are de-signed to try and exploit extant social fissures, by sowing doubt and exacerbating distrust. They are akin to forms of perceptual intervention that are intended to manipulate and 'manage' the ways audiences interpret, think about and

1 Source: p.49 Bittman, L. (1985) 'The KGB and Soviet Disinformation: An Insider's View' (Washington DC: Pergamon-Brassey's).

2 P.218

3 Boghardt, T. (2009) 'Soviet bloc intelligence and its AIDS disinformation campaign', Studies in Intelligence. 53/4.

affectively respond to certain issues of interest. Sometimes this is achieved through outright deception, but other times it is accomplished by 'distorting' aspects of empirical reality in more subtle and nuanced ways. The key point being that Russian intelligence services have a long history and established playbook for constructing disinforming, distorting and deceptive communications, in an effort to create division, doubt and distrust. Bittman (1985) confirms this, describing how the KGB's First Directorate regularly forged press releases and wrote letters that they discretely injected into media outlets, sometimes quite remote ones. The purpose being that by 'laundering' the origins of a claim through securing publication in a nation's newspaper, book or magazine, the content is often absorbed innocently by international media and republished as authentic. Understanding this backdrop, should be particularly important insights for detecting their more recent reinventions of these base methodologies.

On May 6, 2019, Facebook took down a small network of 16 fake accounts attributed by them to Russia. These had been sharing false, polarizing, and divisive content, including attacks on immigrants, albeit achieving little apparent audience engagement. The Atlantic Council's Digital Forensic Research Lab (DFRLab) developed these materials to uncover a larger-scale influence operation spanning nine languages, over 30 social networks and blogging platforms, and multiple fake user profiles and identities. Reflecting similarities with elements of the original Operation Infektion, the DFRLab team dubbed it 'Operation Secondary Infektion.'[4] **Drawing out the parallels, they defined five key features of the updated approach:**

- Repeated use of the same usernames (or variants), publishing the same article across different platforms;
- High operational security awareness and multiple engagement of single-use burner accounts to publish stories;
- The fake personas repeatedly used an unusual combination of sites to post content, including the fringe German-based site homment[.]com;
- Regular language errors in English posts. In particular, operators struggled with the words "a" and "the" and with the word order in questions;
- Use of accounts on other platforms (Twitter and Facebook) to try to draw the attention of politicians, journalists and other influencers to its stories. On Twitter, operation accounts addressed their posts directly to such influencers using @-mentions; on Facebook, they posted the stories into politically focused groups.

As will be detailed, these elements form something of a recurring motif across a number of similar operations. They can be interpreted as a kind of 'behavioural signature' of 'perception infections' that can be used to detect other attempts to influence public definitions of the situation and political agendas.

THE US-UK BREXIT TRADE DEAL 'LEAK'

Sixteen days before the UK General Election in December 2019, Jeremy Corbyn publicised unredacted documents from US-UK trade negotiations. Allegedly these showed that the UK government was preparing to give access to the NHS to American companies in return for a favourable post-Brexit trade deal. Subsequent investigations by Graphika, Reuters, with assistance from Cardiff University, Oxford University and DFRLab, identified versions of this document had been circulating online for several weeks and had probably been placed there by actors with links to the Russian state. Responding to reports of this investigation Reddit confirmed: "we believe this was part of a campaign that has been reported as originating from Russia."[5]

4 Digital Forensics Research Labs (2019) "Operation Secondary Infektion: A Suspected Russian Intelligence Operation Targeting Europe and the United States.
5 https://www.reddit.com/r/redditsecurity/comments/e74nml/suspected_campaign_from_russia_on_reddit/

Table 1 below provides a brief sequence of events in order that the reader can discern the key activities.

Date	Events
18-Feb-19	Images uploaded to Imgur in preparation for operation to commence. The image was not hosted 'publicly', (i.e searchable on Imgur) it requires the link to view.
21-Oct-19	u/gregoratior posts 'leaked' documents to Reddit, multiple attempts to draw attention to it largely ignored.
23-Oct-19	'Max Ostermann' posts story to 3 sites: German subreddit, meinbezirk[.]com; homment[.]com. Same time 'Wilbur Gregoratior' republished an English version on beforeitsnews[.]com.
23-25-Oct-19	@gregoratior Twitter account starts sending total of 51 tweets tagging politicians, journalists and pro-Assad and pro-Putin bloggers (continues into Nov) trying draw their attention to the leak/hack.
19-Nov-19	Corbyn shows redacted version obtained by Freedom of Information request at event.
21-Nov-19	Global Justice Now state to BBC they were alerted to docs on Reddit by anonymous email. They acted as the transmission agents passing documents to the Labour Party
27-Nov-19	Jeremy Corbyn presents full unredacted documents at a press conference.
2-Dec-19	Reuters and Graphika publish reports drawing attention to similarities to Op. Secondary Infektion from May 2019.
06-Dec-19	6 days before election, Reddit takes down 61 accounts + 1 subreddit following 'medium to high confidence' assessment that US-UK Brexit leaked documents about NHS may have been placed by RUS actors.

Table 1: Timeline of Key Events

As should be clear, there are multiple elements that echo the procedures utilised in the earlier 'Operation Secondary Infektion' (and indeed the 1980s version also). These include:

- Initially publishing the documents in a relatively obscure outlet;
- Followed up by repeated targeted attempts to draw attention to these;
- And then, targeting specific individuals because the content of the documents chimes with their established interests.

All as a way of obscuring the origins of the material whilst getting it to filter into the media stream. From an early point, it was our assessment that the documents were genuine.

Of particular interest to us here, is the role played by politicians, journalists and celebrities who were subject to targeted communications by the Russian operatives. These individuals are vital to the operationalisation of the perception infection methodology overall, as they functioned as the 'agents of transmission' for the (dis)information that the hostile state operatives wanted to get circulating. In this regard, their role is akin to a digital equivalent of a 'Typhoid Mary' in other situations of contagion. Named after Mary Callon, who was an asymptomatic carrier of the pathogen associated with Typhoid, it was alleged that in New York in the early 1900s, she was responsible for infecting 51 people as a result of them coming into contact with her. Today, the term 'Typhoid Mary' is used for someone who either deliberately or unknowingly spreads disease or some other harm. This is directly analogous to the role that the targeted influencers were being persuaded to perform through the communications targeted at them. In respect, of the above sequence of events it was Global Justice Now that assumed the 'Digital Typhoid Mary' role, transmitting the key document into the orbit of senior Labour Party members.

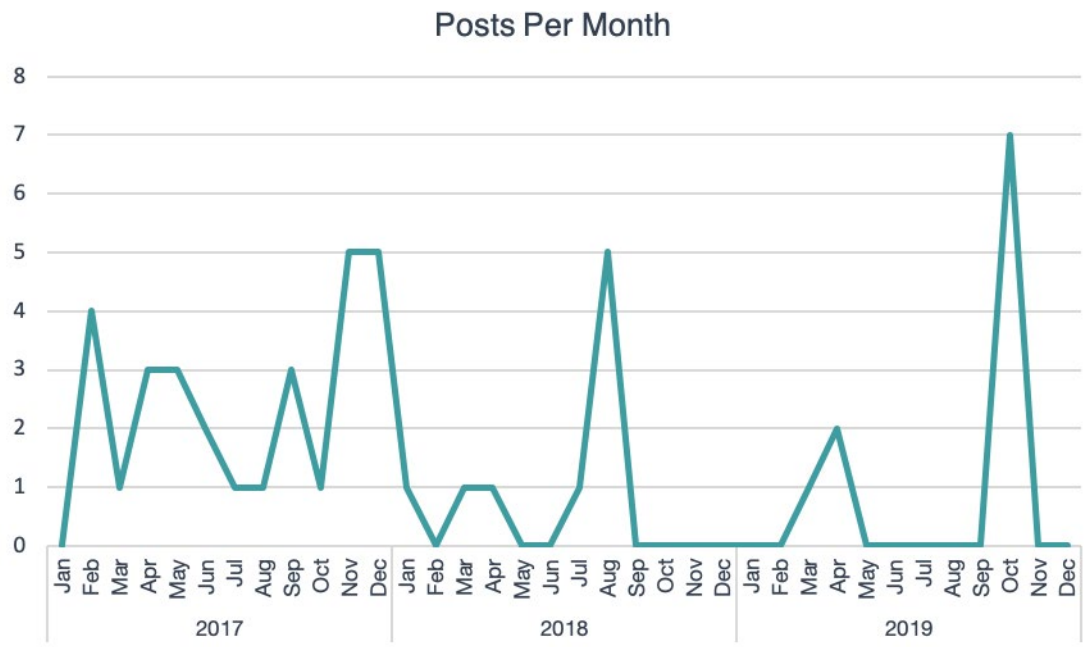
ANALYSING THE 61 REDDIT ACCOUNTS

As rehearsed above, following the US-UK Brexit trade leak allegations, on the 6th of December 2019 Reddit announced they had taken action against 61 accounts. This was because they were all showing a "pattern of coordination" linked in some way to the behaviour of the u/gregoratior account responsible for leaking the 'official-sensitive' classified documents. Reddit's assessment was that all 61 accounts (including u/gregoratior) were tied to the original Secondary Infektion operation identified earlier in the year, albeit specific and precise justifications for this assessment were not published.

The accounts identified were suspended by Reddit and preserved in their final state to enable researchers to investigate them. This section of the report uses the data from these accounts to map some key patterns in their behaviour.

Figure 1 below provides an overview of the posting activity of all the 61 accounts over time. It shows a relatively steady level of activity in 2017, that then falls away, until the dramatic spike in 2019 that relates to the US-UK leaks.

Figure 1: Active Accounts per Month



USER METADATA ANALYSIS

Profiling the posting and commenting volumes across the accounts, together with the topic variety and language, identifies 8 principal modes of behaviour. These are outlined in Table 2 below:

Type	Description	Count
A	Multiple posts, multiple articles, multiple comments	1
B	Multiple posts, multiple articles, no comments	2
C	No posts, single comment	4
D1	Multiple posts, same article, no comments, English	14
D2	Multiple posts, same article, no comments, Non-English	15
E1	Single post, no comments, English	6
E2	Single post, no comments, Non-English	6
F	No posts, no comments	13

Table 2: Reddit User Mode of Activity

Table 3 (opposite) maps the accounts released by Reddit to the modes of activity, along with their time and day of creation, the lag between creation and first posting, the duration that an account was active, and the number of posts each account made. An early observation made was that the majority were activated between Mondays and Fridays, and usually before 12:00 UTC.

The u/gregoratior account's patterns of behaviour were unique and substantively different from the others (the sole Type A account). Potentially this is because it was the only one dealing with apparently genuine (not forged) documents. The account itself was created in 2017 and remained dormant for two years, until it began to comment and post as a normal user on Reddit may do. The account engaged in a variety of subreddits and posts, along with posting a small number of memes in an apparent attempt at "karma farming"; to gain reputation on the site ahead of its operational activation.

The majority of the 61 accounts were 'burner accounts' (categories C to E), only active over a period of a few hours at most (average of 56mins 25secs between creation and last posting). Each of these posted a single article across one or more subreddits either as a "self-post" (where the text is posted directly as the subject), a link to an external blog site (homment[.]com, buzzfeed[.]com, indybay[.]org, medium[.]com), or as a comment to another article. There are two accounts that fall under the Type B category. These generally exhibited the same behaviour as Type D and E accounts, the difference being that they were active on a second day propagating a second article.

There were also a large proportion of 'Type F' accounts with no posting or comment history at all. All but one of these were created on 21st Oct 2019, coinciding with the posting of the official-sensitive documents by u/gregoratior. This implies that they were purely created for the purposes of amplification of the post.

CONTENT ANALYSIS

Fifty accounts submitted content across 81 subreddits. Each of the subreddits posted to was categorised by geographical location (Europe, Americas, US, Africa) and type (discussion forum, technology focused, country focused).

Reddit comprises thousands of subreddits, moderated by volunteer members of the online community. Levels of tolerance for content varies between subreddits, with some being very actively moderated and restrictive to maintain the focus of a subreddit. Others are much more open in how they are managed. Some common reasons for posts being removed from subreddits are that they are considered "off topic" (not relating to the subreddit), inflammatory (posted in bad faith), or the post is of low quality. Of the 180 posts made by the suspect accounts, 78 had been deleted by moderators.

Type	Username	Created DD/MM/YYYY	Day	Hour UTC	Posts	Comments	Creation Lag DDD HH:MM:SS	Operative Time DDD HH:MM:SS	Language	Operation Window
D1	KimJjj	01/02/2017	Wed	10	5	0	000 00:07:25	000 01:04:29	English	OPERATION 1
D2	CharlesRichardson	02/02/2017	Thu	8	3	0	000 00:03:27	000 00:28:03	French	OPERATION 1
D1	SherryNuno	20/02/2017	Mon	13	3	0	000 00:29:04	000 01:00:47	English	OPERATION 1
D1	PushyFrank	27/02/2017	Mon	8	4	0	000 00:19:01	000 01:35:14	English	OPERATION 1
D1	BillieFolmar	27/02/2017	Mon	8	6	0	006 23:46:46	007 01:03:25	English	OPERATION 1
D1	demomanz	10/04/2017	Mon	9	9	0	000 00:10:57	000 02:07:50	English	OPERATION 1
D1	alabelm	20/04/2017	Thu	9	5	0	000 00:06:15	000 01:10:58	English	OPERATION 1
D1	rabbier	29/04/2017	Sat	8	6	0	000 00:24:16	000 03:24:33	English	OPERATION 1
A	gregoratior	04/05/2017	Thu	13	6	17	860 20:26:25	920 19:09:40	English	OPERATION 1
D1	Ritterc	06/05/2017	Sat	9	7	0	000 00:06:02	000 02:18:42	English	OPERATION 1
D1	PeterMurtaugh	11/05/2017	Thu	9	9	0	000 00:10:30	000 03:00:35	English	OPERATION 1
E1	HarrisonBriggs	23/05/2017	Tue	9	1	0	000 00:52:53	000 00:52:53	English	OPERATION 1
C	Rinzoog	26/05/2017	Fri	11	0	1	000 00:00:23	000 00:00:23	English	OPERATION 1
C	MikeHanon	26/05/2017	Fri	11	0	1	000 00:02:13	000 00:02:13	English	OPERATION 1
D1	KlausSteiner	06/06/2017	Tue	10	8	0	000 00:21:06	000 02:25:26	English	OPERATION 1
D1	krakodoc	07/06/2017	Wed	8	9	0	000 00:05:01	000 02:13:40	English	OPERATION 1
D1	fullekyl	29/07/2017	Sat	10	5	0	000 00:01:41	000 01:25:24	English	OPERATION 1
E2	uzunadnan	29/08/2017	Tue	13	1	0	000 00:19:54	000 00:19:54	French	OPERATION 2
D2	LauraKnecht	27/09/2017	Wed	11	4	0	000 00:04:49	000 00:45:54	German	OPERATION 2
D2	lauraferrojo	28/09/2017	Thu	9	5	0	000 00:11:00	000 01:10:27	Spanish	OPERATION 2
E1	TomSallee	28/09/2017	Thu	9	1	0	000 00:08:46	000 00:08:46	English	OPERATION 2
D2	NicSchum	12/10/2017	Thu	12	3	0	000 00:04:26	000 00:33:17	German	OPERATION 2
D2	brigittemaur	01/11/2017	Wed	7	4	0	000 00:11:47	000 00:51:41	German	OPERATION 2
D1	MilitaryObserver	10/11/2017	Fri	10	2	0	000 00:09:01	000 00:19:49	English	OPERATION 2
E1	RuffMoulton	13/11/2017	Mon	13	1	0	000 00:16:10	000 00:16:10	English	OPERATION 2
D1	kempnaomi	24/11/2017	Fri	9	2	0	000 00:01:53	000 00:19:16	English	OPERATION 2
E2	MaxKasyan	29/11/2017	Wed	10	1	0	000 00:08:03	000 00:08:03	Ukrainian	OPERATION 2
B	davecooperr	06/12/2017	Wed	9	2	0	000 00:10:24	000 23:14:40	English	OPERATION 2
E1	LuzRun	07/12/2017	Thu	11	1	0	000 00:04:25	000 00:04:25	English	OPERATION 2
D2	jaimeibanez	21/12/2017	Thu	7	7	0	000 00:07:34	000 01:16:04	Spanish	OPERATION 2
E2	bernturmann	21/12/2017	Thu	10	1	0	000 00:04:59	000 00:04:59	German	OPERATION 2
D2	blancoaless	25/12/2017	Mon	7	2	0	000 00:09:44	000 00:21:15	Spanish	OPERATION 2
D2	almanzamary	09/01/2018	Tue	7	8	0	000 00:11:12	000 01:32:08	Spanish	OPERATION 2
B	delmaryang	21/03/2018	Wed	11	8	0	000 00:11:56	015 02:27:42	English	OPERATION 2
D2	estellatorres	27/07/2018	Fri	7	6	0	000 00:01:59	000 00:56:42	Spanish	OPERATION 2
F	EllisonRedfall	01/08/2018	Wed	10	0	0	000 00:00:00	000 00:00:00	None	OPERATION 2
D2	chavezserg	09/08/2018	Thu	7	6	0	000 00:05:20	000 01:16:30	Spanish	OPERATION 2
D2	bellagara	10/08/2018	Fri	7	4	0	000 00:07:15	000 00:44:55	Spanish	OPERATION 2
D2	francovaz	16/08/2018	Thu	8	5	0	000 00:12:17	000 00:56:54	Spanish	OPERATION 2
D2	claudialopezz	22/08/2018	Wed	9	6	0	000 00:13:08	000 01:32:39	Spanish	OPERATION 2
E1	garrypugh	29/08/2018	Wed	11	1	0	000 00:06:07	000 00:06:07	English	OPERATION 2
D2	gilbmedina84	26/02/2019	Tue	7	7	0	000 00:06:23	000 01:36:15	Spanish	OPERATION 2
C	McDownes	28/03/2019	Thu	13	0	1	000 00:01:10	000 00:01:10	English	OPERATION 2
E1	robeharty	22/04/2019	Mon	8	1	0	000 00:05:42	000 00:05:42	English	OPERATION 2
D2	AntonioDiazz	24/04/2019	Wed	8	2	0	000 00:24:56	000 01:00:47	Spanish	OPERATION 2
E2	zurabagriashvili	09/10/2019	Wed	8	1	0	000 00:09:56	000 00:09:56	Russian	OPERATION 2
E2	Defiant_Emu	21/10/2019	Mon	9	1	0	000 00:17:34	000 00:17:34	Russian	OPERATION 2
F	PastJournalist	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	MaryCWolf	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	StevtBell	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	victoriasanches	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	FeistyWedding	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	Party_Actuary	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	ZayasLiTel	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	davidjglover	21/10/2019	Mon	14	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	vasiliskus	21/10/2019	Mon	15	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	feliciahogg	21/10/2019	Mon	15	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	ciawahhed	21/10/2019	Mon	19	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
F	saliahwhite	21/10/2019	Mon	19	0	0	000 00:00:00	000 00:00:00	None	OPERATION 3
E2	Ostermaxnn	23/10/2019	Wed	9	1	0	000 00:38:39	000 00:38:39	German	OPERATION 3
C	KattyTorr	29/10/2019	Tue	7	0	1	000 00:08:35	000 00:08:35	English	OPERATION 3

Table 3: Account Classification and Operational Activity Window

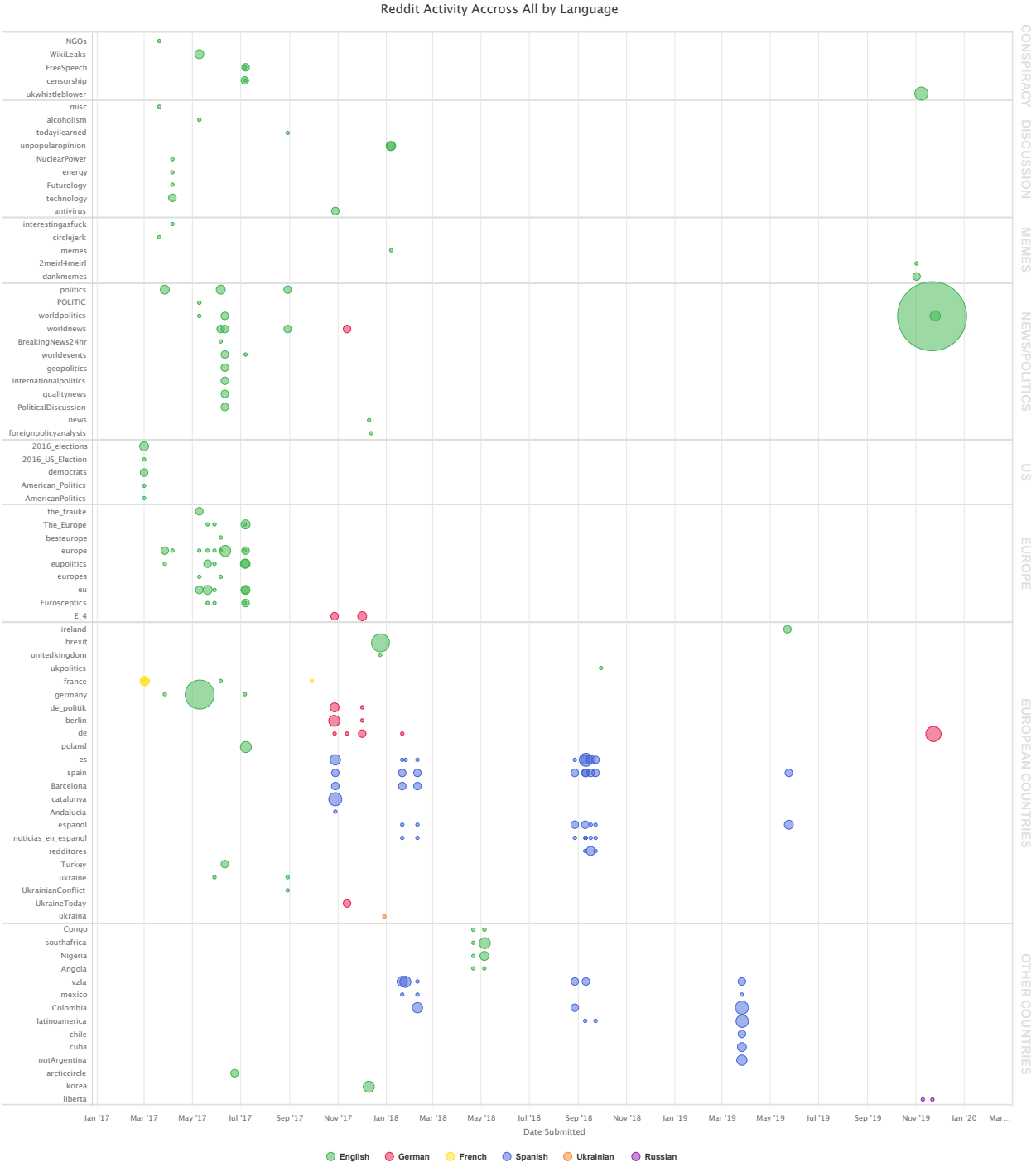


Figure 2: Posts by Language across Subreddits

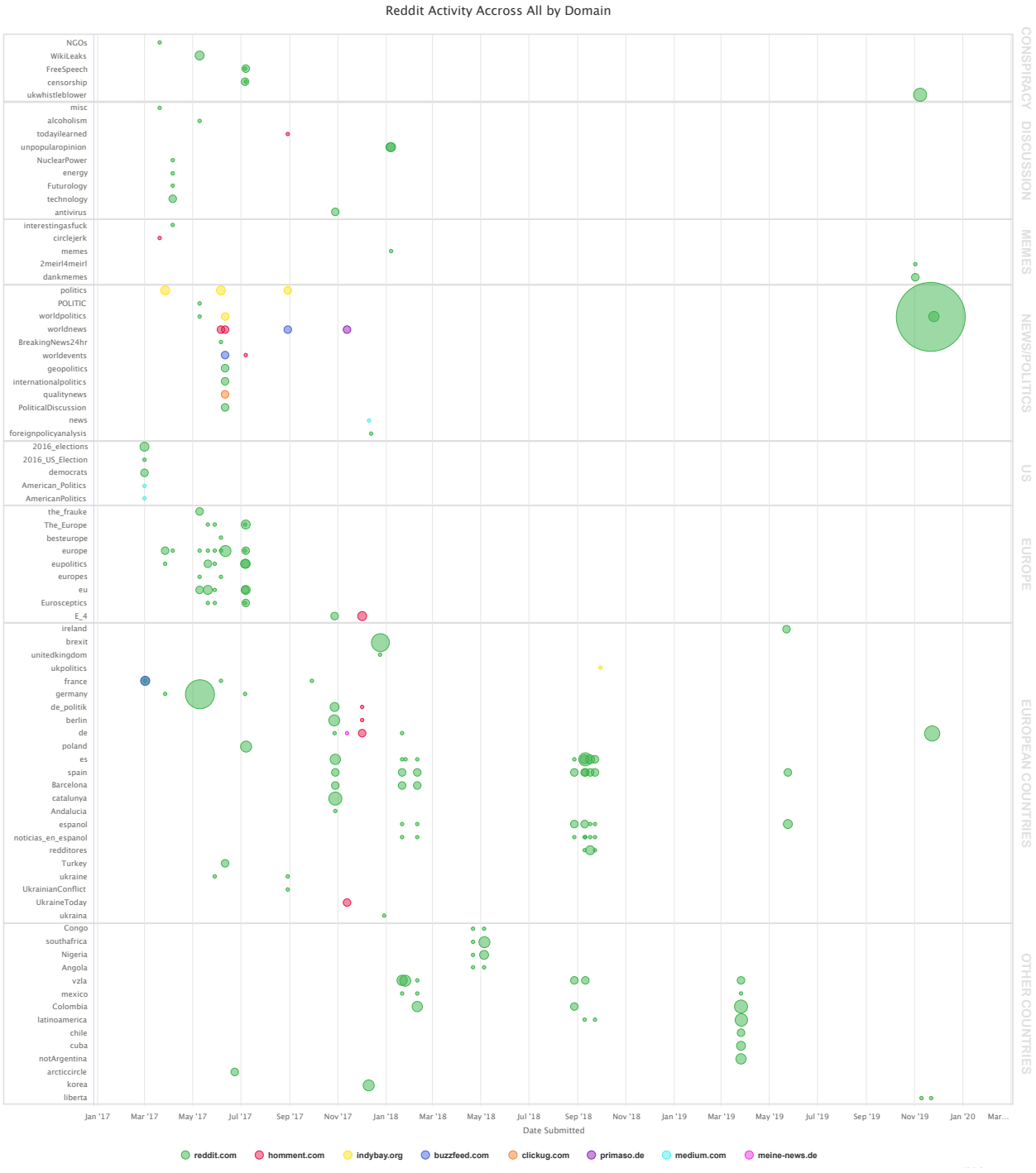


Figure 3: Posts by Domain across Subreddits

Country	The main country discussed in the post. This is not necessarily the country that the subreddit a post is submitted to.
Subject	The main subject covered in the post. E.g. a political leader, deep state, civil unrest.
Message	The main message that is being put across in the post. E.g. corruption of lead-ership, election meddling, western interference.
Method	The writing style present in the post. E.g. rumouring, presenting an alternate explana-tion, factually reporting.
Tone	The tone expressed by the author. E.g. lecturing, scandalous, speculative.
Type	How the information is presented. E.g. with a supporting document released, linking through or reposting a blog, postulating via a "self post".
Language	The language used in the post.

Table 4: Reddit Post Schema

The post histories for all the accounts highlighted by Reddit were gathered and assessed, using the categories in Table 4. These were then mapped onto a number of scatter-graphs that plot posts to subreddits against time (see Figure 2). We clustered the subreddits based upon the main focus of discussion (country or topic focused). The magnitude of each post reflected the number of comments made. The majority of submissions targeted European based subreddits (both Europe wide and country specific) or site wide news, politics, discussion and conspiracy focused subreddits.

As depicted in Figure 2, a shift in the use of both language and target audience over time indicates a significant evolution of focus, with the empirical data suggesting three distinct operational phases.

OPERATION 1 - 2017

This was the most active operational mode, spanning 2017 and consisted primarily of accounts that were predominantly of type D1 and C.

The initial posting style was confrontational and mainly focused on personal attacks on western leaders, their political decisions, character and interests. Content was often hyperbolic, sarcastic or mocking of a country's current situation. There was a modest US focus at the beginning of the period, but that quickly shifted to focus on European leadership. Election meddling by immigrants/non-local voters was a common trope found within this set of articles.

Of note, is that a number of posts were supported by multiple copies of the same article posted to third-party blogging sites (homment[.]com, buzzfeed[.]com "community" pages, indybay[.]org and medium[.]com) which can be observed in Figure 3. These were primarily English language messages and posted to wide interest subreddits, with the reddit "self post" versions spread across a mix of country specific and general interest subreddits. Articles were often supported with satirical or alarmist imagery (photographs, graphics and cartoons). This operation was the most regular of the three, with multiple articles posted each month.

OPERATION 2 – 2017 TO 2019

August 2017 saw the emergence of more Type D2 and E2 foreign language (French, German, Spanish and Ukrainian) posters that form the core of the second operational mode. Critically, their activity focused more upon releasing 'leaked/hacked' documents, with supporting text used to emphasise key elements of the claimed conspiracy or scandal. Few involved posting to 3rd party sites. Most of the effort was on Reddit, but followed a similar style to other document leaks found on the third-party blogging sites. This involved posting images of the government documents, accompanied by a conspiratorial or scandalous interpretation of what the document contains.

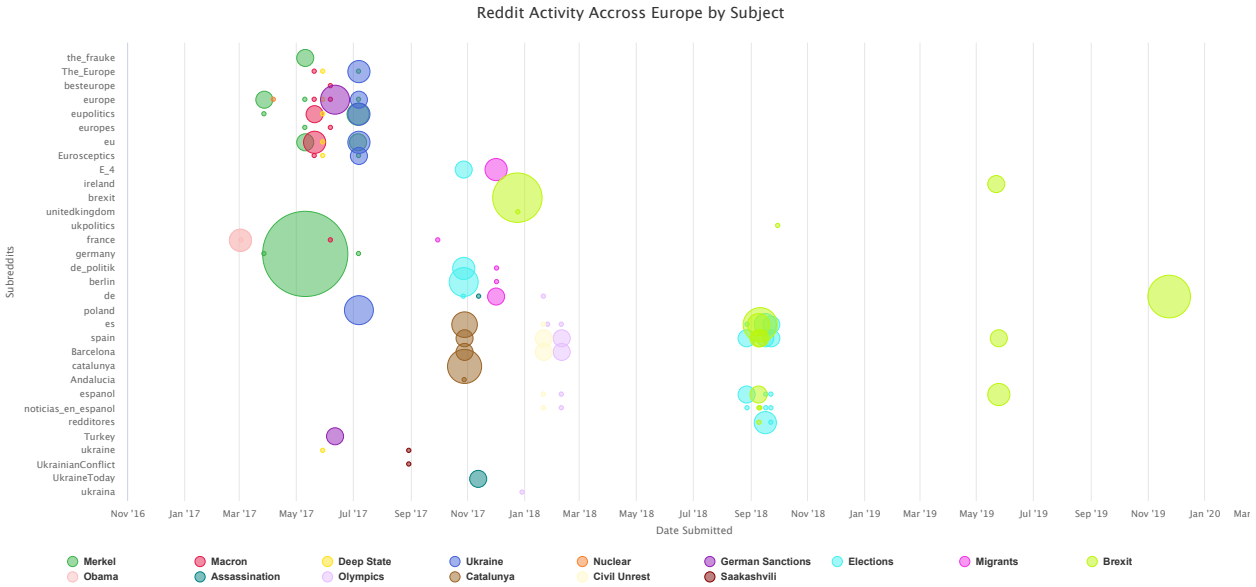


Figure 4: Posts by Subject across European focused Subreddits

Initially, the non-English language messages focused on conspiracies around tensions within the EU, such as the EU's support for Catalonian independence and election meddling through the use of migrants. There then followed a series of posts targeting the Winter Olympics in South Korea (bleeding into Jan 2018). These either promoted a conspiracy that the Olympics was cover for a South Korean invasion of North Korea, or suggesting that the Olympic games will be unsafe with attendees raising concerns and that Western powers are ignoring these risks for the sake of profit. Towards the end of 2017/early 2018 there was a noticeable drop off in the variety of subreddits targeted.

Figure 4 provides a representation of the focal subjects present in the posts submitted to the European focused subreddits. It shows the shift in the content of posts from attacking political leadership and policy, to focusing on election meddling and seperatist movements (Catalan independence and Brexit) in 2018/19, where activity was much more concentrated to specific months, with two large multi-month gaps in activity, and a lack of D1 and E1 posting (see Figure 2).

The majority of the document release posts during this period were targeting Spanish language subreddits. 'Brexit' was also a topic of interest, with two Spanish language posts in August rumouring an assassination attempt against Boris Johnson and an alleged email leak between Arlene Foster and Michael Barnier over the Northern Ireland border. There was also an English language third-party post to an indybay[.]org article "British border guards threaten to close their customs points along the border with the EU" [6], but this was subsequently removed.

To extend the analysis, we recorded all the document release images still accessible, looking at which organisations the communications were sent between, and the general subject of the 'leaked/hacked' documents (see Table 5). The vast majority were focused upon Western (mainly EU) interests, centred around geopolitical stress points (Ukraine, Brexit, Venezuela, Far Right parties). In the majority of cases, the language of the document differed to the language used in the post. An explanation for this is that it creates a barrier of understanding for any reader, who may consequently rely more heavily on the accompanying interpretation of the document, rather than reading it themselves. The documents were all uploaded to image hosting sites that strip EXIF data on upload, meaning original creation information is lost.

Whilst the majority of posts in this operation window were non-English, there were two instances where an account made a post on more than one day (u/davecooperr, u/delmaryang), both of which were English language posters. This suggests that there were attempts by the operators in this phase to see whether serial posting had a different effect on target audiences.

The first of these accounts posted two separate "self-posts" (blog posts on the Reddit site) on concurrent days in December 2017 on the r/unpopularopinion subreddit. The messages centred different subjects each day, but adopted the same conspiratorial tone (NATO was built to undermine Russia, and Turkey has been driven away by Europe and

6 https://www.indybay.org/newsitems/2018/08/29/18817191.php

Document	Post Author	"Post Date DD/MM/YYYY"	Post Lang	Doc Lang	"Doc Dated DD/MM/YYYY"	"Post Lag DDD HH:M-M:SS"	Subject	From/To
DOC001	PeterMur-taugh	11/05/2017	English	English	20/04/2017	021 00:10:30	EU	"F: Alliance for Shared Values (Turkey) T: Head of Federal Chancellery (Germany)"
DOC002	KlausSteiner	06/06/2017	English	German			Military	
DOC003	lauraferrojo	28/09/2017	Spanish	Spanish	25/09/2017	003 00:11:00	EU	"F: Secretary of State for Territo-rial Administrations (Spain) T: Vice President (Catalunya)"
DOC004	jaimeibanez	21/12/2017	Spanish	Ukranian	27/11/2017	024 00:07:34	NATO	"F: National Security and De-fense Council (Ukraine) T: Prime Minister (Ukraine)"
DOC005	blancoaless	25/12/2017	Spanish	German	19/12/2017	006 00:09:44	Olympics	"F: Sports Federations (Germany) T: Olympic Sports Confederation (Germany)"
DOC006	estellatorres	27/07/2018	Spanish	English	10/07/2018	017 00:01:59	EU	"F: Vice Chancellor (Germany) T: People's Democratic Party (Turkey)"
DOC007	chavezserg	09/08/2018	Spanish	Spanish	01/08/2018	008 00:05:20	Brexit	"F: Ministry of Foreign Affairs (Spain) T: Interior Comminssion Presi-dent (Spain)"
DOC008	bellagara	10/08/2018	Spanish	English	30/07/2018	011 00:07:15	Brexit	"F: Democratic Unionist Party (UK) T: Brexit Negotiation Team (EU)"
DOC009A	claudialo-pezz	22/08/2018	Spanish	English	02/08/2018	020 00:13:08	SDP	"F: Secretary of State (USA) T: Foreign Affairs (Poland)"
DOC009B	claudialo-pezz	22/08/2018	Spanish	French	08/08/2018	021 00:06:07	SDP	"F: Le Front National (France) T: Sweedish Democrats Party (Sweden)"
DOC010	gilbmedi-na84	26/02/2019	Spanish	English	20/02/2019	006 00:06:23	Venezuela	"F: USAid (Colombia) T: Interim President (Venezuela)"
DOC011	robeharty	22/04/2019	English	Arabic Script	18/04/2019	004 00:05:42	Brexit	"F: RealIRA T: Islamic State"
DOC012	AntonioDiazz	24/04/2019	Spanish	Arabic Script	18/04/2019	006 00:24:56	Brexit	"F: RealIRA T: Islamic State"

Table 5: Date, Content and Language of 'Document Leak' images

seeks a stronger alliance with Russia). It is salient that they were quite targeted, rather than blanket posting.

Contrastingly, the second account did blanket post across subreddits (r/congo, r/southafrica, r/angola, r/southafrica) on two separate occasions a month apart (March and April 2018). Again only posting within the site and not linking out. The two posts were serial in that the second post linked back to the same text via a medium[.]com link[7], and covers alleged CIA influencing in Africa. Interestingly, the medium[.]com posts were never directly posted to Reddit.

In 2019 activity reduced further. A possible interpretation of this trajectory is a strategic shift to other platforms and / or concentrating on more focused releases. Another Brexit related narrative was posted in February two days apart by two accounts (u/robeharty in English to the r/Ireland subreddit and u/AntonioDiazz in Spanish to the r/spain and r/espanol

7 https://web.archive.org/web/20191111121510/https://medium.com/@delmaryang/liberian-friend-informs-langley-89d36f0309a3 via Way-Back machine

subreddits), presenting the same screenshot purporting to be the Irish Republican Army attempting to recruit Islamic State fighters.

OPERATION 3 – 2019

In late 2019 there was a significant shift in operational focus and tempo. This phase was wholly focused around the release of the official-sensitive documents by u/gregoratior. It engaged: the original account (created back in 2017, but not active until 2019); the bulk of the Type F accounts created on the day of posting, presumably for the sole purpose of amplifying the document leak via "upvoting" the post; and a small number of C to E accounts that amplified the post by linking back to the document release.

The u/gregoratior account operated for a few days before the leak posting some memetic content, possibly as a karma farmer (trying to leverage reputation) before setting up the r/whistleblower subreddit and then leaking the UK documents. The u/gregoratior account made one final post a few days later, possibly attempting to bait people into clicking on his profile and finding their way back to the leak. Supporting actions were performed by the u/Ostermaxnn account who's only post was in German linking directly to the leak post.

RELATIONS BETWEEN OPERATIONS

Framed in this way, Op1 and Op2 represented an evolution of tactics and targets, shifting from high frequency posting to the Anglosphere focused on discrediting world leaders, to more sophisticated document releases to non-English communities seeking to undermine the credibility of the EU/NATO. The fact that the posting frequency deteriorated during 2018, maybe implies there were diminishing returns being generated by this strategy.

Op3 was significantly different however from its predecessors. It was solely focused upon the release of a single set of documents. The single use burner accounts (Type F) that amplified the u/gregoratior post were created between 14:00 and 15:10 UTC at roughly 10-minute intervals, suggesting a manual rather than automated effort. There was then a gap, before two more accounts were created at 19:00 UTC. It is feasible that during the gap in Type F creation, the original accounts relating to Op1 and Op2 were retrieved and used to amplify as a short-cut to obtaining accounts that could amplify the u/gregoratior post. It suggests that these documents were considered to be much more valuable than anything posted in Op1 and Op2, to the point that it was deemed acceptable to "burn" the accounts present in Op1 and Op2 for the benefit of Op3, leading to them all being identified by Reddit and released for academic scrutiny.

Having set out the broad patterns of activity associated with these accounts; we now shift to explore some of the content they disseminated. Using the same unusual combination of sites employed in the Brexit leaks (and also in Latvia according to DFRLabs)[8], as a kind of 'behavioural signature', we have discovered a further campaign that involved 'seeding' leaked or forged documents on the Homment platform, before spreading them via Reddit and other social media platforms.

POLISH CASE STUDY: SMEARING JAROSLAW KACZYNSKI

In 2016 the operators running the Reddit accounts manufactured a narrative that the high profile Polish politician Jaroslaw Kaczynski (Leader of the Law and Justice Party, former Prime Minister and brother of the former President) was afflicted by the hereditary disease Fragile X Syndrome. Fragile X Syndrome symptoms include a severely reduced IQ, 'psychopathic disturbances' and facial structure changes. The narrative was used to suggest that the difficult relations between Poland and Germany (and therefore the EU) were being caused by the former being led by a dangerous leader.

Table 6 below provides a brief timeline of the key events and developments regarding this narrative becoming

8 https://medium.com/dfrlab/lingering-infektion-latvian-operation-mimicked-secondary-infektion-tactics-bc0bb62eacaa

public.

Table 6: Timeline of key events regarding Kaczynski campaign

Date	Events
20-Feb-2016	'Proof' is provided by an account purporting to be a German MP on Medium, Homment and Indy-media.
21-Feb-2016	Comments sharing a link to the story are made on two Polish websites, Reddit and the Economist.
22-Feb-2016	'JoseFever' writes an article on BeforeItsNews.com and a comment is left on blogspot.
24-Feb-2016	'JoeHashever' writes an article on Indymedia. An article is posted on a Swedish news site. A peti-tion is created on the site Avaaz calling for the EU to carry out a public health test on Kaczynski.
25-Feb-2016	The same author writes articles on five different Ukrainian websites in a short amount of time, pro-moting this narrative.
26-Feb-2016	An article is submitted in Portuguese to a Portuguese website.
03-Mar-2016	Comment is submitted to Polish forum, expressing outrage about the story and sharing the link.
12-Apr-2016	The campaign is rebooted. An account claiming to be a different German MP uploads an article to Medium, Homment and IndyMedia.
19-Apr-2016	A burner account uploads a video ostensibly from the hacker group Anonymous to Vimeo.
05-May-2016	An answer is submitted to Quora that includes nearly every link/source in this timeline. This is the account's only answer.

The key claim can be traced to German MP Sabine Boeddinghaus. On the 20th February she authored two articles in her name on the Medium and IndyMedia platforms. As proof of the central allegation, she included scans of a document (in Russian) from the Russian Academy of Sciences, dated September 2010, that she claims are genetic test results on the body of Jaroslaw's identical twin brother Lech. Lech, who was Poland's leader at the time, died when his plane crashed in Russia in 2010. Also included was a translation of this document into English.

Other evidence presented was a screenshot, purporting to show Boeddinghaus' attempts to contact two leading Polish geneticists with this information. The screenshot shows a Web.De club email address in her name (instead of her official MP account), with the email written in English. The email was sent to two addresses that are publicly available on the geneticist's respective webpages.

Sabine Boeddinghaus' Twitter account has been active since July 2015. However, she had never previously made reference to these two articles that she was apparently so desperate to share. In fact, she had never mentioned Kaczynski or Poland on her Twitter account. Consequently, we infer that Boeddinghaus has been the victim of identity fraud by persons unknown, promoting this disinformation campaign using spoof accounts created in her name.

20th – 22nd February 2016

The campaign began on 20th February 2016 with the two articles attributed to Sabine and one anonymous Homment piece. The latter contained the same text as the other articles. The first phase of activity involved publicising these articles by posting comments on other websites. In the following two days, six comments were posted on six different websites. Three used links to the Homment article and three to the Medium article; all were left on old news stories about Poland. For example, the Reddit post that was commented upon was 81 days old at the time, meaning a user would be highly unlikely to come across it by accident or chance, as it would be submerged by Reddit's algorithm. A plausible inference, therefore, is that all these posts were made by one individual. 'JoseFever' authored an article on the beforeItsNews website, known for sharing conspiratorial stories. He had published 68 stories between April 1st 2015 and July 27th 2016.

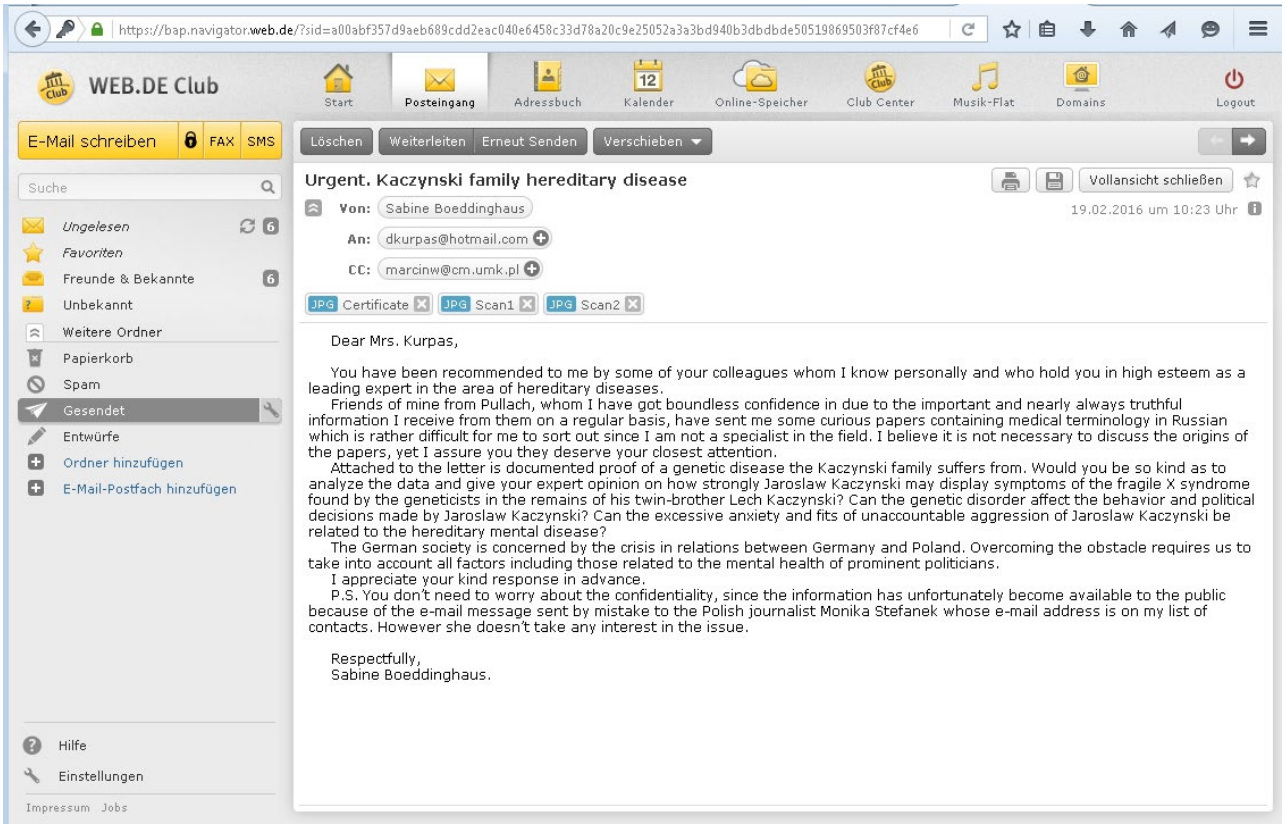


Figure 5: Screenshot from Medium and IndyMedia articles

24th – 26th February 2016

Phase 2 began with a petition on the Avaaz website. The petition aimed to get the European Commission to conduct a public health examination of Kaczynski, based on the allegations outlined above. The petition was only signed by 30 people. However, this new 'development' did accompany eight new articles targeting readers in Portugal, Sweden, the UK and Ukraine.

3rd March 2016

The campaign then went silent for a week before 'john_tucker' commented on a Polish forum. His technique was the same as the other commenters - posting the Homment link and 3 links to Imgur. However, his narrative was different, expressing outrage about the 'scandal' that the Russians have examined the remains without permission from the relatives. That said, in doing so, he revived the thread (about the possibility that Lech Kaczyński's plane was taken down with a bomb), with 19 new comments appearing that month. However, none discussed his comment.

12th – 13th April 2016

Based upon what we have seen in other campaigns, this should have been the end of it. However, the operators appeared to try to 'reboot' this narrative a month later on 12th April using exactly the same method. This time however they chose a German MP named Volker Kauder to attribute their Medium and IndyMedia articles to. The operators also created an anonymous Homment post as before, along with a post on CyberGuerilla.org, which is known for hosting documents from the hacktivist group Anonymous. It appears they managed to mislead the owners there. There is now a comment from a moderator on CyberGuerilla.org to this effect, stating they have been duped by these false documents. A day later someone posted an article on a Ukrainian website, ostensibly about Polish border disagreements, but in reality using it to promote this narrative.

19th – 26th April 2016

One week later, a video was posted to popular sharing site Vimeo. The video was professionally edited and supposedly from the group Anonymous. It included a link to the CyberGuerilla website in the description. The following day three LiveJournal accounts shared this narrative, one of which is very popular and may be a genuine believer in the story. Roughly another week passed, and two further articles were created on IndyMedia and Medium, this time under the name 'MonRoe'/'MonRo'. Importantly, the focus here was ostensibly defending Kaczyński from these lurid attacks by liberals. For evidence, the authors used screenshots of an article supposedly published on the website of The Warsaw Voice, that the author managed to obtain before it was 'taken down'. This was followed by another IndyMedia article including links to nearly every other site featuring in the campaign, including obscure ones such as one written in Portuguese. From an 'operational security' perspective, this represents poor 'tradecraft'.

Figure 6 maps the interactions between the posts and articles that the operators of this campaign created. This clarifies that the content created under the name of German MP Volker Kauder was never linked to. Similarly, the IndyMedia article in the name of Sabine was also never linked to, and the Medium article written in her name was only linked to three times. This raises a question about 'why go to the trouble of creating this content and then not linking to it?' That said, the original Homment article and the Imgur links to the documents were used extensively.

However, this campaign was not the only one the operators were working on during the February – May 2016 period. The next case study implies that some of the mistakes highlighted above could be explained by the operators running simultaneous different operations.

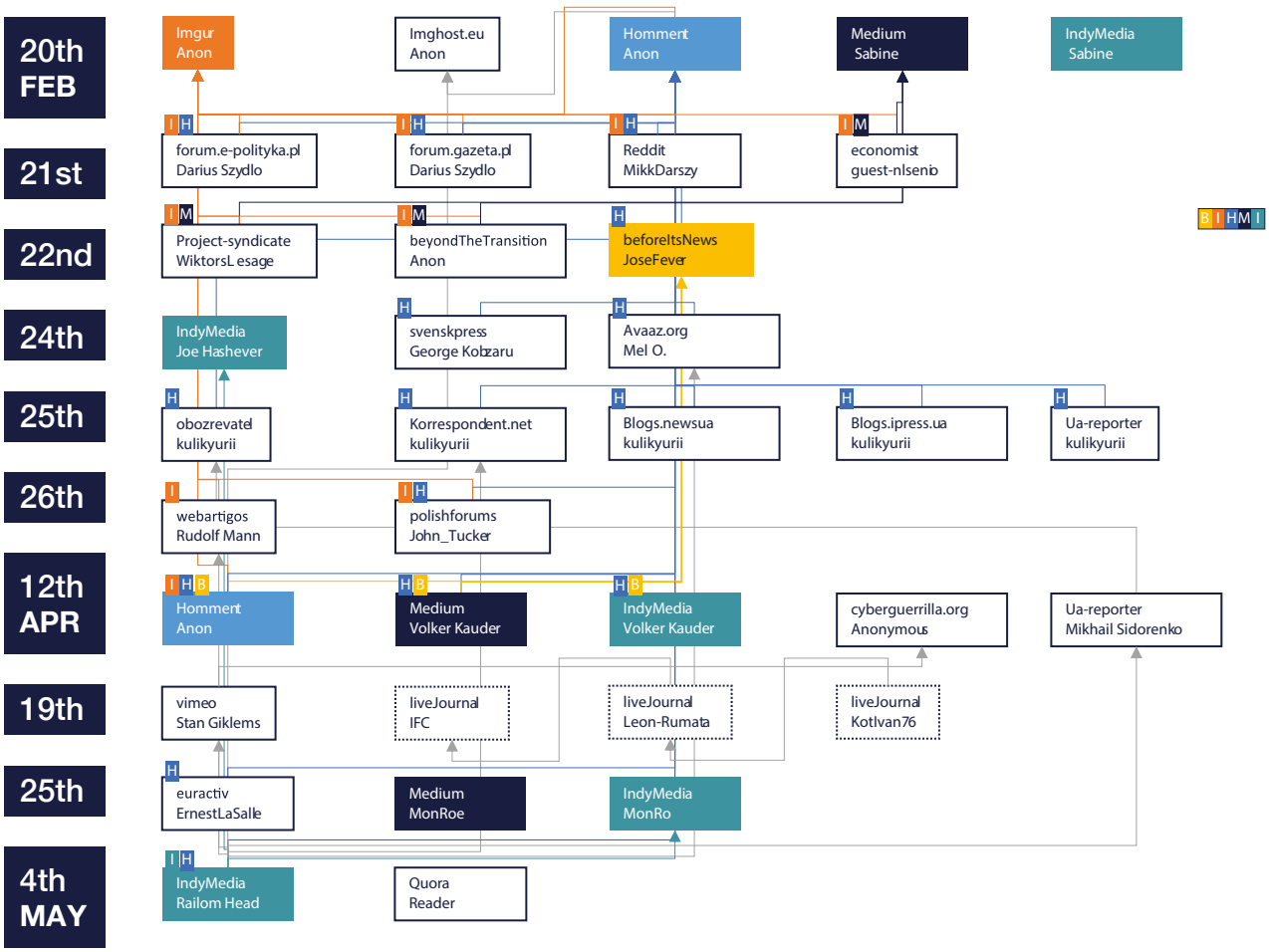


Figure 6: Map of Cross Links

THE CASE OF TWO QUORA COMMENTATORS

On the 5th May 2016 an account named 'Reader' submitted an answer to the question 'Has Poland become a dictatorship in 2016?' on the platform Quora[.]com. His answer included links to nearly every 'source' listed above and was his only answer submitted to the site, indicating that he was probably part of the operation. The original question was posed by an anonymous user and first answered by an account saying: "More and more questions and variations of this question on Quora, seems like an organized action". Quora is a popular American question and answer site that is known for having questions answered by high profile individuals such as President Barack Obama and Facebook COO Sheryl Sandberg. Upon further investigation of the site we found multiple accounts that appeared dedicated to increasing friction between countries, usually in Eastern Europe.

Two 'spoofed' accounts, active on multiple sites amplifying the disinformation narrative described above were identified. Unlike the majority of other accounts in this campaign that were typically 'burner' accounts, these two stayed active and had extensive 'backstories'. With regards to this campaign, Josef answered the question 'Can Poland destroy the EU?' with a link to the documents on Homment. Steven answered the question 'What is the current state of Poland?' with links to many of the sources shown in Figure 6, as well as directly uploading the documents to Quora. Table 9 summarises their activities.

Identity	Steven Laack	Josef Hashever
Answers	26	29
Questions	1	1
Followers	3	4
Following	11	
Edits	43	38
First Post	October 16th 2015	October 20th 2015
Last Post	June 8th 2016	June 10th 2016
Content viewed by	31,600 people	21,400 people
Twitter account	Yes	Yes
Blogspot Website	Yes (June 2014 – June 2016)	Yes (December 2015 – August 2016)
Facebook	Maybe	Yes
Google Plus	Yes (118394627822760465663)	

Table 7: Alias account activity

Steven Laack's biographical information on both Quora and Twitter contains examples of non-native English use: "saying white when see white, saying black when see black" and "just a happy man, proud to be American but unhappy to be US taxpayer, a patriot to this country, freeminder and politics of no bullshit lover". However, Steven claims to be an 'immigrant from Sweden' so that might explain his non-native English use.

Figure 7 on the following page, contains two similar images. On the left is Steven Laack's profile picture on Twitter and Quora. The image on the right was used by "Glazychev Anton Stepanovich" on profi-lex.ru.

Figure 7: Steven Laack Image Comparison

We judge the image on the right to be the original because of three factors. It is higher quality, containing more pixels. It contains more of the original scene, including details of the roof and his knuckle that cannot be seen on the Steven Laack image. Finally, the individual's shirt is blue. On the 'Steven Laack' image the shirt colour has been changed to burgundy, we can tell this by comparing the lapel, the burgundy shirt has a green 'artefact' from the colour changing process. The flipping, lower quality, cropping and colour adjustment were likely all performed in an attempt to make the image harder to reverse image search. It appears likely that the operators stole this profile picture from the user on profi-lex.ru and edited it for their own ends.

Josef Hashever is a name mentioned in the previous case study. On 24th February 2016 that name published an article on IndyMedia entitled: 'European unity is being undermined by a retarded politician'. A day before that "JoseFever" had posted an article with the same name on the website beforeItsNews.com. That account has published 68 stories between April 1st 2015 and July 27th 2016, which is very similar to the timeframe that the Josef Hashever Quora account was active. Josef Hashever also featured in the Vimeo video purportedly made by the hacktivist group Anonymous. Details from that video identify his Facebook, Twitter and blog (lunaticJoe.blogspot, very similar to his Twitter username), although he did not have any biographical information on any of his accounts.

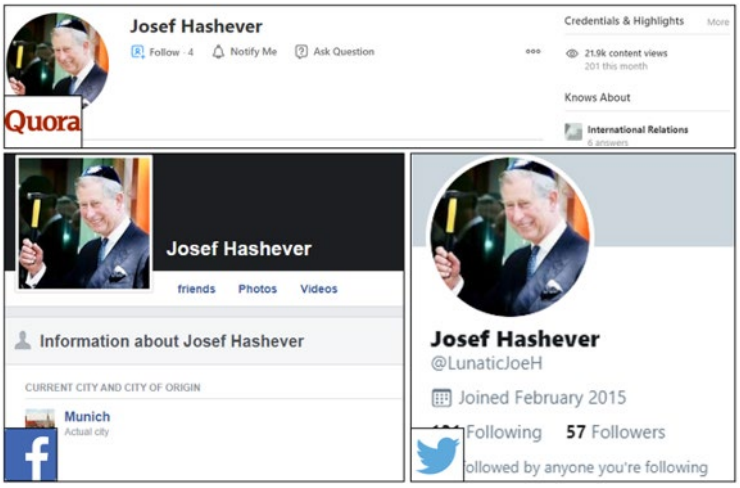


Figure 8: Screenshots of Josef Hashever accounts

Comparing the Twitter accounts of Josef and Steven we can see they share one follower in common. This Twitter account is active in the same general time period (May 2014-July 2016). Josef also has a Medium account where he has written one article. In this article he used a leaked/hacked document from USAid that implies that NGOs are recruiting people from post-Soviet states to fight for ISIS and that unfortunately the US has lost control of these fighters. This document can also be found on Homment, in a German language article posted three days after the Medium article.

On Quora the two accounts have strikingly similar activity, but rarely answer the same questions. For example, Steven answered:

> *"What impact could the Panama Papers have had on the Dutch Ukraine-EU Association Agreement referendum results?"*

Whereas Josef answered:

> *"Is Netherlands' overwhelming rejection of Ukraine association agreement yet another confirmation of how undemocratic the EU has become?"*

Both of their replies link to Medium articles. The article Steven links to (@MekitsonDuo) is under investigation by Medium, but Josef's link is still active. It was posted by '@Stepp81' who has only ever posted that article.

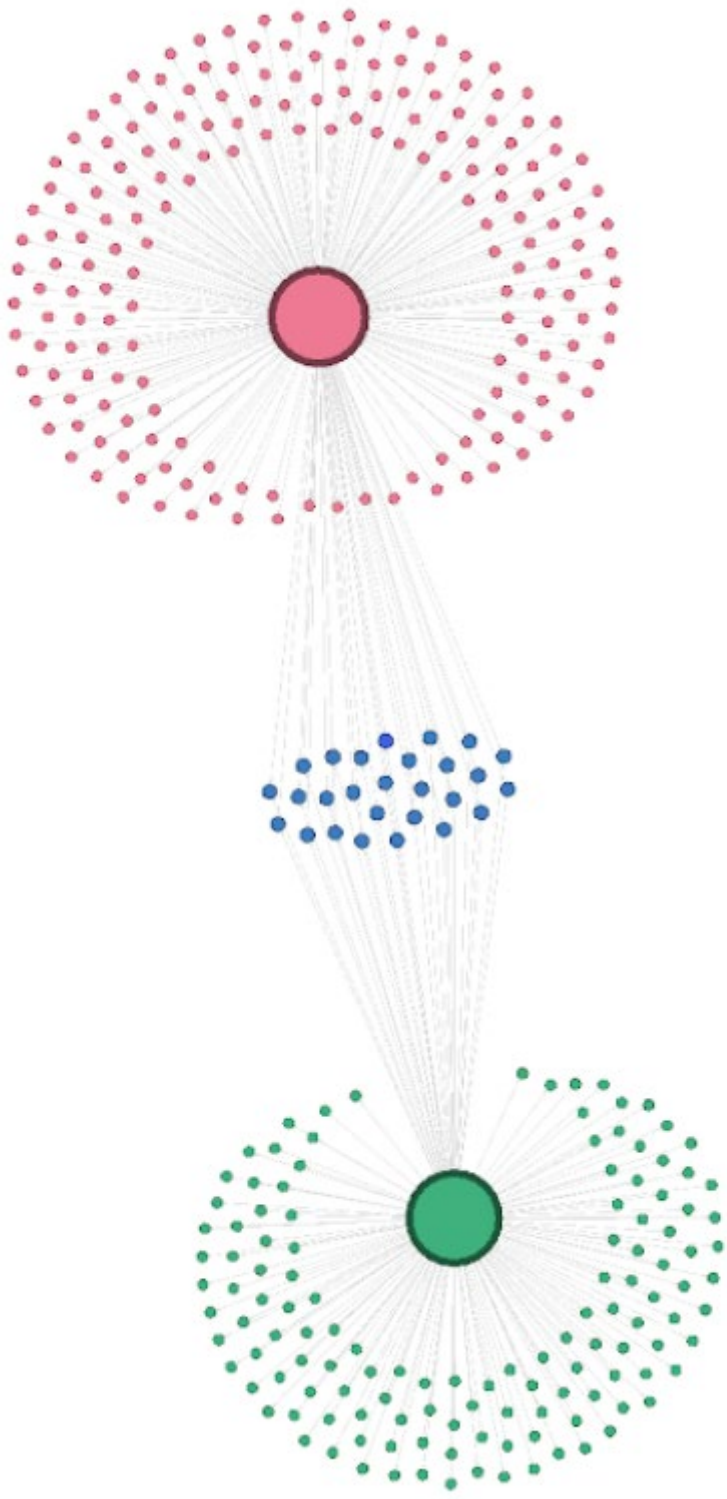


Figure 9: Outgoing links from both blogs

Using Hyphe we can map both websites' (doubtingSteven.blogspot and lunaticJoe.blogspot) outgoing links to other sites, to provide a sense of their overlap (Figure 9). When compared we see that they have both shared links to 27 domains. Excluding mainstream media sites such as the BBC, 16 domains are of particular interest (Table 8).

Domain	Count of domain
cyberguerrilla.org	35
indymedia.org.uk	15
homment.com	14
vimeo.com	10
medium.com	9
reddit.com	8
pdf-archive.com	8
cdn-images-1.medium.com	4
topix.com	4
cyberlegion.org	4
i.imgbox.com	3
ntv.livejournal.com	2
blackdefence.wixsite.com	2
youtu.be	2
onejournal.de	2
kotsyuba.livejournal.com	1
Grand Total	124

Table 8: Totals for domains linked by both blogs

Nearly all of these sites support user submitted content in some way. The most popular sites are the same ones that have been used by operators in our Polish case study and Op. Secondary Infektion. However, Vimeo appears more frequently than previously thought. Another site of particular interest is blackdefence.wixsite.com/blackdefense (Figure 10). It is interesting to note the two different spellings of defence in this URL, which could indicate confusion by a non-native speaker.

It has been previously reported that the Internet Research Agency organised and paid for self-defence classes for African Americans living in the US through a 'blacktivist' Facebook front group.[9] The blog on blackdefence.wixsite.com was active between January and December 2015. The contact information gives an address listed in Cuba, potentially because some members of the Black Panthers fled to Cuba.

Figure 10: Screenshot of Black Defense Foundation

9 https://money.cnn.com/2017/10/18/media/black-fist-russia-self-defense-classes/index.html

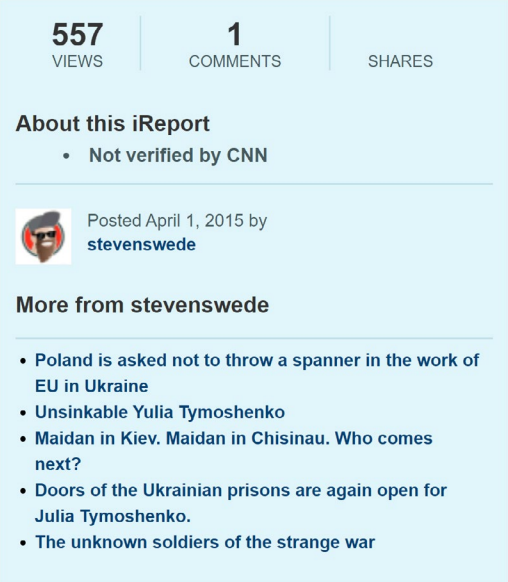


Figure 11: Screenshot of 'stevenswede'

The video section of the website has 9 videos listed under the banner 'History of Suffering'. Four of these videos are no longer available. The oldest video was uploaded to YouTube by 'Piter Preston'. This account has no other activity, no liked videos, playlists or comments. The video 'Police lawlessness. Violence against African Americans' was uploaded on the 3rd April 2015. It appears to be a homemade montage that juxtaposes police violence against African Americans with video of hyenas and wolves attacking prey. The author also uses amateur skills to animate policemen shooting high profile victims, such as Trayvon Martin and Eric Garner.

One of the Homment links shared by Steven Laack on his website is to a CNN iReport. CNN introduced the iReports format as a way to democratise the news - anyone can be a reporter. This iReport claimed that the current acting president of Lithuania Dalia Grybauskaite worked for the KGB during her student years in Leningrad. To prove this, they show 'scanned' documents from that era. This report was created by 'StevenSwede' on April 1st, 2015.

In the screenshot opposite we can see 'StevenSwede' also created a report called 'Unsinkable Yulia Tymoshenko'. This also happens to be the first line of Steven Laack's answer to the question "Is Yulia Tymoshenko of Ukraine likely to lead a new government?" on Quora and the title of a post he authors on his blog, so it is highly likely that this account is controlled by the same operator as 'Steven Laack'.

Title	Evidence	Date	Target
Muslim Turkey 11/21-27 – the worst trip ever in my life.	nothing	27-Nov-15	Turkey
The US exposes ties between Turkey and Jabhat al-Nusra?	documents	11-Feb-16	Turkey
Will American senators support Fethullah Gulen in his dispute with Turkey?	documents	18-Feb-16	Turkey/Armenia
Poles are hiding the truth about mental health of Jaroslaw Kaczynski	documents	20-Feb-16	Poland
Atlas is unsheathing his sword	nothing	09-Mar-16	US/Britain
Ukraine asks the EU for help to get rid of Po-roshenko and Yatsenyuk	documents	14-Mar-16	Ukraine
Freedom in exchange for stability. The Kurds will get independence.	Screen-shots	30-Mar-16	Turkey
Jaresko dissociated herself from the letter to Nuland, not from the pressure on the Dutch	video	31-Mar-16	Ukraine
Being friendly American way. The USA was spying on the British Royal Family	documents	05-Apr-16	US
Kaczynski's FRAXA threatens Europe! Why the truth is concealed?	documents	12-Apr-16	Poland
Turkey was about to open second front vs. Armenia	Screen-shots	16-Apr-16	Turkey/Armenia
Dalia Grybauskaite: Seven Years of Lies	documents	16-May-16	Lithuania
Saakashvili did not receive Hahn's assurances that 'interim' Groysman's Cabinet resigns in 2017...	documents	17-May-16	Ukraine
Independent Journalists: the new faces, though old methods. Who 'throws dead cats on the table' today?	documents	31-May-16	Bellingcat

Table 9: List of Homment[.]com Links

ANALYSIS OF HOMMENT ARTICLES

Informed by the Poland case study it seems plausible to infer that this methodology typically begins with a posting on the German site Homment. Table 9 shows the 14 Homment links that were shared on the two blogspot sites discussed above.

The table above shows the prolific pace at which these operators were creating these campaigns, many based on (presumably) faked documentation. The category of 'screenshots' is unique in that it typically contains screenshots of provocative stories from mainstream media. For example, one such claims that The Telegraph has published a "series of articles under the high-sounding titles on future independence of Kurdistan."

The operators claim to have taken screenshots of the articles before they were removed by the media. The operators explain that articles are: "usually posted at prime-time to be deleted two or three hours later. This is the most widely known method of exploring the public opinion when during the minimal time interval the reaction of the maximum number of respondents is checked."

The operators include 'reactions' from readers, for example in Figure 12 there is a comment from The Sun website, written in non-native English that probably qualifies as hate speech.

Figure 12: Screenshot of Commenting Behaviour

It appears that an account called jbird65 was posting to The Sun who won a caption competition in January 2014. https://www.thesun.co.uk/archives/news/513319/give-us-a-quip-on-our-funny-pics-72/

It is possible that the 'jbird65' account was run by foreign operatives, although it seems unlikely that they would display this much nuance in 2014. We cannot find this comment on the original site, suggesting it could have been a forged image. Alternatively, it may have been posted then deleted.

Many of the messaging campaigns identified were directed at Turkey and took place just after Turkey shot down a Russian fighter-bomber after claiming it had strayed from Syria into Turkish territory. Oddly, the first 'campaign' occurred just 3 days after that incident and included no 'evidence', unlike the majority of the other campaigns. The post in question was supposedly written by a German who had vacationed in Turkey and provides a rambling account of his experiences there. The content is hateful. For example, at the airport he meets a German woman whose daughter has become a sex slave. Much of the content is made up of anti-Muslim stereotypes, including: "Turkish women - wearing black plastic garbage bags on their heads" and "last night in neighboring hotel a group of muslim youths raped underage girl from UK".

Despite operating during the same time period (Oct 2015- Jun 2016), and answering roughly the same number of questions on the same topics, the 'Steven Laack' and 'Josef Hashever' Quora accounts only answered the same question once: "Why doesn't the West denounce the current Moldovan Government?"

This question was posed by 'Joe Fangas' which is itself a suspicious account. The last question he asked in January 2017 was 'Where is the proof Russia hacked the elections'. In total, he answered 12 questions, 7 of which were either pro-Trump or anti-Bernie Sanders. Three others related to Game of Thrones.

The 'Josef' account was first to respond to the question, with a long post including links to sites where content can be hosted, such as forums, some of which have now been removed. However, he also provided more links to reputable sources such as the BBC and Radio Free Europe, and also to Wikipedia articles on American Imperialism and the demographics of Moldova. His main narrative thread being that the US wants Romania to annex Moldova.

Two days later Steven answered the same question. His lengthy response only included two links: one to an IndyMedia article that he likely authored (as it contains the same text as his response); and the other to his blog site. In these two responses we can see the familiar pattern of Secondary Infektion, with regards to the sources and the use of 'one off burner accounts' on those source websites. However, what is different is the use of two overarching 'legends' that have

extensive social media presence in order to provide legitimacy and exposure to these campaigns through sites such as Quora, CNN and Buzzfeed.

A recurring and defining component of the empirical cases reviewed above is how they all engage in implanting information into different parts of the media stream, seeking to surreptitiously hi-jack different facets of the mechanisms of the media ecosystem to draw attention to the materials involved.

THE DEMOCRATIC NATIONAL COMMITTEE HACK

Having distilled these patterns and sequences of activity into an empirically-led conceptual model, it is intriguing that there are similarities with at least two other high-profile IIIOs. Because these have been discussed in detail elsewhere, herein we will only briefly reprise their key elements in order to lend credibility to the insights afforded by the model of perception infection methodology. The two cases in question are: (1) The Democratic National Committee (DNC) website hack/leak in 2016; (2) the Integrity Initiative hack/leak.

In their work for the US Senate and beyond, Stanford's Internet Observatory (2019) has detailed a range of methods associated with a number of hack and leak operations attributed to the GRU. Informed by data provided to them by Facebook, they describe how operators sought to 'launder' narratives, by using multiple fake personas and accounts. As they correctly identify, these are long-established procedures in the active measures playbook. These methods feature prominently in the distribution of the materials obtained from the hack of the servers of the DNC in 2016, a series of events that have been attributed a role in undermining Hilary Clinton's presidential campaign.[10]

Table 10 below provides a brief timeline of the key events and developments regarding the DNC data becoming public.

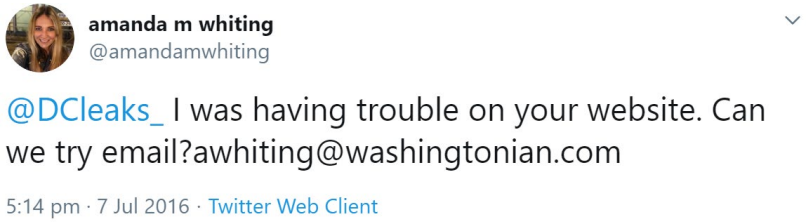
Date	Events
March 2016	Phishing emails sent
April 2016	DCLeaks[.]com address is registered using Bitcoin payment.
08-Jun-16	First transmission event sees release of 'George Soros files' on DCleaks. Files date back to 2008/9 as well as some from 2016.
15-Jun-16	Editor-in-Chief of investigative news site The Smoking Gun, receives email bearing a small cache of documents marked "CONFIDENTIAL."
2nd half of June	DCleaks begins uploading DNC documents. "Guccifer 2.0" account begins directing reporters to DCleaks
01-Jul-16	The Intercept publishes details from DCleaks of 'NATO General plotting against Obama on Russia policy'.
02-Jul-16	RT reports the above story
22-Jul-16	Wikileaks uploads the files to their site, prompting widespread dissemination and discussion in the mainstream media.

Table 10: Timeline of Key Events regarding DNC data hack/leak

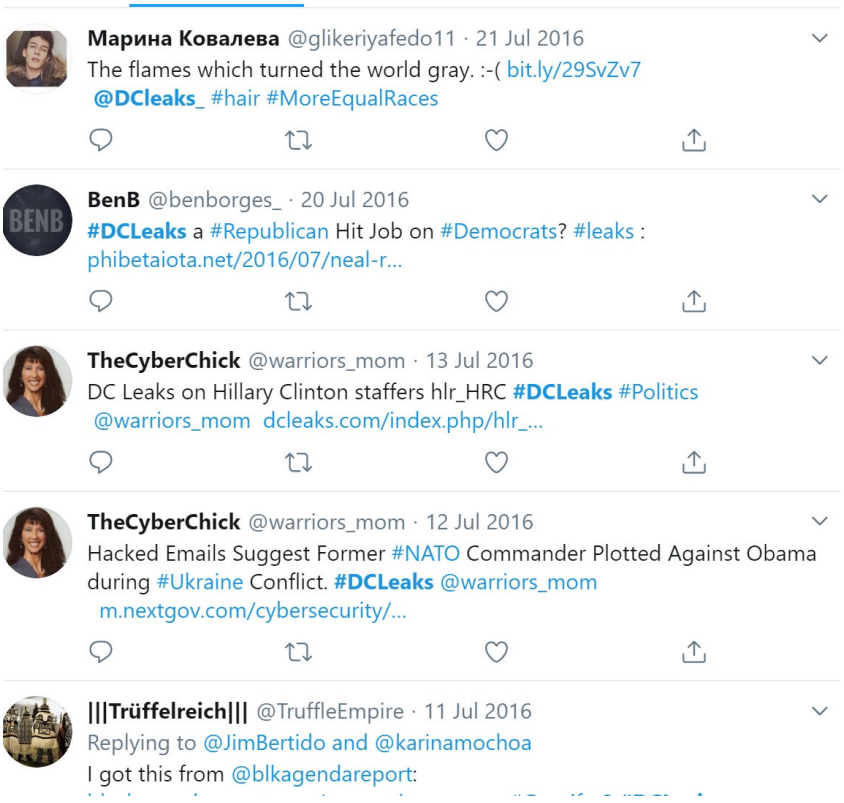
A day before The Smoking Gun was contacted, four tweets were sent with the same content at the same time promoting the hashtag DCleaks and the website. Two of these accounts were pro-Green Party accounts and two were pro-Bernie Sanders. Interestingly, despite Bernie Sanders being the democratic frontrunner in the 2020 election, neither pro-Bernie account has tweeted in the last two years.

10 For example, see Jamieson, K. (2018) Cyberwar: How Russian Trolls and Hackers Helped Elect a president. New York: Oxford University Press.

Despite DCleaks hosting the files from mid-June, surviving tweets about the website do not mention Hilary Clinton or the DNC until the 9th of July, this is despite evidence that the @DCleaks_Twitter account was actively reaching out to journalists in early July:



It could be that the documents were provided to Wikileaks because the operatives had failed to get mainstream press or broadcast outlets, or social media, interested in them. There appear to be only 5 tweets mentioning DCleaks between the 11th and 21st July, although Twitter may have removed some tweets between now and 2016:



Interestingly, confirmed IRA accounts did not start tweeting about DCleaks until July 22nd 2016 when the files were released by Wikileaks. This promotion was started by the infamous TEN_GOP persona. The hashtag 'DCleaks' wasn't used until August. The DCleaks.com website was never shared. In total, known IRA accounts shared 214 tweets, 146 (68%) of which were retweets. However, the 'Russia Jan 2019 dataset' has one account that retweeted the @DCleaks_ Twitter account twice on June 16th but those tweets were not to do with the DNC, they were about George Soros and the Supreme allied commander of NATO. The account doesn't mention the documents with regards to the DNC until August.

The IRA also did not promote the Podesta emails until they were released by Wikileaks. Even then the majority of their involvement was retweeting others' messages, with 1331 tweets between October 7th and Jan 1st 2017, 1109 (83%) of those being retweets. Ultimately, the Russian operatives have scored a notable success, inasmuch as President Trump has publicly and repeatedly invoked the unfounded rumour that the cyber security firm Crowdstrike had backups of the material on a server in Ukraine. He made these statements despite this claim being contrary to the assessment of the Department of Justice that this rumour was itself a Russian state invention, and who have indicted several Russian security staff.

THE INTEGRITY INITIATIVE

The Integrity Initiative was a programme run by the Institute of Statecraft in receipt of funding support from the UK Foreign and Commonwealth to help counter Russian disinformation and propaganda. In September 2018 it was subject to a series of cyberattacks, with stolen files containing various embarrassing and confidential content released into the public domain in several waves. The material concerned was covered by both RT and Sputnik.

Table 11 below provides a brief timeline of the key events and developments regarding the Integrity Initiative data becoming public:

Date	Events
05-Nov-18	Documents posted on the CyberGuerrilla site, which is associated with the hacktivist group Anonymous
06-Nov-18	Three burner accounts are used on three different forums to promote the link
07-Nov-18	One burner account posts to the main German subreddit and another posts a comment on Spiegel
08-Nov-18	Two burner accounts post to Reddit, one of them on the r/ukPolitics sub-reddit. One burner account posts to a Swedish forum and another to a Spanish forum.
12-Nov-18	'Andrew Farrel' authors a story on Indybay.org, publicising the documents. A burner account spreads the link on a French forum. He asks people to sign a change.org petition. 'Adancast' authors an article on a Spanish site claiming that Britain has interfered with Spanish politics. An account with the same name and picture is created on Reddit and posts the link multiple times on Spanish subreddits. An article is written by 'CamilleCarminot' saying that Britain is destroying French sovereignty. She later posts a comment to two different French forums. 'Nick Woodland' writes an article in German to indymedia.org and to German site ask1.org.
14-Nov-18	'AdanCast' leaves two comments in Spanish in response to his own article.
21-Nov-18	Russian media report on the story.
22-Nov-18	Six Russian liveJournal sites publicize the story. okolokremlya.ru translates some of the documents into Russian. Mueller indicted company Federal News Agency also reports on the story.
23-Nov-18	Russia Today and Sputnik report on the story.

Table 11: Timeline of Key Events regarding Integrity Initiative data hack\leak

Whilst this case is not as closely aligned as the others reported on in the rest of this analysis, its base pattern possesses salient similarities with the core precepts of the perception infection model to warrant inclusion.

IMPLICATIONS AND CONCLUSION

Current understandings of disinformation campaigns by hostile states, have been strongly influenced by the discovery of the Russian Internet Research Agency's activities around the 2016 US Presidential Election. Set against this backdrop, increasing numbers of studies have evidenced similar types of social media based 'organic' influencing interventions across a range of countries and contexts. The empirical analyses reported above, informed by several other prior studies, delineates the components of an alternative methodology for manufacturing perception infections. In the Polish case study above, the intent was to malignly influence public perceptions of a high profile politician, as a pathway to shape perceptions of German-Polish relations.

In the study of fear of crime, the concept of 'perceptual intervention' has been introduced to describe actions deliberately intended to manipulate public views and understandings of a situation or events.[11] **Saliently for the current discussion, it has been suggested that perceptual interventions work along two linked pathways, shaping:**

- **What is seen** – by steering audiences to attend to some events or issues rather than others;
- **How it is seen** – subtly framing the ways that the same events or issues are interpreted.

These two dimensions provide an incisive description of the mechanics of the two principal case studies analysed in this report. For both the Brexit negotiations and Polish politician narratives, the content of the disclosures sought to bring new information into the public sphere (what is seen), whilst attaching negative connotations to the subjects (how it is seen). Thus, we infer that these dimensions are integral to how and why perception infections can be effective.

A defining feature of perception infection methodology is that where orthodox disinformation campaigns pivot around spoofed accounts and fake stories, some of the events described herein make use of genuine documents. This places them more in the domain of 'information operations' than disinformation campaigns. That said, as Bruce Schneier (2018) has recently written, this doesn't quite capture the contemporary dynamics of the information age suffused by internet and social media platforms. He prefers the term 'influence operation', as do the Estonian Intelligence Service.[12] But in light of what has been seen in the preceding sections, this formulation appears equally partial and limited.

Thus, informed by the analysis reported above, we propose the concept of 'Information, Influence and Interference Operations' to provide a comprehensive and rounded account of the varied ways in which digital influence engineering is performed. The point is that each of the conceptual elements of this definition (information + influence + interference) are distinctive components and play an important role, in terms of delivering different outcomes.

11 Ditton, J. and M. Innes (2005) "Perceptual intervention and its role in the management of crime fear" in N. Tilley (ed.) The Handbook of Crime Prevention. Cullompton: Willan.

12 Estonian Foreign Intelligence Service (2020) Annual Report. https://www.valisluureamet.ee/pdf/raport-2020-en.pdf

Framed in this way, we conclude that there are at least six key methodologies that can be defined in terms of how Russian state assets and actors are seeking to influence public perceptions and political agendas:

01 **'Pure' or 'classic' disinformation campaigns** – where communication pivots around the transmission of purposively and deliberately false information, often relating to both the message and messenger. Thus, disinformation combines both an intent and action designed to deceive.

02 **Misinformation into disinformation pathway** – is where unintentionally misleading material is deliberately amplified to induce negative consequences.

03 **Disinformation into misinformation pathway** – is an ideal scenario for hostile state actors, in that others amplify a false message sincerely believing it to be true or accurate

04 **Information – Influence Operations** seek to shape the ordering of reality through perceptual management and manipulation. This can involve distortion of factually accurate information, as opposed to outright disinformation.

05 **Information – Interference Operations** involve physical 'real world' interventions, as opposed to psychological, mechanisms.

06 **Information, Influence and Interference Operations** are the most complex version, and involve both psychological and physical interventions to shape public perceptions and political agendas.

Developing coherent and comprehensive conceptual frameworks to capture the variety of ways in which perceptual interventions are being made to influence the ordering of reality is an important step in developing a 'richer picture' understanding of how these kinds of influencing activities are being transacted. For if these kinds of strategic methodologies can be configured, then the next step is to discern the specific tactics and techniques associated with each of them.

Based upon this analysis, it is our assessment that personal targeted communications that try to influence and persuade certain individuals to act as 'Digital Typhoid Marys' and spread misleading and harmful information, are becoming an increasingly important component of Russian IIIOs. The logic of perception infections is that with a single unit of (dis) information that is replicated by exploiting the established processes of a media ecosystem, you can subtly manipulate how some people interpret and define key events in the world, by feeding information and disinformation into the media stream such that it influences what comes to be viewed as 'real' and 'true'.

The analysis and findings in this report were partly supported by funding from UK government.

Get in touch.

OSCAR, Crime and Security Research Institute, Cardiff University
Level 2, Friary House, Greyfriars Rd, Cardiff
CF10 3AE

+44 (0) 2920 875440

crimeandsecurity@cardiff.ac.uk

@CrimeSecurityCU

www.crimeandsecurity.org