DEMOS

Warring Songs

Information Operations in the Digital Age

Alex Krasodomski-Jones
Josh Smith
Elliot Jones
Ellen Judson
Carl Miller

May 2019

Support for this project was generously provided by the

OPEN SOCIETY
EUROPEAN POLICY
INSTITUTE

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to over-come them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales.
(Charity Registration no. 1042046)

Find out more at www.demos.co.uk

DEMOS

Published by Demos May 2019.

76 Vincent Square
London, SW1P 2PD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

Contents

Introduction

The poisoning of online discussions of the world cup in 2014 by a group calling itself Islamic State took many by surprise. Without warning, internet users were encountering horrifying images and terrorist propaganda, spoonfed onto their devices as they tried to follow the football. It was, for many, their first contact with an internet that had become a battlefield.

The trickle of warnings soon gave way to a deluge: the Cambridge Analytica scandal, surrounding the company's use of personal data to target political advertising broke in March 2018. Social media's pivotal role in the spread of anti-Rohingya content in Myanmar broke later that year. Elections from the US to France, from Hungary to the Philippines, from Italy to India added new stories to a growing tapestry of digital manipulation.

It is now clear: the past decade has seen democracies around the world become the target of a new kind of information operations, a war that governments have frequently failed to prepare for, recognise or respond to effectively, a war that required new definitions, descriptions and labels that we often didn't have.

This report aims to change that. We propose a framework through which the aims, strategies, tactics and actors participating in information operations can be understood. We begin by defining information operations, stressing the breadth of tactics and strategies we must contend with and building a taxonomy of information operations. We expand this with three case studies of Russian information operations in Germany, France and Italy examining the patterns and themes in tweets definitively attributed to Russian information operations. Finally, we set out some lessons, and reflect on the ramifications of our conclusions for EU policymakers in advance of the upcoming EU elections.

This report would have not been possible without the time and effort of our partners at OSEPI. In particular, we would like to thank Iskra Kirova, who guided our questioning from the outset and provided invaluable feedback throughout.

Information operations are an incredibly complex subject. It defies clear-cut definitions. It involves a dizzying array of actors, participants and targets, it tests the boundaries of governmental responsibility, and it mutates and transforms at a breakneck pace. This short report cannot be a comprehensive analysis, but we believe is a vital step forward in understanding what governments around the world are up against. Responses will require a coalition of partners in government, technology, civil society and the wider public. We hope this report goes some way towards this.

All errors and omissions remain the authors' own.

Alex Krasodomski-Jones

Executive Summary

This report uses a review of hostile information operations around the world and new data analyses of hostile action carried out against three European countries to reveal the contours of modern day information operations. We find:

- The widely-held focus on 'fake news' is myopic: information operations are vast in scale, varied in target and numerous in strategies and tactics.
- Much of the information shared during information operations is not 'fake', but the selective amplification of reputable, mainstream media stories to fit an agenda.
- IRA accounts targeting the three countries examined overwhelmingly shared content from reputable media sources in every case study.
- Of 39 cases we reviewed, 20 primarily involved content which could be assessed as true or false: the remaining 19 did not contain fact statements, challenging the narrative that tackling inaccurate news through fact-checking is a catch-all solution.
- Information operations are characterised by erratic bursts of activity rather than consistent output, and responses to them must be able to scale quickly to avoid becoming swamped.
- Information operations are as likely to exploit cultural and social division in a country as they are to target an individual political event.
- Although information operations are coordinated, they are inconsistent, with discrepancies across language, timing, subject-matter and geography. This presents a challenge to third-party identification of inauthentic accounts.

Recommendations

We suggest:

- European governments expand their definitions of information warfare to include the full range of information operation strategies in order to alert citizens, the media and civil society of the ways they may be targeted or exploited.
- That given commitments by governments to protecting free speech, and the challenges this poses when dealing with the spectrum of disinformation, a focus on the aspects of information operations that are not free-speech issues may be valuable. This also applies to platforms.
- Those responding to information operations recognise that 'factfulness' is not an attribute of all information operations as a whole. In half our reviewed cases there was no factual statement made. Fact-checking must be supported with responses to non-factual operations.
- Governments must recognise that information operations are operating with long-term aims, but are capable of bursts of activity that can overwhelm first-responders. Long-term investment in intelligence and on-going analysis is needed, alongside a more agile ability to scale up a response at short notice.
- Digital platforms must accept the demands by regulators and lawmakers for change, and cooperate with and support the efforts of civil society and academia in identifying the ways their platforms are being exploited, including a commitment to co-create a robust evidence base on safe platform design.

Aims, Strategies and Tactics of information operations

Aims	Strategies	Tactics
Affect sympathetic changes in behaviour and perception	Build political support Feign public support Encourage conspiratorial thinking Promote sympathetic voices	Astroturfing (fake grassroots support) False amplification of critiques of opponents False amplification of marginal voices False amplification of news Impersonation of public figures Impersonation of political allies
Reduce oppositional participation	Reduce critical voices in media Undermine trust in political representatives and institutions Undermine trust in institutions of government Undermine trust in electoral institutions Incite societal and cultural divisions Voter suppression Abuse of legal systems	Defamation Doxxing Hacking and leaking documents Interference with political processes Intimidation and harassment Dark advertising
Reduce quality of communications environment	Create confusion and anger Denigrate compromise Undermine channels of productive communication Reduce trust in digital communications Disrupt channels of communication	Exploitation of content moderation systems Playing both sides Scare stories Shocking or graphic content Communications disruption Hashtag poisoning Spam
Reduce quality of available information	Undermine trust in media institutions Undermine trust in digital media Blur the boundaries of fact and fiction Suppress critical content Promote sympathetic content Shift the balance of content in actor's favour	Algorithm exploitation and manipulations Deepfakes Dissemation of doctored images, videos and documents Dissemation of false, misleading or misattributed content Impersonation of websites Restriction of availability of information to the public Dissemation of conspiracy theories

01.

What are Information Operations?

Background

Information operations and their overarching aims are not new but the actors, strategies and tactics involved are developing as technology advances. At its most fundamental, the 'information domain' is now recognised as a space where genuine military operations can occur, and governments and security services are responding accordingly.

Information operations are increasingly prominent - they hit the headlines around the 2016 US Presidential election, when the Russian intelligence agency, the G.R.U., was implicated in hacking the Democratic National Committee to release documents damaging to Hillary Clinton's campaign.[1] And though Russia is often mentioned in relation to information operations, the mutation of the internet into a theatre of war has brought with it a wide range of combatants.[2] Many countries are suspected to be complicit in acts of information operations, with more piggybacking on an already-disrupted information environment to cement their own interests.

A widespread disinformation campaign by the Myanmar military against the Rohingya led to UN investigators criticism of Facebook for the role the platform played in inciting violence, and said that Myanmar officials should be facing charges of genocide.[3] [4] Protesters in Mexico City faced arbitrary arrest and police violence after a hashtag being used to communicate safety advice amongst protectors was poisoned with spam from suspected government bots.[5] The Chinese government works to steer online conversation away from controversial issues by employing '50c party' members to pose as genuine social media users and create posts, estimated at 448 million comments a year.[6] And in the Philippines, President Duterte's brutal 'war on drugs', which includes extra-judicial killings, seeks justification through information campaigns, including for instance, his campaign spokesman sharing a graphic photo of a young girl killed and falsely attributing the death to crime in the Philippines.[7]

As a result, digital information and the information space have come under increased scrutiny, not only from academics, researchers and journalists, but from policymakers, civil servants, international institutions, and militaries. NATO has affirmed in its military policy that no NATO decision should be made 'without considering its potential impact on the Information Environment'.[8] The UK Digital, Culture, Media and Sport Select Committee held an inquiry, coordinated with other Parliaments across the world, into disinformation and 'fake news', and has recently announced a Subcommittee to continue its work looking into the threat of disinformation.[1] [9] The European Commission last year set up a High Level Expert Group on Fake News and Online Disinformation[10], and has published a voluntary Code of Practice on Disinformation to secure industry buy-in on tackling this phenomenon.[11]

However, while the aspects of information operations have multiplied, there has grown a fixation with increasingly narrow aspects of these activities. There is a worrying tendency in the discourse around information operations to focus on 'fake news', or to implicitly

1 The term 'fake news' has become near-meaningless since its rise to prominence in 2016. We use the term here as deliberately representative of the narrowness of the debate, and more specifically to refer to digital content that presents verifiably false information. It could be replaced with narrower terms, such as 'false information' or 'false content' without changing its definition as used here.

equate 'information operations' with either disinformation or harassment. Both of these are central elements of information operations which should not be discounted, but to focus on them alone risks excluding proper scrutiny of the dangers and possible responses to the much wider myriad of information operations.

Non-state and state-aligned actors are also responsible for ongoing information operations. At their most extreme, terror groups have shown themselves to be adept at using social media channels, online content hosts and closed networks to produce coordinated campaigns targeting their opponents. Non-violent extremists, including groups on the far-left and far-right, have also replicated these tactics for political, social or cultural ends.

People are not confident that they are equipped to deal with the challenges posed by information operations. Across the EU, at least 70% of respondents in each country surveyed by the European Commission saw 'fake news' as a problem in their country. While 71% of Europeans said they were at least 'somewhat confident' that they could identify 'fake news', 26% said they were not very or not at all confident. 83% of Europeans said they thought 'fake news' was a problem for democracy.[12]

One aspect of why social media can present a threat to democracy is that it blurs categories that had once been seen as relatively clear-cut. Social media has already made headway in redefining the categories of public and private, and information operations online may seek to redefine the categories of truth and falsehood. As the possibilities for information operations through social media expands, individuals outside the military may be increasingly implicated in sharing, boosting or disseminating disinformation - either knowingly or unknowingly - blurring the categories of war and peace, soldier and civilian.

Whilst the offensive side of information operations has grown rapidly, defense against information operations has been much slower to emerge. A number of things are unclear: the legitimate role of liberal democratic Governments in defending, and possibly intervening into, a domestic press; the efficacy of fact-checking and other attempts to debunk misinformation; whether skills and digital literacy can form an effective safeguard against information operations, and how it can evolve as quickly as the techniques it seeks to defend against. Especially in the run-up to the European Parliamentary elections, this asymmetry between offence and defense will likely become stark.

This research has underlined the complexity and scale of the challenging facing policymakers, technology companies, civil society and the public. The response from policymakers interested in defending democracy and fundamental human rights, at national and international levels, in the face of this complex, evolving threat, must be nuanced, evidence-based, and in full awareness of possible risks, both of information operations and proposed responses to it.[13]

What are information operations?

One of the most challenging questions facing governments, civil society and the media in responding to information operations is in defining them. To date, commentary on

information operations has suffered from contradicting shortcomings: too broad and too myopic.

Too often, the focus has been on singular tactics of information operations, such as harassment or 'fake news'. This has obscured the fact that these tactics are part of broader strategies that see information as the principal agent in achieving certain geo-political outcomes.

We propose the following working definition of information operations.

> *A non-kinetic, coordinated attempt to inauthentically manipulate an information environment in a systemic/strategic way, using means which are coordinated, covert and inauthentic in order to achieve political or social objectives.*

This definition is explored further below.

1. Non-kinetic

We understand information operations here to be confined to use of information, and not to include the use of kinetic operations such as sabotage or electronic interference.

2. Coordinated

We understand information operations to require coordination between individuals and groups of individuals. This ranges from coordination at a state or state military level down to the use of chatrooms and message boards to ensure consistency of aims and message.

3. Inauthentic

We understand inauthenticity to be central to an understanding of information operations: this may include identities, content, messaging, or amplification. Authentic expressions of, or efforts towards social, political or economic aims by ordinary people are not information operations, and we believe it is dangerous to conflate the two. We do, however, include the processes of data gathering and targeted political advertising as worthy of close examination.[14]

4. Strategies

We understand information operations to have four broad strategies, which we have brought together under the banner of manipulating the information environment.

(a) Insert, remove and amplify information

Altering the nature and quality of information that can be accessed, and the visibility of that information, is a central pillar of information operations.

(b) Degrade the information environment

Altering the space in which information is shared and communication takes place to facilitate supportive communication and the spread of supportive information, or to frustrate opposing communication and the spread of opposing information.

(c) Limit the participation of opposing voices

Reducing the ability or willingness of politically, culturally or socially opposed voices to take part in the communications space.

(d) Effect sympathetic changes in behaviour or perception

Building or feigning political, social or cultural influence among a target population in a way that benefits or aligns with the aims or outlook of the perpetrator.

5. Social or political objectives

Much of the behaviour noted above has been recorded as taking place outside of clear aims. We understand information operations to require an overarching purpose: societal or political change, or a change in economic circumstance.

Our focus here is on the information space, rather than kinetic operations, such as military strikes against communications infrastructure. Although military activities have targeted and exploited information for years and states have undertaken large-scale propaganda campaigns using traditional media, the transformation of our online communities into warzones is a new phenomenon that will require solutions that extend far beyond the scope or capability of the military.

As noted above, strategies employed by hostile groups have included everything from fabrication of news to false amplification of unwitting journalists; from harassment and abuse of politicians to gaming recommendation algorithms. It underlines the importance of looking broadly at the information ecosystem and the actors that make it up, rather than focusing on single piece of the puzzle. 'Fake news' is a tiny cog in a much larger machine.

02.

A Taxonomy of Information Operations

A wide range of strategies and tactics constitute information operations but this diversity is often not reflected in discussions of how to respond to these activities, by the media or policymakers. We aim to provide a basis for expanding the scope of these discussions, through analysis of a diverse and wide-ranging selection of the types and instances of actors, techniques and impacts that are involved in or are products of information operations.

Researchers carried out a literature review as the basis for this analysis, covering academic literature, civil society reports, and journalistic analysis and news items.

Initial Literature Scoping

Academic literature was reviewed through keyword searches on terms 'information warfare' and 'disinformation' in Google Scholar. This produces 1,498,200 results, with 166,600 results from 2013-2019.[15]

This was supplemented by reviews of grey literature, including reports which collated multiple cases of information operations in order to ensure a broad selection of examples was included.[16] This stage focused primarily on searching keywords, including 'fake news', 'disinformation', 'information warfare' in Google.[17] Searches of '[country name] + keyword' were also carried out on countries from five continents to ensure examples of particular political salience were included - such as those where information operations have been directly linked to serious human rights violations, as in Myanmar and India.

References within articles reviewed and within the authors' previous work on this topic were also used to source further literature for review.

Sourcing Case Studies of Information Operations

From 53 pieces of literature[18], spanning from 2013-2019, 106 case studies were extracted, spanning 31 countries across 5 continents. The case studies were of information activity which have or could plausibly be described as potential instances of information operations. For each case, where accessible, details were extracted as to the country associated with the information activity (country of origin and/or country within which the activity was carried out), the actor responsible for coordinating the activity, the specific techniques used and the resulting impact. Russia was a focus of the review, given the scope of this report which in the section 'Disinformation In Action' examines Russian information operations specifically.

Selecting key case studies

A subset of these case studies was selected for more in-depth analysis. In making these selections, researchers took into account the clarity of the case study as an example of information operations, the scale and level of coordination of the operation, and the potential (or actual) scale and costs of impact; the level of information available about the case study, and with the aim of producing a set of examples with a breadth of countries, actors and techniques. Case studies mostly, but not exclusively, were of information operations with an online or digital element.

This was then supplemented by further research:

- where more detail was needed on a particular case
- to include techniques and case studies of particular salience, such as those which had cut-through into the mainstream with apparent political or cultural impact (e.g. Cambridge Analytica algorithm manipulation)
- as further reports of relevant information operations were reviewed, where they highlighted an existing gap in the techniques included in the taxonomy.

Case studies were removed from the subset when, on further analysis, they did not meet the definition of 'non-kinetic and coordinated'- for example, where information activity had occurred but there was no indication that it involved intentional coordination.

In-depth analysis

As a result, 39 case studies, across 19 countries, were analysed to identify features which were common to multiple instances of information operations, and how these features varied across the different cases. This identification was informed by the background research and comparative analysis of the individual case studies. The spectrum of actual and intended impacts of information operations was then extrapolated from the instances of information operations (also informed by the background research).

Limitations

There are of course limitations to this taxonomy - it is not exhaustive, and the examples selected are not a representative sample of all information operations, meaning that conclusions cannot be drawn at a general level about the proportion of information operations which exhibit a particular feature.

The judgements made on which information activities met the definitional criteria to qualify as information operations, and which case studies exhibited certain features or belonged to a certain category of influence operation, may be subject to disagreement, as they involve a subjective element. The features of information operations have also been simplified to a certain degree (the answer to whether a tactic exhibited a certain feature or not in reality is not always a clear yes/no).

What this taxonomy is able to demonstrate clearly is that there exists a great diversity of tactics which can be described as information operations. As such it provides a basis on which to draw general inferences about information operations, identify future cases of information operations and inform decisions about how the effects of information operations might be mitigated.

Aims, Strategies and Tactics of information operations

Aims	Strategies	Tactics
Affect sympathetic changes in behaviour and perception	Build political support Feign public support Encourage conspiratorial thinking Promote sympathetic voices	Astroturfing (fake grassroots support) False amplification of critiques of opponents False amplification of marginal voices False amplification of news Impersonation of public figures Impersonation of political allies
Reduce oppositional participation	Reduce critical voices in media Undermine trust in political representatives and institutions Undermine trust in institutions of government Undermine trust in electoral institutions Incite societal and cultural divisions Voter suppression Abuse of legal systems	Defamation Doxxing Hacking and leaking documents Interference with political processes Intimidation and harassment Dark advertising
Reduce quality of communications environment	Create confusion and anger Denigrate compromise Undermine channels of productive communication Reduce trust in digital communications Disrupt channels of communication	Exploitation of content moderation systems Playing both sides Scare stories Shocking or graphic content Communications disruption Hashtag poisoning Spam
Reduce quality of available information	Undermine trust in media institutions Undermine trust in digital media Blur the boundaries of fact and fiction Suppress critical content Promote sympathetic content Shift the balance of content in actor's favour	Algorithm exploitation and manipulations Deepfakes Dissemation of doctored images, videos and documents Dissemation of false, misleading or misattributed content Impersonation of websites Restriction of availability of information to the public Dissemation of conspiracy theories

We have identified four broad strategic aims that information operations seek to achieve.

Affect sympathetic changes in behaviour and perception

Actors, in particular government actors, rely at least in part on public support to enable them to achieve their aims. Actors therefore make use of information operations to bring about changes in how they are perceived in terms of the level of support they have. That may be through actively building or strengthening support through engaging in false amplification/creation of criticisms of their opponents[19] or of news supportive of their cause.[20]

Alternatively it can be through feigning higher levels of public support, through astroturfing[21], impersonating public figures[22], political allies[23], or even political opponents[24], to spread apparent support for their cause from multiple angles. Feigning and building public support may not be independent - amplifying real support may help feign it, and increasing fake support may translate into real support when it is perceived by the unaware audience.

Reduce oppositional participation

Actors, state, non-state, or individual, have a clear interest in reducing the prominence or participation of their opponents within discourse or political processes.

This can be achieved in different ways, including through inciting societal and cultural divisions which undermine a certain group; engaging in targeted harassment and intimidation to drive them out of information spaces or to gain control of their online identities to use in favour of the actor (such as the White Trolls do against journalists in Turkey).[25]

Leaking documents and interfering with political processes can also undermine trust in politicians and political institutions, which can reduce those institutions' ability to act against the interest of the information operatives.[26] [27]

Reduce quality of communicaitons environment

If the integrity of communications environments are compromised, co-ordination - most particularly anti-government coordination - cannot be achieved as effectively, and meaningful discourse cannot occur, and trust in communications channels themselves as sites of discourse are undermined.[28] Most starkly, this appears in the case of the Mexican Peñabots disrupting protester coordination, but more broadly, manifests in directing or incentivising reporting of critical comments online, dominating online discourse with spam rather than meaningful content, or posting graphic or inflammatory content designed to shock and inflame discourse rather than contribute to it.[29] [30] [31] [32]

Reduce quality of available information

This is a particularly widely-discussed category when it comes to Russian information operations in particular. There is some overlap with the other categories - in that

sympathetic content will be sought to be promoted and critical content suppressed, regardless of its truth or contribution to the discourse. More generally, however, this type of information operations seeks to induce epistemic paralysis - by blurring the boundaries of fact and fiction, and manipulating the criteria by which something is assessed to be true or false, dissent is rendered impotent as objections or contradictory facts can be dismissed without any rational basis. This is the 'post-truth' information operations, which has been described as 'weaponised relativism' - breaking down the idea of objective truth to serve the interests of those already in power against those who might seek to use the truth to change the state of affairs.[33] [34]

A single influence operation can and frequently does span the breadth of these aims. The objectives of information operations may be social, political or economic - or a combination of these. These strategies often overlap or are employed in conjunction with each other. For instance, attempting to deflect criticism of a government's actions against a particular group can be achieved by e.g.

- Working to persuade people that the group is a legitimate target (affecting sympathetic behaviour or perception)
- Discrediting and defaming their opponents (so that they are less able to defend themselves, for instance if they have been discredited)
- Coordinating content on social media to dominate hashtags (reducing the quality of the communications environment)
- Spreading disinformation and false content through media and social media channels and third party commentators (reducing the quality of information)

All of these examples are taken from a single Russian-linked disinformation campaign in Syria.[35]

03.

Features of Disinformation

In reviewing information operations, each tactic was judged against a series of attributes or features. In doing so, we are able to present a series of general attributes we believe should be taken into account when approaching the subject. Taken together, they represent a set of heuristics we believe are vital in trying to understand information operations as a whole.[36]

Concealed coordination

Although information operations can be fuelled, shared or participated in by unwitting citizens and groups, we understand information operations to require an intentional actor engaging in concealed coordination of the activity. In our analysis, we reviewed instances of information operations which were coordinated by a range of actors, including state, state-aligned, and non-state actors.

This is of critical importance to policymakers, and must be taken into account when considering steps to take in building resilience to information operations. Although citizens being wrong on the internet is unlikely to be a government concern, in the case of a coordinated information operation it is overwhelmingly likely that its source is a hostile actor of some kind.

The nature of information operations online means that although some cases involve the actor directly participating in the majority of the information activity (for instance, Russian Internet Research Agency trolls spreading both positive and negative stories about vaccinations), frequently also individuals act as conduits for these activities, for instance by sharing and amplifying anti-vaxx claims.[37] [38] Coordinated campaigns can nevertheless appear inconsistent - such as spreading both support and opposition to one cause, as we will show below.

However, not all information activity which pose serious dangers to people is coordinated to the same degree.

Actors may co-opt existing forms of information activity in their interests. In Cameroon, a video from a Nigerian film set which appeared to depict someone cooking human body parts over a fire went viral on Facebook, with people falsely claiming it showed separatists engaging in cannibalism. It is not clear where these claims first originated, or if there was a coordinated agent behind them - however, the claims went on to be used by the Cameroonian government as a justification for its ongoing crackdown against separatists[39], amplifying and using the disinformation for their own political aims.[40]

In March 2019, false rumours spreading on Facebook and Whatsapp in France about Roma people carrying out child abductions sparked violence against the Roma community; echoing attacks in India in which people were killed after similar rumours of abductions spread.[41] The information activity in these cases may not have been coordinated, but the impact on human life remains.

In these cases, the danger of the information activity arises from individuals sharing, believing and acting on these stories. Where culpability lies, beyond the originating actor, becomes increasingly blurry - these individuals may or may not know or believe that the

information is false and will have their own reasons - likely social, economic or political - for sharing it.

Responses from policymakers will need to be mindful of the challenge of identifying intentional actors, and distinguish carefully between the actors coordinating information operations and those participating in it organically. How to respond effectively and legitimately to the risks posed by uncoordinated information activity will also need further consideration.

Concealed Identity

Another common - but not universal - feature of information operations is a disguised messenger - that is, the identity of the person who is transmitting the information or engaging in the information activity is concealed, either through anonymity or through impersonation.

In 39 cases we reviewed, 30 had a disguised messenger. However, 9 did not - such as those involving state media channels, individuals online, official government communications or politically aligned websites/pages.

Disguised messengers can be a useful flag, therefore, to identify where information activity may be an instance of information operations (though by itself, cannot be conclusive).[42] However, the possibility of transparent messengers in information operations is crucial to acknowledge as though the anonymous trolls and bots may make better headlines, citizens and policymakers should be aware that disinformation can be spread openly by recognisable actors and well-known outlets.

Key examples of opaque messengers would include Twitter bots, such as the Peñabots, to engage in activities like hashtag poisoning, where hashtags being used by government opponents (e.g. to communicate about human rights abuses) are used by bots in spam posts, overwhelming the hashtag with useless content.[43] In this case, the bots conceal who is directing the activity, as a bot appears like an anonymous or unverified Twitter user.

A case of distorted, not simply concealed, messenger identity being used in information operations can be found in the actions of the Myanmar military against the Rohingya, specifically when members of the military created accounts impersonating celebrities and used them to share fake news posts inducing violence against the Rohingya - not only possibly leading more people to believe or share these posts, but allowing the military to evade Facebook bans on their overt activities.[44]

An example of information operations carried out using transparent messengers includes the practice of giving prominence to hand-picked commentators, a tactic of state media organisations. This allows sympathetic information to be spread by commentators who are portrayed as authorities. However, there is no deception involved in who is spreading the message - rather it is the message, and legitimacy attributed to it that are deceptive.

Truth, falsity and deception

'Fake news' is a classic trope in information operations, and refers to false information shared because people believing that piece of information will be beneficial to the sharer's interests.[45] Our review shows that false content is a common feature of information operations that it involves - however, it is by no means the whole story:

- The fakery involved in information operations is not always a property of the content a message is expressing
- Not all information operations relies on deception for its efficacy.[46]

While the majority of cases we reviewed involved some deceptive elements, some did not. Of 39 cases we reviewed, 31 involved deception in some way; 6 did not; and 2 involved both. The majority of cases which we reviewed did involve deception in some way, but this was not restricted to content alone - for instance, false information being disseminated is deceptive, but so is the use of false accounts to share content - true or false - online.

Leaked documents, for instance, in the case of the MacronLeaks, were partially genuine and partially fake.[47] The main issue was not that true or false information was being transmitted but that these documents had been sent into the public sphere in order to damage someone politically. In cases of doxxing, true information is used to reduce opponents' participation in information spaces - which relies on its truth for its efficacy.[48]

'Non-deceptive' cases are, for example, where content moderation or legal systems are being abused, such as the government either offering financial incentives to individuals to report people online who are criticising them (as in Thailand[49]) or the government issuing fines to those who are found guilty of crimes such as 'disrespecting the government' (as in Russia).[50] Another notable instance is the sharing of graphic images, some of which are genuine, to serve as recruitment propaganda by groups such as IS.[51]

Hence if we concern ourselves only with fighting 'fake news', or even deception more broadly, we will be missing an important portion of instances of information operations. It is important not to narrow the scope of what we regard as information operations, especially when considering policy responses to it, to only consider the threat of false content. This is not a battle for fact-checkers alone. Information operations can make use of true content, and false content can be a product of activities which are not information operations. Moreover, focusing on the distinction between true and false content misses that true facts can be presented in ways which are misleading, or in a context where they will be misinterpreted in a particular way that serves the aim of the information operative.[52]

Non-Factual information operations

In some cases, there is no content in the information being disseminated which can be described as true or as false. Of 39 cases we reviewed, 20 primarily involved content which could be assessed as true or false. In 14 cases the salient aspect of the operation was either value-based rather than fact-based (e.g. expressing criticism or disapproval),

or derived its efficacy from process rather than content (e.g. fining dissenters, spamming an online space, promoting certain ads or events).[53]

This reinforces the lesson that we need to look at information operations in a broad context, and not simply concentrate only on whether and how false information is spreading.

For instance, manipulating an algorithm so that political ads are targeted at certain groups is not simply information operations in virtue of the content of those ads, but in virtue of the manipulation of an information environment.[54] Astroturfing and false amplification of news[55] may communicate falsehoods, in that an audience may conclude 'this social media user supports the Government' or 'there is a lot of online support for that policy' - but the purpose is not always to express specific false facts in the messages.

Emotional manipulation

The risk of focusing only on truth or falsity, moreover, is that emotional forms of information operations may be missed, when inflammatory content can incite anger, hatred and physical violence.[56]

In cases of targeted harassment and threats, while some forms do rely for their efficacy on transmitting true content e.g. doxxing someone's true identity, others may not need to be identifiably true or false.[57] The volume and vitriol of attacks in targeted harassment will likely be sufficient to drive someone away from an information space, as has been documented to occur in Bahrain, or even away from engaging authentically in political processes generally.[58] [59]

Other forms of information operations may make claims which can be evaluated as true or false, but whose primary function is not simply to transmit false beliefs but to inflame emotions - such as the Internet Research Agency campaign against the White Helmets in Syria, which includes false claims about the group, such as that they faked chemical attacks, but also emotional content, such as celebrating when members of the White Helmets are killed.[60]

Similarly, circulating news about how a certain group is responsible for violence against another transmits false claims, but does so in a deliberately inflammatory way, which may provoke anger and hatred before any assessment of the likelihood of the truth of the content, as has been seen in Nigeria where fake news foments ethnic tensions and violence.[61] This tactic of exacerbating social divisions will also be shown below to be an aspect of Russian information operations. Inciting hatred against minority groups has long been a tactic of warfare to entrench the power of another group, and it is still very much present in online information operations - and as it is associated with acts of physical violence, not only an altered information space, requires an urgent, robust, and of course evidence-based response.

Is it aligned with the government or against the government?

Most tactics of information operations could be deployed either in service of or against the interests of a government. However, of the cases we looked at in detail, a majority of them were government-aligned.[62] Of 39 cases, 34 were aligned with a government, and 4 were aligned against government.[63] [64]

Moreover, we may typically think of cases of information operations which are between governments - for instance, Russian attempts to interfere in US elections, or defend its actions and allies in Syria through global disinformation campaigns. However, of the cases we reviewed, most were focused on internal audiences (that is, their intended targets were within their own country). Of 39 cases reviewed, 24 focused on an internal audience, 10 on an external, and 5 on both.

Examples of cases aimed at influencing domestic audiences include disinformation campaigns by the Myanmar military, hashtag poisoning by the Peñabots in Mexico, or the 50c party in China.[65] There is clearly some overlap - for instance, fake news intended to justify political actions, for instance, can serve both as domestic and international justification.[66] Nevertheless, it is telling that there are many instances of information operations being effectively conducted by a government against its own people.

These attributes are important to recognise - given that policy responses to information operations will be determined largely by governments, it is necessary to be cognizant of the role that governments play in perpetrating information operations, not only against other governments but against their own citizens.

Targeting Sympathisers or Opponents

The aims, tactics and strategies of information operations are varied and so are its targets.

The majority of cases we reviewed aimed to ultimately impact the information operatives' opponents (to discredit them, spread fake news to turn others against them, to damage their standing and so forth). Of 39 cases we reviewed, 30 were aiming to ultimately impact opponents, 1 to impact sympathisers (IS recruitment videos), and 8 to impact both.

However, how this was achieved varied between engaging with opponents directly to target them with acts of information operations (such as targeted harassment), or engaging sympathisers, through sharing content which delegitimises their opponents, in order to weaponise them against opponents. Of 39 cases we reviewed, 12 were primarily trying to engage sympathisers, 10 trying to engage opponents, and 17 trying to engage both.

When trying to map out how information operations spreads and reaches its final destination, it is necessary to bear in mind the variety of routes through which information activities are directed and disseminated. This also shows how non-information operatives can be implicated in information operations.

Online effects or offline effects

There was also a distinction in where the primary impact of the act of information operations seemed to be intended to occur, namely whether the impact was intended to be online or offline.[67] Of 39 cases reviewed, 27 seemed to have a primary intended impact online, 11 offline, and 1 both.

This is a distinction which helps to illuminate the overall aims of information operations - information can be weaponised in online spaces not only to affect the integrity of those spaces, but to bring about other effects outside of that context. It, however, highlights that changing what happens online often is an end in and of itself, as online spaces become more widespread and entrenched as sites of communication and discourse.

Examples of intended online effects would be getting genuine hashtags removed through hashtag poisoning and deliberately disrupting conversation on Twitter; or using coordinated bot campaigns to simultaneously distribute large amounts of material and so dominate the online discourse.[68] [69] Conversely, examples of intended offline effects would be spreading material intended to incite violence against other groups[70], or trying to affect e.g. voter behaviour in anticipation of an election.[71]

Conclusions

Generally, we can see that information operations involve deliberate deception of some kind; that they are often directed by a government against their own citizens; and that they employ a combination of (allegedly) factual and emotional content to bring about certain behaviours online and offline.

But these features are not universal by any means - and to treat them as such, and focus only on catchy phenomena like 'fake news', risks failing to recognise important instances of information operations. Information operations can use truth and falsity; employees and citizens; sympathisers and opponents; anonymity and publicity; overtly or subtly political content - it is able to weaponise whichever aspects of information and information spaces will serve its aims, and to change form and scale rapidly. Information operations can look like organic activity, and vice versa - meaning detection poses a challenge that needs to be acknowledged. Whether as critical consumers or policymakers, the variety of forms which information operations can take must not be neglected.

The different forms of information operations can also serve to illuminate broader elements of an information crisis - the fact that people will of their own volition engage in government-directed information action; that they will share information which could harm others; that they will believe deceptions even in the face of evidence. The challenge of information operations must be considered in the context of the challenge of the current epistemic environment.[72]

04.

Disinformation in Action

On 17 October 2018, Twitter released data about 9 million tweets from 3,841 accounts affiliated with the Internet Research Agency (IRA), all of which have since been suspended from the platform. The IRA, a Russian organisation founded in 2013 and based in St Petersburg, is accused of using social media platforms to push pro-Kremlin propaganda and influence nation states beyond Russia's borders, as well as being tasked with spreading pro-Kremlin messaging in Russia.[73]

This is one of the first major datasets linked to state-operated accounts engaging in information operations released by a social media platform. Although large, we cannot say with confidence what proportion of Russian state-operated accounts that were active over the period this data represents. We are equally dependent on Twitter's determination that these are indeed IRA accounts. This is a useful window into Russian information operations, but we cannot be sure it is a representative one.

The research team analysed tweets attributed linguistically to three EU countries: Germany, Italy and France; subsequent to a UK case study was published by Demos in January 2019. An initial review of the language annotation metadata provided by Twitter suggested content related to these three countries was prevalent in the data. We then performed our own language annotation on the datasets attributed to these three countries to verify their relevance.

Language testing

This research chose data for each case study according to the language in it was written. This information was included in Twitter dataset, which provides an annotation for each Tweet indicating its language.

In order to test the accuracy of this information, Twitter's annotation was compared against an external, albeit imperfect, 'source of truth': Google Translate's language detection service, which has been benchmarked as performing well in tests between hard-to-distinguish languages. Researchers also tested the accuracy of using Twitter's language detection alongside 'langdetect', a Java language detection library implemented within Method52.

To do this, a measure was first taken of the precision of each language coding - i.e. the % of Tweets coded as Italian which were actually written in Italian. A random 1000 Tweet sample was taken from Tweets judged either by Method52 or Twitter to be written in each language. We then tested each of these samples against Google Translate, producing the following results:

PRECISION	Twitter	Twitter and Method52
Italian	87.1%	95.8%
German	92.3%	96.8%
French	32.7%	66.3%

Fig. 3 - precision of language annotation in labelled Tweets

A measure was also taken of recall - i.e. the number of Tweets actually written in a language which would not be correctly labelled using each strategy. A large random sample of 9,329 Tweets (chosen to be large enough to be representative) was taken from the whole dataset and analysed using Google Translate. Researchers then assessed how many of these Tweets, both alone and combined with Method52, each method had labelled correctly.

RECALL	Twitter	Twitter and Method52
Overall sample - Italian	92.9%	87.0%
Overall sample -German	94.2%	93.1%
Overall sample -German	82.0%	72.0%

Fig. 4: Recall of language annotation in labelled Tweets

As shown above, the use of Method52 language labelling alongside that provided by Twitter tends to improve accuracy without causing a considerable drop in recall. This is particularly true for French content, for which (according to Google Translate) only one in three Tweets was correctly labelled by Twitter. Use of Method52 in this case doubles precision - although this analysis shows that we should still expect one in three French Tweets to be mislabelled.

Throughout the research below, we have only included Tweets labelled by both Twitter and Method52 within the dataset for each language.

The final German dataset contained 94,529 tweets by 858 accounts; the final Italian dataset contained 17,437 tweets by 522 accounts; and the French dataset contained 5551 tweets by 860 accounts. The first tweets occured in early 2012 but the majority of the content was occured from 2014 onwards. The last towards end of 2017, when the last of the accounts appears to have been suspended by Twitter.

The analysis of these three countries is based on unsupervised metadata analysis, analysis of hashtag use, and translated sampling of the data.

This analysis identified four key themes, discussed below, and are we believe crucial characteristics of information operations that those looking to resist it must prepare for. .

1. They are characterised by erratic bursts of activity rather than consistent output
2. Not just focused on electoral politics but exploiting social tensions too.
3. The action is coordinated but appears inconsistent across time and geographies.
4. This is not just ‘fake news’

Bursts of Activity

The first key theme is that activity is concentrated in bursts around particular events, rather than a consistent stream of activity. These dramatic increases in activity are unpredictable, sometimes significant events like terrorist attacks, referendums and elections trigger massive spikes and other times they go by completely unremarked. These spikes give only a few days for fact-checkers and moderation efforts to respond before activity subsides. If these spikes could be predicted with some confidence, then pre-emptive action and preparations could be taken.

Terror Attacks

The most intense periods of activity above often correspond to high-profile terror attacks, be it Hamburg or Brussels.

In the French data, the single most active day was March 22nd 2016, the day of the Brussels bombing terrorist attack, with 142 tweets. Prior to this, the activity had mostly concerned miscellaneous chatter about sports, television, general news etc. This altered drastically on the 22nd, with content turning to discussion of specific details of the terrorist attack and promoting anti-Islamic sentiment. In this period, 21 tweets were sent containing #IslamKills and 16 tweets used the hashtag #StopIslam:

"#StopIslam #IslamKills eh recommencez meme pas avec vos #PrayForBrussels la comme si a allait changer qqchose"

Yet the Paris terror attacks the November before, the deadliest in French history, provoked a substantially smaller uptick of activity and anti-Islamic sentiment, not significantly different from the period surrounding it.

Again, in the German data, a clear spike can be seen in July 2016, around the time of the Wurzburg, Ansbach and Reutlingen attacks, and again, in July 2017, when the Munich shooting and Hamburg attacks take place. However, this tactic is again inconsistent. For example, the attack on Berlin in December 2016 occurs when activity appears to be at its lowest, despite being one of the most deadly in this spate of attacks. Further, the Dusseldorf and Munich Knife attacks are not particularly active periods, compared to the weeks around them.

This is in contrast to the previous UK case study, where terror attacks were the central driver of much of the most widely shared material and provoked reaction with every incident.

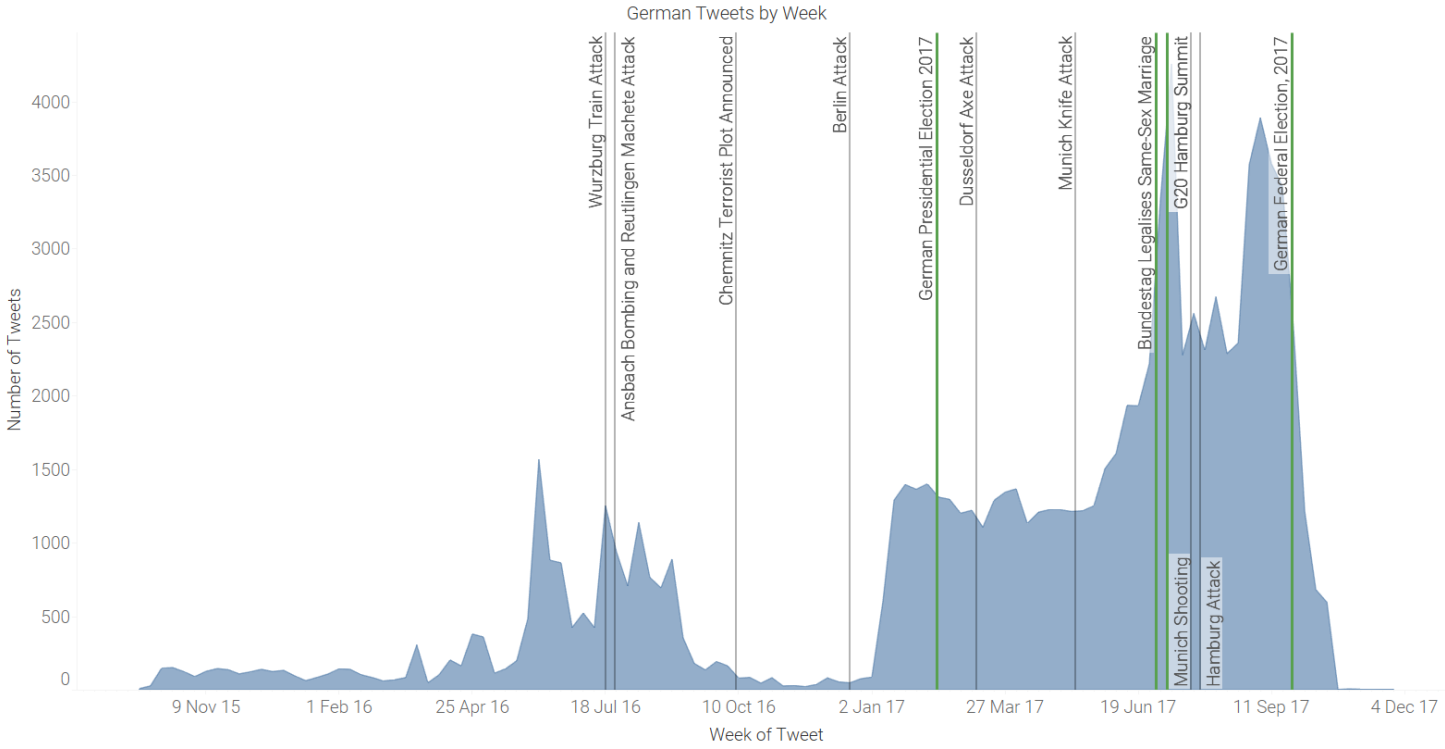

Fig 5: Number of Tweets per week by IRA operatives in German-language dataset between October 2015 and December 2017

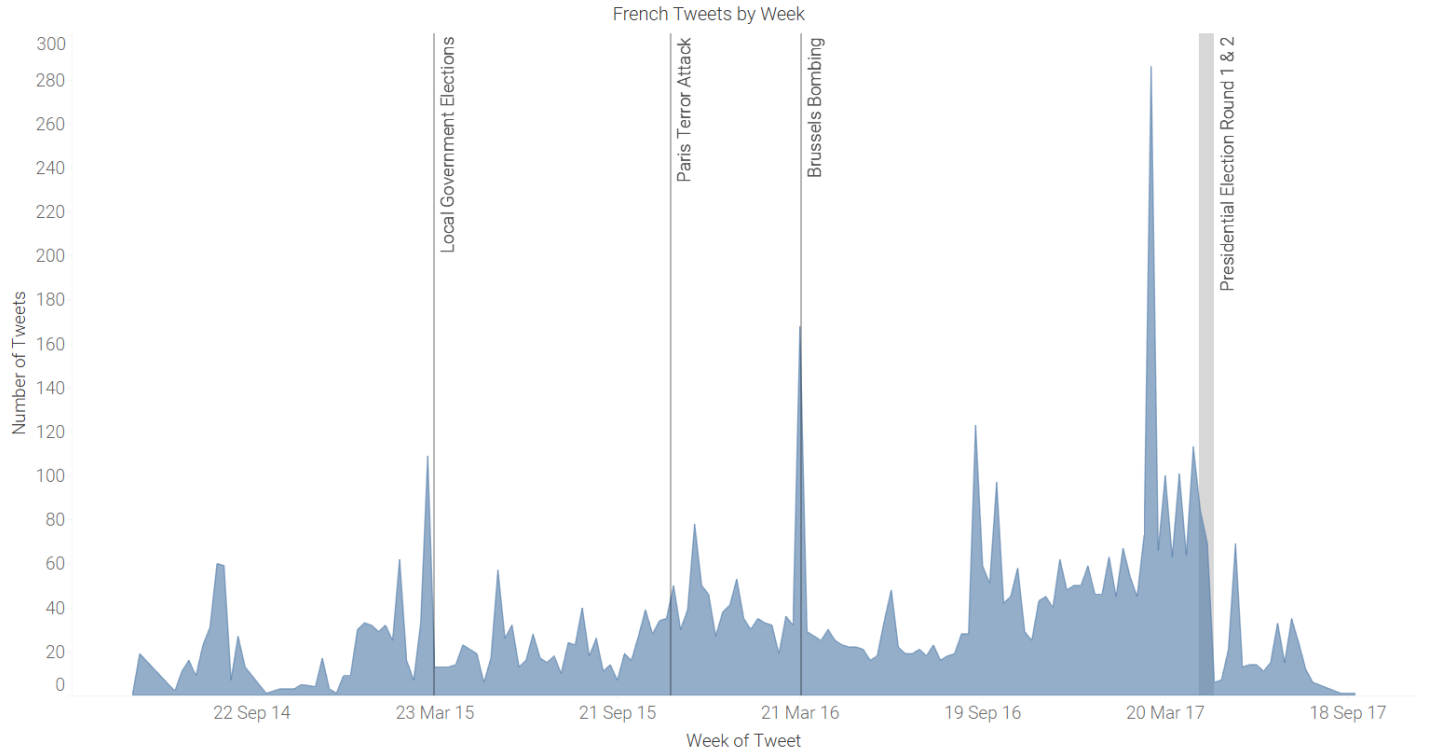

Fig 6: Number of Tweets per week by IRA operatives in French-language dataset between June 2014 and September 2017

Electoral and political events

Information operations surrounding elections are a source of global concern, particularly following the US 2016 election, in which Russian interference has been alleged to be a significant reason why Trump won.[74] Our analysis of the data did indeed display a pattern of increased activity around electoral events.

For two years between October 2015 and March 2016, the German dataset shows long periods of relative inactivity, followed by sustained periods of concentrated Tweeting, and punctuated by high-volume spikes, often lasting a few days. This suggests that accounts were being kept 'dormant' until needed for a concerted push, with low levels of activity maintained to increase the apparent legitimacy of the accounts.

This approach changes notably in January 2017, with a sudden uptick in the period leading up the German presidential elections, when a high level of activity - over 100 German language Tweets per week - is maintained until the federal elections later in the year. The federal elections see another dramatic uptick even compared to the previous sustained activity. The sudden fall in tweets seen in October 2017 is likely to be due to the accounts being identified and shut down by Twitter - if so, this graph suggests that this activity might otherwise have been maintained.

There was also a significant spike around the G20 summit in Hamburg, the single most active week in the German dataset. The most used hashtags, when grouped by topic, show that over 300 tweets sent during this period contain hashtags directly related to the G20.

The French dataset demonstrates a similar pattern of inactivity followed by sustained uptick around electoral events. The first French Tweet was sent in May 2012, and volumes do not reach double digits until May 2014. The first clear spike in the data occurs in the week leading up to the French local elections in early 2015.

By far the most active week in this dataset is the week beginning 6th of March, 2017. However, this spike in volume does not appear to contain any directly malicious intent. Instead, the content consists primarily of Tweets about flowers, songs, and International Women's Day.

As this occurs only three months before the 2017 Presidential election, this may well be an attempt to blend in and seed seemingly normal accounts in preparation for the electoral event. Shortly after this week, the discussion does appear to shift primarily to discussion of French domestic politics and remains at much higher level than it was previously.

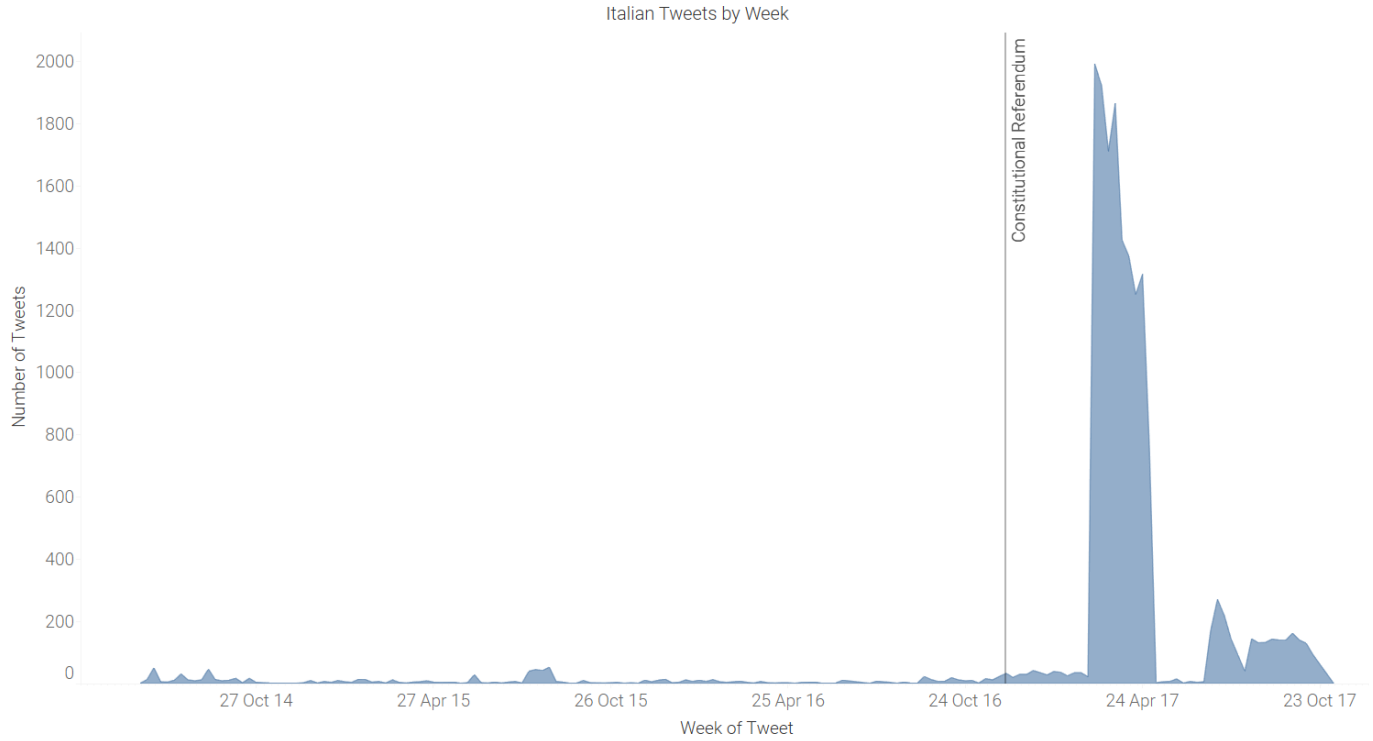

Fig 7: Number of Tweets per week by IRA operatives in Italian-language dataset between July 2014 and December 2017

The first message sent by the Italian accounts are in December 2012, but tweet volume does not enter double digits until July 2014. Unlike the countries examined in this and our previous report, Italy did not experience any terrorist attacks during the period these accounts were active.

Neither did they have any national elections, though they did have a national constitutional referendum in 2016, leading to the resignation of the then current Prime Minister, Matteo Renzi, a week later. Yet, Figure 7 shows little activity leading up-to and in the immediate aftermath of the referendum.

Instead, activity was intensely concentrated in March and April 2017, with a brief and significantly diminished resurgence in July and August 2017, with no obvious national events they apparently targeting. There is a similarly unexplained spike in activity in the French dataset around September and October 2016.

All of this taken together paints a chaotic picture where constant low-level activity is punctuated by sudden and dramatic spikes. These spikes give only a few days for fact-checkers and moderation efforts to respond before activity subsides. If these spikes could be predicted with some confidence, then pre-emptive action and preparations could be taken.

Elections are certainly predictable with at least a few weeks notice but terrorist attacks, the other major target of activity, are by their nature unexpected. Further, across both categories we identified as causing bursts of activity, we see spikes sometimes and not others without any obvious pattern. Finally, sometimes bursts of activity occur seemingly unrelated to anything at all, with a flurry of all kinds of content yet none of it overtly political or divisive.

All of this taken together makes both preparing counter-activity difficult and responding to every spike as it happens (if they can be identified at all) highly inefficient even if it does prove effective.

Party-Politics and Divisive Issues

While it is often presumed that the target of Russian interference in Western democracies is directly on electoral processes, we find that it is just as much about stirring up cultural and social divisions without any direct party-political connection. Still, there are notable upticks in activity around elections and a fair amount of focus on political parties.[75]Tactics to influence overtly political processes as well as exacerbate existing social divisions were found in the literature review, in particular in order to achieve the aim of reducing oppositional participation (though that aim cannot be conclusively extrapolated to this dataset). Disinformation in particular has been described as consistently being 'either ethnocentrically prejudiced or...ideologically motivated'.

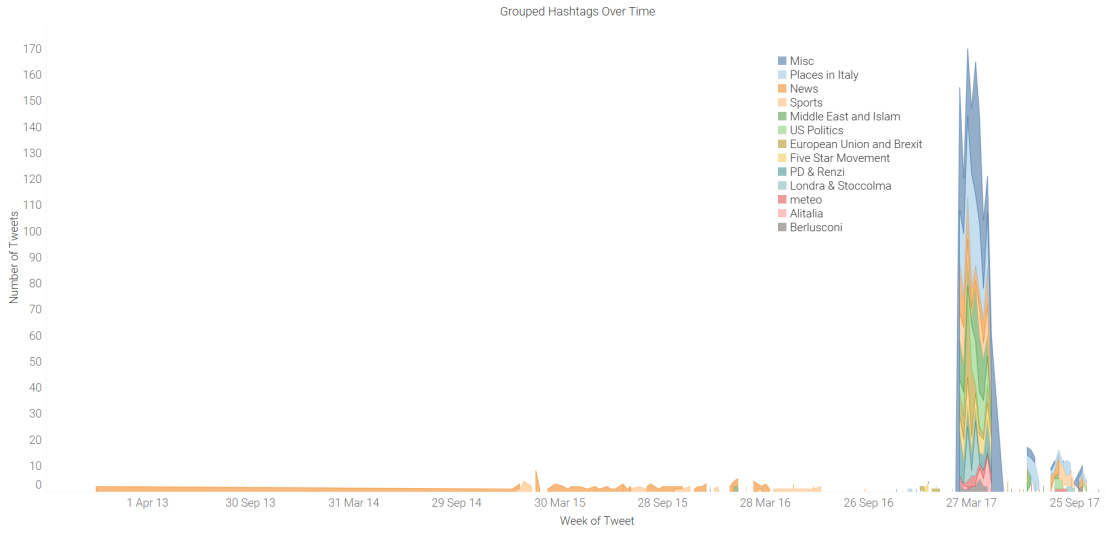

Fig 8: Number of tweets, containing hashtags grouped by topic, by IRA operatives in Italian-language dataset between November 2012 and November 2017

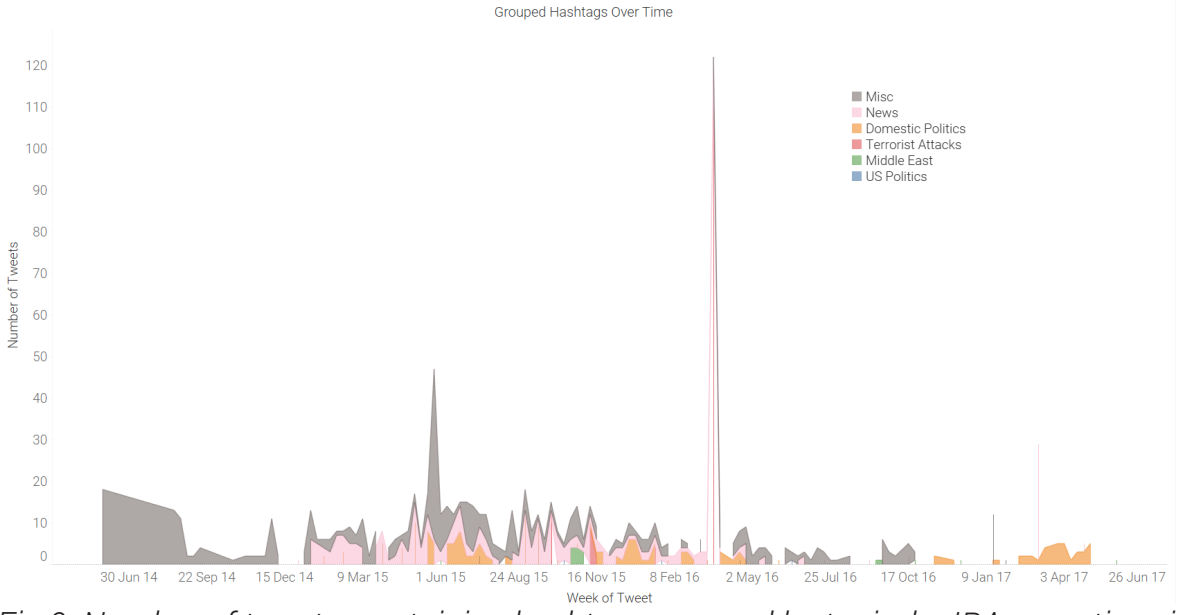

Fig 9: Number of tweets, containing hashtags grouped by topic, by IRA operatives in French-language dataset between June 2014 and June 2017

Domestic Party Politics

Through all the datasets, discussion of domestic party politics is a consistent feature, unsurprisingly being mostly concentrated in the run-up to electoral events.

In the German dataset, the Christian Democratic Union, the Social Democratic Party, Martin Schulz (leader of the SPD) and Katja Kipping (Chair of Die Linke, a left-wing party), are in the top 50 most mentioned accounts and among the few not journalists or newspapers. The French dataset is somewhat more sparse but Marine Le Pen does come out as the second most mentioned figure, at 83 mentions, and Emmanuel Macron also received 31.

Overall, the discussion of the CDU and SPD seems pretty neutral, and mainly consists of sharing factual articles written by or about them, along with the occasional supportive statement. Early Tweets portray Merkel in a positive light - #Merkelmussbleiben is the third most popular hashtag in the dataset overall - but was only Tweeted during July 2016. By the time the 2017 Bundestag elections arrive, attitude to Merkel is much more mixed.

However, especially as the Bundestag elections approach, state-run accounts appear increasingly to push pro-AfD comments and tweet far more about the AfD than other parties, sending, for example, 281 tweets using the hashtag #AfD versus 210 containing #CDU, and 177 for #SPD.

#AfD ist die aufrichtigste Partei auf dem politischen Feld Deutschlands, was die #Turkei Frage angeht #Erdogan #Gabriel https://t.co/qjKjGX9M3N
Mit #Merkel in den Untergang oder warum ich habe #AfD gewahlt! #BTW17 #Deutschland #wahleAfD https://t.co/ObGUB4iCWm

The above shows that, rather than remaining committed to supporting a single party, accounts were flexible in the approaches and stances taken, and responsive to campaigns and events.

Mentions of party-politics also appear in the Italian data, mostly concerned with criticism of Matteo Renzi, the then prime minister and support for the Five-Star Movement, a left-wing movement rather than the right-wing parties Russia had shown a preference for in other countries, but one that was more sympathetic to Russian interests than other Italian parties.[76]

The G20 Summit

The single most active week was the week in which the G20 summit took place in Hamburg. The most used hashtags, when grouped by topic, show that over 300 tweets sent during this period contain hashtags directly related to the G20.

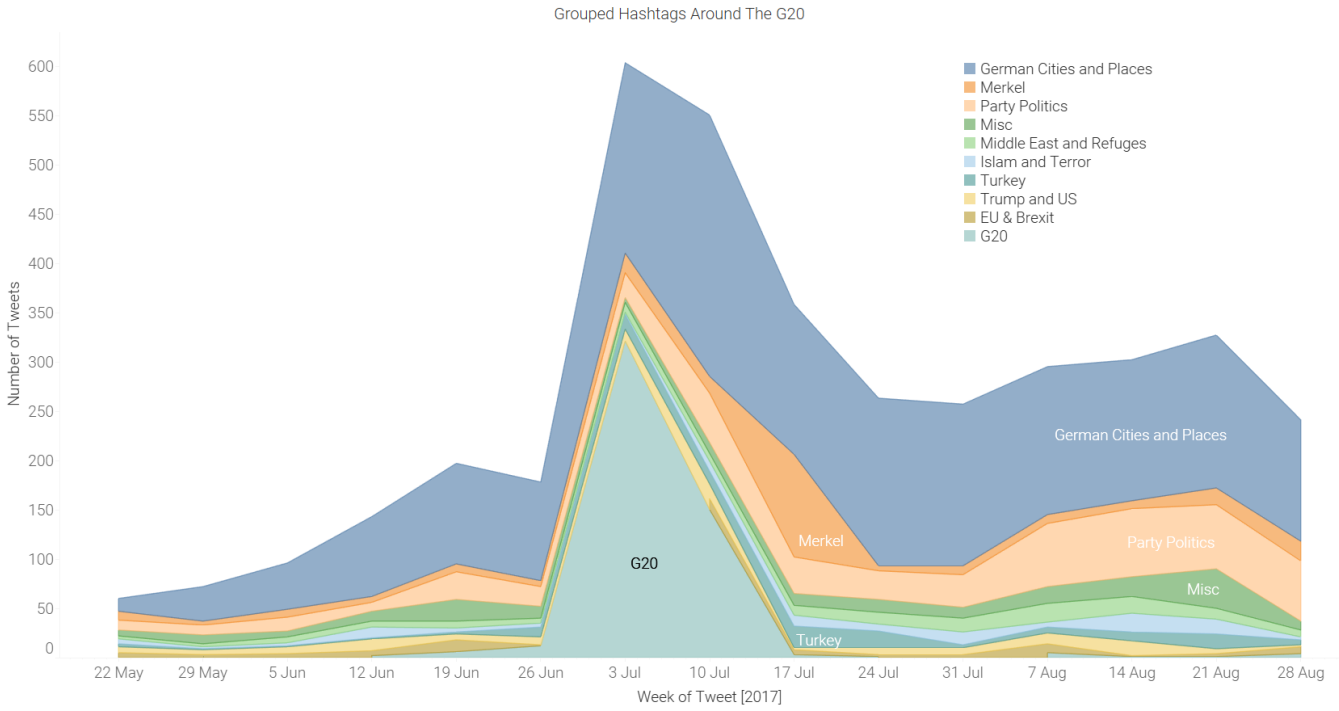

Fig 10: Number of tweets, containing hashtags grouped by topic, by IRA operatives in German-language dataset between May 2017 and September 2017

Interestingly though, while this event might be expected to bring with it a significant amount of geopolitical messaging, the narrative being pushed here by the IRA, both through tweets and retweets, is almost exclusively focused on the police and protesters (though criticism of Erdogan does also appear, which we discuss later on). Specifically, accounts can be seen retweeting factual articles about police movements along with very pro-police and anti-protest sentiments, setting things up as a conflict between order and chaos rather than something directly party-political or country specific.

We have already noted information operations being weaponised against protestors in other contexts, such as through the Peñabots in Mexico. In the Mexican case, however, hashtag poisoning was used by a power to disrupt protests hostile to that power. Here, Russia is criticising protestors against a government which is not their natural ally. It is possible that this represents an attempt to sow division by portraying protesters as violent enemies of the police to concerned citizens following the event through major hashtags.

For example:

Staat der nicht mehr zu seiner Polizei und seinen Soldaten steht, ist nicht mehr mein Staat #G20Ham #Hamburg #G20 https://t.co/JCxbOvSHl0

Ich bin stolz auf unsere Polizei..Was diese wieder geleistet haben, zollt hÃ¶chsten Respekt #g20protest #Hamburg #G20 https://t.co/oFkgj5ybUV

#Polizei starmt #G20-Protestcamp in #Hamburg. Vielen Dank an die @PolizeiHamburg! https://t.co/LvX2mivBLS

European Union

Surprisingly, this research found very little mention of EU institutions, or conversation around the EU as a construct. No German Tweets were found containing @mentions of EU institutional accounts, MEPs and other senior EU figures, and only 580 mentions of EU related keywords were identified, representing 0.6% of the total dataset. (A full list of keywords used is included in an appendix to this document).

Researchers did find 563 Tweets containing an EU-related hashtag, found within the Top 100 hashtags, and the EU was the 7th most popular hashtag topic group in this list. However, this discussion was pretty much exclusively focused on Brexit and spiked in the couple of weeks prior the Brexit referendum.

As in the German case, Italian Tweets sent by the IRA were broadly silent on the topic of the EU. No Tweets were found by searching for @ mentions of EU institutions, MEPs and other senior EU figures in the dataset, and a search for EU Related keywords found only 207 Tweets, making up a mere 1.2% of the dataset. 100 Tweets with EU-related hashtags were found, and were equally split between discussions of Brexit and tweets related to the 60th anniversary of treaty of Rome and the EU more generally.

All tweets concerning the 60th anniversary were sent between the 24th and 26th of March. Many of these were retweets of pro-EU messages, but linked these to the need to deal with terrorism, e.g.

"RT @Quirinale: #EU60 #Mattarella:Ancora una volta il terrorismo ha colpito, a un anno dagli attentati di Bruxelles, una delle capitali dâ€™Euâ€¦"

"RT @RaiNews: In diretta ora il presidente Mattarella #EU60 "contro terrorismo occorre risposta comune"â†' https://t.co/97WGphzFBm #TrattatiRoe¦"

Discussion of the European Union did not feature heavily in the French dataset either. We found 117 mentions of EU-related keywords, representing 2.1% of the data. There was no mention of the EU in the hashtags used; Brussels was mentioned but only in relation to terrorist attack, e.g. PrayForBrussels

The only notable specific EU individual at all prominent in the dataset was Federica Mogherini (@FedericaMog), High Representative of the EU for Foreign Affairs and Security Policy. Vice President of the EU Commission. She is mentioned 22 times in the dataset, and is the 11th most mentioned account. This content appears to just be retweets of factual coverage about her work in the Middle East, e.g.

"RT @eu_eeas: .@FedericaMog ""UE a un interet strategique a soutenir le #Liban, ses institutions et peuple libanais"". Conf. de presse avec @G"" - 23 January 2017

"RT @eu_eeas: .@FedericaMog rencontre MAE #Algerie Ramtane Lamamra. Importantes discussions sur relations bilaterales & situation regionale" - 10 April 2017

It is odd that such a pivotal institution, especially one that has been a relentless target of Russian criticism in the past, garners such little attention in this data. Nevertheless, It

highlights that specific electoral processes and democratic institutions are not as much of a focus as we might have previously assumed.

Social Divisions

Opposition to migrants and amplifying of stories related to volume of migrants and migrants failing to integrate is present across all the data, though most obviously in the German data. This is a phenomenon which has been previously seen in cases of information operations and misinformation in Europe, including in Italy and Germany.[77] They also implicitly and explicitly relate migrants to ISIS and terrorist attacks and the discourse around the migrants is tied up in Islamophobia.

"#Merkel bittet #Migranten um #Toleranz furr #Schweinebraten Was sie sagen sollte: Wenn es dir nicht passt"

"Im Juli sind weniger #Migranten in Italien angekommen als in den Monaten zuvor. Es klingt nicht schlecht!"

"Warum kÃ¶nnen unsere Kriegsschiffe diese #Migranten nicht sofort zurÃ¼ckschicken? #stopptTerror"

A focus on anti-Islamic emotional manipulation after terrorist attacks was a key feature of operations we identified in the UK and this appears to be a consistent theme through Russian operations around Europe.

Not all of their focus on social issues is traditionally far right. For example, in the French dataset on International Women's Day, they appear to be complaining about gender inequality, for example, on unfair naming of streets:

"Des fleurs gratuites dans la rue, c'est bien marrant! — #InternationalWomensDay #MakeHerSmile #JourneeDesDroitsDesFemmes https://t.co/rbpGFHGBQM"

"Faites plaisir aux femmes en leurs offrant des fleurs! Bon #JourneeDeLaFemme a toutes les femmes! #IWD2017 #MakeHerSmile https://t.co/YdqTMNrV1x"

Russia's Foreign Policy Objectives

Criticism of Erdogan is present throughout the German dataset - consistent with the Russian government's involvement in discourse within another country with whom it has an at times uneasy relationship. This content is particularly prevalent during the summer of 2016, following the attempted coup in Turkey on the 15th of July, and subsequent purges throughout the summer. Russia's information operations regarding the conflict in Syria are well documented, and are discussed above.[78]

The dataset occasionally featured criticism of Erdogan specifically for attacking journalists, especially around the time of the G20.

Ich halte #Erdogan's bewaffnetes Sicherheitspersonal fur wesentlich gefÃ¤hrlicher als

die Demonstranten #G20 #Hamburg https://t.co/c3EiYElh3c

Die Nachricht gefÃ¤llt dem #Erdogan... Schwarze Liste bei #G20: Journalisten arbeiteten in turkischen Kurdengebieten https://t.co/IYeff3f1wr

Germany may have been targeted in particular in this way as the country has a substantial Turkish population, and Angela Merkel repeatedly condemned Erdogan over the period.

"Erdogan ist verrackt! Turkei setzt Europaische Konvention fur Menschenrechte aus https://t.co/3UYvOw7qQz"

Interestingly an anti-Israeli account, @opboycott, features quite highly in the French dataset, with 43 mentions - the 3rd most overall. Mentions of this account exclusively retweet and amplify content focused around Israel and Palestine, e.g. calling Netanyahu a war criminal and condemning Israeli attacks on Gaza. Israel-Palestine is widely regarded a divisive non-domestic issue and criticism of Israel fits into a wider pattern of attempting to reduce support for countries in opposition.

"RT @opBoycott: 1-Manifestation a #Londres contre la visite aujourd'hui du #CriminelDeGuerre, Benyamin #Netanyahu! #UK #NotWelcome #Boycott"

"RT @opBoycott: Les avions sionistes ont recommence ce matin,d'asperger de pesticides toxiques,des terres agricoles Palestiniennes,sur le Suâ€¦".

Taken together, the themes above underline the importance of looking beyond political events and moments when imagining possible targets for information operations and planning responses. Targets are frequently cultural and social, particularly in moments of vulnerability such as in the wake of a terror attack, and the objectives longer-term than a single election.

Coordinated but Inconsistent

No clear focus

There often appears to be no clear focus to the messaging, even during periods of intense activity. This is most apparent in the Italian data, where sampling and hashtag grouping suggests that the significant burst of activity between February and April 2017 appears to be completely unfocused activity. It covers an assortment of topics which include International Women's Day, the Alitalia strike and subsequent administration, US politics, Five Star and Democratic Party, general sports and much more, without any taking predominance over the others.

This may be due to a lack of effective coordination, or may be symptomatic of the tactic discussed above, whereby accounts engaging in information operations take steps to appear like 'normal' accounts, either in order to avoid detection or to make more people engage with or take their disinformation seriously. This is another layer

of deception on top of having a disguised messenger - not only concealing the identity of the messenger, but taking steps to create an alternative identity for them.[79] It could also be occurring with the aim of reducing the quality of the information environment by increasing inauthentic content. It is also possible that activity on these accounts was increased in preparation for a concerted action, which was then called off or interrupted by Twitter takedown of these accounts.

The case is not so stark in the French data but hashtags within the tweets sent by the Internet Research Agency suggest a significant proportion of the tweets sent are talking about miscellaneous topics like sport, the weather, food etc. especially towards the beginning of the dataset. However, they do appear to become more focused towards the end of the information campaign, a pattern which also appears in the German data, e.g. after the G20, activity becomes much more focused on party politics.

Previous analysis of IRA activity in the USA found that the IRA employed tactics including the dismissal and redirection of attention of social media users from political issues (as China's 50c party does), as well as the creation of entire, ersatz information ecosystems to build trust with specific demographics who could then be targeted with political content.[80] This focus on non-political news may be part of a similar strategy.

Connection with other Russian interference

In January 2016, there was a serious case of Russian state and media apparatus spreading disinformation about and within Germany.[81] On January 11th, a 13 year old Russian-German girl, Lisa, went missing for 30 hours and it was falsely reported by First Russian TV that she was raped by migrants, when in truth she had throughout been safely with a friend. Despite being a fabrication, the story was intensively reported in Russian domestic and foreign media, even being referenced by Russian Foreign Minister Sergei Lavrov.

Strikingly, there is absolutely no mention of this incident in the dataset. There are references to refugees and migrants from January 11th to the end of the month but we could find no indication of state-run accounts trying to boost this story, even while it had originated from their own media sources.

There are three possible explanations for this (which are not mutually exclusive):

1. The IRA felt the story was getting sufficient coverage by traditional media, and didn't feel the need to intervene.

2. There was a lack of coordination on the part of the Russian state's disinformation campaign, either due to organisational constraints, decentralisation and initiative given to operatives, or even competition between various divisions of the campaign.

3. Social media accounts were responsible for spreading the story on this occasion, but are not included in this dataset. This could be due to identification limitations. Twitter's analysis may have been unable to find all the Russian state-run

accounts, with the most sophisticated ones escaping detection. It could also be due to platform limitations, e.g. this story was promoted primarily via Facebook or other platforms.

We know that the Internet Research Agency has used the issue of vaccinations and the rise of the anti-vaxxer movement as a wedge issue in the US, stoking tensions on both sides. In Italy, vaccines has become a particularly political issue with populist parties Lega and M5S opposing vaccination legislation in their 2018 election campaigns. However, using keyword searches for relevant terms, e.g. vaccino, anti-vaccini, vaccinazione, etc. we could only find 11 references to vaccinations, with the content being pretty equivocal.

Similar to the Lisa case above in the German case study, this could simply be a product of Russian state actors pushing this narrative on different platforms in Italy. However, it may also suggest that this issue is actually more home-grown and organic than we might like to believe, and so may require a different response.

Not Just Fake News

The analysis of information operations globally showed that the use and efficacy of false content is only a subset of what information operations aim to do and how they work. Analysis of these datasets supports this finding.

Across all three datasets, there is a significant focus on the accounts of journalists and newspapers. This seems to suggest their main intention was to amplify existing stories from real news sources to push a particular narrative, or an attempt to push specific pieces of information on to real journalists who could then produce 'clean' stories based on that information.

A significant majority of the top 50 most mentioned accounts involve the German press, both local and national. The most mentioned account is @welt, which appears in 1124 Tweets, with @spiegelonline, the second most mentioned, appearing in 456. In the Italian dataset 24 of the 25 most mentioned accounts were reputable news outlets, tv channels and radio channels. The only account in the top 25 which didn't fit this description was @elena07617349, which appears to be one of the suspended state-run accounts themselves. Like with the other datasets, news outlets and journalists make up the bulk of the mentions in the French dataset.

Another strand of the operations is much more normative and provocative rather than factual. This particularly evident around the Islamophobic content and narrative-generation during and right after terrorist attacks.

Die Frage der #Moscheenkontrolle soll immer neu angesprochen werden #stopptTerror
Wer die Terroristen ausbildet, sollte in der HÃ¶lle brennen #stopptTerror

Vor der Terrorgefahr sollte sich keiner beleidigt fÃ¼hlen, es geht um die Sicherheit von jedem #stopptTerror

In the German dataset, both of these can be very clearly seen in their targeting of the G20 protests. Accounts can be seen retweeting factual articles from reputable new sources about police movements along with very pro-police and anti-protest emotional sentiments that lack any claims about facts at all.

Crucially, none of these tactics are 'fake news'. Certainly they are trying to change people's beliefs but not through the spread of verifiably false information, but rather by selectively highlighting some information above others and setting the tone of the debate.

Overall Insights

While our previous report examining the Internet Research Agency's efforts in the United Kingdom found that exploiting division after Islamic terrorism proved the central part of Russia's strategy, these new case studies paint a more mixed picture. There is clear exploitation after the Brussels attack in the French dataset but the Paris attacks, one of the most severe acts of Islamic terrorism in Europe, prompted a relatively minor reaction in comparison. Similarly, in the German dataset, the Berlin truck attack which killed 12 people, marked one of the most inactive parts of the data, though other attacks, particularly Hamburg, did receive attention and traction.

This is not to say that Islamophobia is not a clear undercurrent of all the case studies. It appears to focused be more on the sharing of news stories about (implicitly or explicitly Muslim) migrants, refugees through the time-period across each case study. This is presumably sowing the seeds to shift into pushing a more emotional, directly Islamophobic, narrative during and right after terrorist attacks. This is clearest in the reaction to the Brussels bombing, e.g. #IslamKills #StopTerror.

This shift from baseline sharing news content to more normative discussion also occurs around the G20 when discussing the protests, where it appears to be much more praising the police and demonising the protests than for instance the occasional news story about police movements being shared, where discussion of police before the G20 was more focused on reports of police tackling crime. The extent to switch this seeding-a-narrative followed by emotive exploitation during an important event needs to be explored more deeply but does at least appear to be a theory of tactics worth exploring.

There also appears to be much more focus on domestic politics across these three case studies compared to the UK. They focus on, and astroturf in favour of, more populist and pro-Russian politicians and parties in the run up to national elections, e.g. Marine Le Pen in France, AfD in Germany and Five Star in Italy. This may be due to the more proportional nature of these systems, which makes marginal support for more fringe parties more valuable than in the first-past-the-post system in the UKIP where supporting parties other than Labour or the Conservatives, both relatively anti-Russia, isn't a good use of resources.
Finally, affecting sympathetic changes in attitudes and behaviour and reducing the

quality of the communications environment appear to be the two main aims of the majority of content produced by the Russian state-run accounts across these datasets. For example, the false implication of traditional new sources and a focus on journalists and news outlets appears to be a prominent part of their methodology, with these making up the vast majority of the most mentioned accounts across all three case studies. This is combined with providing false support to extreme, minority, views through astroturfing and a significant amount of spam, though this may be an attempt to blend in and appear more like a normal account as the spam is generally not politically relevant content.

More research is needed to establish the precise aims of these information operations, but these findings are plausibly broadly consistent with the aims identified above, of reducing oppositional participation, affecting sympathetic (or at least politically expedient) changes in behaviour and perception, and reducing the quality of the information environment/available information.

Conclusions

The advent of the digital world, and its subsequent evolution into a battleground, is one of the chief threats to democratic progress. Its exploitation in the service of a new kind of information operations presents a major challenge to national governments around the world.

It is of central importance that we are clear about what this threat looks like. A myopic focus on one small part of information operations risks distorting our response.

A focus on 'fake news', for instance, overemphasises the importance of 'fact' and fact-checking, and ignores the role of emotional manipulation.

A focus on disinformation and misinformation ignores the role played by traditional media organisations, and the selective amplification of content that is factually accurate. A focus on 'troll farms' and state-sponsored information operations risks underplaying the importance of the wider digital ecosystem that make this kind of warfare possible. A focus on Facebook cannot come at the cost of ignoring the legion smaller platforms that play a critical role in these efforts. As shown in the taxonomy in sections one and two, there are dozens of strategies and tactics employed in information operations.

It it, however, still possible to identify these tactics, to identify the salient aims and objectives of information operations. Recognising the breadth of threats should not lead to decision paralysis. It shows the need to be aware of the diversity of forms information operations can take and be alert to what features may indicate an act of information weaponisation by foreign actors. It will also help guide our thinking as to who, ultimately, has responsibility in managing these threats. It requires a coalition across government, the military, technology and civil society to predict, identify, take precautions against, and if necessary respond to their use.

It demonstrates the need to look deeper into the conditions within which acts of information operations are most likely to be successful, and at who the victims of these acts are. It also highlights that there are forms of information activity which do not qualify as information operations, but may still require preventative action. It also shows that further research is required into the possibilities and ramifications of applying national and international legal systems to situations of information operations, and whether those systems are fit for purpose in this rapidly changing context.

The review of data pertaining to some Internet Research Agency activity in France, Italy, Germany and (previously) the United Kingdom underlines this. Across all four countries, an undercurrent of islamophobic and anti-refugee activity is present. At times, this is explicit and obvious, such as in the spikes in activity around attacks in Brussels and in London, complete with the spreading of lies and false information. At other times, this activity is subtle and drawn out, evidenced in the long-term amplification of media and voices aligned with the aims and objectives of the IRA.

As the 2019 European elections draw near, this report calls for action and awareness. In the short-term, it will be vital for governments and technology companies to work together in exposing the exploitation of digital communications platforms in the most explicit way, and to support those NGOs and civil society groups who are able to respond

most effectively to elements of information operations.

But this is not enough. We must recognise that the transformation of the digital world into a battlefield has altered the vulnerabilities of our society to hostile influence, and that the vulnerability will be long-lasting. Longer term solutions around regulation, platform architectures and perhaps even digital literacy initiatives will be essential.

Finally, it's vitally important that in our drive to fight against information operations, we do not conflate it with political expressions online. There is no doubt that the online world has created new spaces for new politics, and with it have come expressions of political belief that can be uncomfortable. Bundling these in with information operations and attempting to legislate or regulate them out of existence will cause more harm than good.

Appendices

Appendix 1: Examples of information operations

Putting together true news and circulating in a way which allows false inferences to be drawn, (e.g. in USA, chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf)

Elevating/citing fringe commentators who perpetuate disinformation, (e.g. in Russia, medium.com/@Brian_Whit/vanessa-beeley-the-syrian-conflicts-goddess-of-propaganda-2c84f850dba4; thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf)

Fabricate millions of social media comments per year at coordinated times, (e.g. in China, gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf)

Use personal data to target political ads, (e.g. in USA, theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far)

Co-opting government petitions, (e.g. in Russia, wired.com/story/misinformation-disinformation-propaganda-war/)

Making and distributing content critical of opponents on social media, (e.g. in USA, theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/)

Spreading false claims of violence against others by particular groups, (e.g. in Myanmar, scholarspace.manoa.hawaii.edu/bitstream/10125/59711/0271.pdf)

Creation of sites mimicing authentic news sites to spread propaganda, (e.g. in Iran, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Using chat bots to engage people on political issues e.g. deportation, (e.g. in UK, ft.com/content/49f19c76-3375-11e9-bd3a-8b2a211d90d5)

Create accounts posing as celebrities to disseminate propaganda, (e.g. in Myanmar, mic.com/articles/191899/myanmar-military-members-fake-news-facebook#.ggl3PU9Of)

Posting graphic propaganda videos showing executions, explosions etc., (e.g. in Syria, theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war)

Posting pro and anti-vaccination messages to sow discod, (e.g. in Russia, bbc.co.uk/news/world-us-canada-45294192)

Spreading news about fake suicide challenges, (e.g. in UK, theconversation.com/momo-

challenge-shows-how-even-experts-are-falling-for-digital-hoaxes-112782)

Claming particular groups are bad actors, terrorists or anti-democratic, (e.g. in Nigeria, bbc.co.uk/news/resources/idt-sh/nigeria_fake_news)

Creating fake websites to pretend to be allies of a political cause, (e.g. in Iran/Syria, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

High-reach accounts using hashtags hundreds of times to dominate discourse at key news moments, (e.g. in Russia, thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf)

Fining those who spread 'fake news' or 'disrespect of the state', (e.g. in Russia, bbc.co.uk/news/world-europe-47488267?ocid=socialflow_twitter)

Introduce fake hashtags and use bots to overwhelm them so they knock genuine hashtags out of trends, (e.g. in Mexico, motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent)

Overwhelm real hashtag with spam (via bots) so that the hashtag is no longer useful, (e.g. in Mexico, motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent)

Overwhelm real hashtag with spam (via bots) so that the hashtag is detected as spam and removed, (e.g. in Mexico, motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent)

Coordinated campaign of accounts simultaneously retweeeting false or defamatory content, (e.g. in Russia, thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf)

Assert that certain groups are terrorists, celebrate their deaths &c., (e.g. in Russia, thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf)

Pollute hashtags with anti-enemy propaganda, (e.g. in Bahrain, exposingtheinvisible.org/resources/automated-sectarianism; freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Doubleswitch attacks, (e.g. in Venezuela, Myanmar, Bahrain, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf, accessnow.org/doubleswitch-attack/)

Hacking and leaking documents allegedly relating to other governments' anti-disinformation activity, (e.g. in Russia/UK, news.sky.com/story/highly-likely-moscow-hacked-uk-agency-countering-russian-disinformation-11656539)

Attacking integrity and business prospects of pro-vaccination campaigners, (e.g. in USA, theguardian.com/technology/2019/feb/27/facebook-anti-vaxx-harassment-campaigns-doctors-fight-back)

Attack/harass journalists, (e.g. in Turkey, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Offering rewards for social media users who report opponents online, (e.g. in Thailand, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Monitor/report online behaviour of opponents, (e.g. in Thailand, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Report people who criticise those in power, (e.g. in Thailand, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)

Using fake persona to engage with activists and then disseminate their identities via Twitter, (e.g. in Bahrain, westminsterpapers.org/articles/abstract/10.16997/wpcc.167/)

Could introduce deepfake of political actors to ruin reputation or disrupt international cooperation, (e.g. in Future, unspecified, cfr.org/report/deep-fake-disinformation-steroids) Disinformation via journalists and state media publication/promotion, (e.g. in Russia, nato.int/docu/Review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm; scholarspace.manoa.hawaii.edu/bitstream/10125/59711/0271.pdf)

Spreading falsified and deliberately inflammatory news, (e.g. in USA, scholarspace.manoa.hawaii.edu/bitstream/10125/59711/0271.pdf)

Create websites and Twitter accounts posing as news outlets to disseminate disinformation, (e.g. in Russia, wired.com/story/misinformation-disinformation-propaganda-war/)

Use bots to amplify fake (and/or leaked) documents, (e.g. in France, papers.ssrn.com/sol3/papers.cfm?abstract_id=2995809; tandfonline.com/doi/pdf/10.1080/23738871.2018.1462395?needAccess=true)

Omit information from news reports, (e.g. in Cuba, miamiherald.com/news/nation-world/world/americas/cuba/article166582192.html)

Sharing outated stories in context where they seem to have new relevance, (e.g. in Phillippines, rappler.com/nation/148007-propaganda-war-weaponizing-internet)

Videos shared claiming to be of separatist cannibals, (e.g. in Cameroon, firstpost.com/tech/news-analysis/viral-fake-video-shared-via-facebook-causes-political-upheaval-in-cameroon-5505611.html)

Publishing/sharingphotos of dead people falsely claiming they have been killed by a particular group, (e.g. in Phillippines, Myanmar, thediplomat.com/2019/02/southeast-asias-battle-against-disinformation/;theguardian.com/world/2018/aug/31/myanmar-army-fakes-photos-and-history-in-sinister-rewrite-of-rohingya-crisis; rappler.com/nation/148007-propaganda-war-weaponizing-internet)

Publishing/sharingphotos of dead people falsely claiming they have been killed by a particular group, (e.g. in Nigeria, bbc.co.uk/news/resources/idt-sh/nigeria_fake_news)
Hack legitimate news orgs to spread false information, (e.g. in Syria, aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html)

Use fake accounts to promote support/attack opponents before an election, (e.g. in Philippines, freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf)
Sending threats to parliamentarians/government officials, (e.g. in UK, thetimes.co.uk/article/1a6f281e-412c-11e9-aa0a-30b9d78dd63b)

Attacks on trustworthiness of institutions and media, (e.g. in Unspecified, Multiple sources)

Promoting Facebook events and contacting activists via Messenger, (e.g. in Russia, Multiple sources)

Use fake accounts to join popular groups and voice support for government (Facebook, WhatsApp), (e.g. in Sudan, Multiple sources)

Appendix 2 - Case Study Data

EU Figures and Institutions

Twitter Handles of EU Figures and Institutions

Avramopoulos	Ansip_EU	JHillEU	MAC_europa	StylianidesEU	europeforall	mariannethyssen	MofCap
CorinaCretuEU	MimicaEU	EU_TTIP_team	gr2014eu	EUCourtPress	JHahnEU	UE_Luxembourg	EUombudsman
GOettingerEU	RP_France_CdE	EU4BE	EU_EDPS	V_Andriukaitis	EU_CoR	UEFrance	eu_echo
EU_Justice	MalmstromEU	FedericaMog	EUHomeAffairs	EU_Budget	MarosSefcovic	JMDBarroso	donaldtusk
NatashaBertaud	EurobarometerEU	EU_Eurostat	EUTenders	EURLex	RPFranceUE	EUinmyRegion	EU_EESC
PhilHoganEU	LithuaniaMFA	CoEinBrussels	LaszloAndorEU	EURightsAgency	EUCouncil	KarmenuVella	EUCouncilPress
eucopresident	EUSciencelnnov	CoE_fr	JunckerEU	NeelieKroesEU	EU_Commission	CCMI_EESC	KGeorgieva
EUInterpreters	APiebalgs	EU_Careers	eu_eeas	EUPublications	EC_AVService	EUCouncilTVNews	Montijano
pierremoscovici	coe	jyrkikatainen	Moedas	europeaid	vestager	MichelBarnier	Bulc_EU
JeanArthuis	catherinemep	marabizzotto	MCArnautu	beatrizbecerrab	beghin_t	ayuso_pilar	marcoaffronte
NBarekov	JamesJimCarver	pepeblancoEP	SoledadCabezon	EnriqueCalvet	DanielaAiuto	MargreteAuken	PervencheBeres
DominiqueBilde	L_Cesa	EricAndrieuEU	josebove	ElmarBrok_MEP	UdoBullmann	balcytis	PaulBrannenNE
PASCALARIMONT	LNBDublin	GoffredoBettini	JeanMarieCAVADA	M_AndersonSF	MalinBjork_EU	MichalBoni	IvoBelet
Isa_Adinolfi	MEPDanielBuda	MaxAnderson	MAlliotMarie	Dr_KlausBuchner	androulakisnick	AndreaBocskor	renatabriano
Janice4Brexit	WimvandeCamp	JonathanArnott	Franc_Bogovic	Tim_Aker	AlainCadec	JonathanMEP	DavidCasaMEP
LucyAndersonMEP	BalasGuillaume	Andrikiene	AgeaLaura	mattcarthy	HuguesBayet	NicolaCaputo	NChildersMEP
MCBoutonnetFN	BiljanaBorzan	GerardBattenMEP	borrellidavid	a_chauprade	petras_petras	brandobeneifei	caspary
gannemans	VictorBostinaru	xabierbenito	CaterinaChinnic	AmjadBashirMEP	BasBelderMEP	mercedesbresso	IzaskunBilbaoB
SteeveBrioix	JerzyBuzek	IAyalaSender	DCBMEP	RichardAshMEP	BendtEU	FMCastaldo	MarinaAlbiol
charanzova	ClaraAguilera7	NicolasBay_	bueti	delcastillop	Jbergeronmep	simonabonafe	Mariearenaps
rosadamato634	Alberto_Ciriio	Stefan_Eck_MEP	knufleckenstein	SilviaCostaEU	MEPDohrmann	SebDance	tfajon

ddalton40	andicristeamep	comilara	Jane_CollinsMEP	Fjellner	AndreElissen	ignaziocorrao	r_czarnecki
OleEU	M_DiaconuMEP	jonasfernandez	federley	RaffaeleFittto	MichelDANTIN	Chrysogonos_K	LFerraraM5S
NirjDeva	paolodecastro	eleonoraforenza	Nigel_Farage	JMFernandesEU	MepMCramer	CarlosCoelhoPE	DeirdreCluneMEP
lBenEuropa	LefChristoforou	SalvoCicu	Cofferati	MichaelDetjen	HerbertDorfmann	csakypal	petervdalen
IsabellaDeMonte	AnnaMariaCB	Delahaye_Europe	EpitidGeorgios	Mdlabajova	jfostermep	AndorDeli	MarkusFerber
IsmailErtug	JoseFariaMEP	dajcstomi	gerardeprez	DantiNicola	Miriamdalli	Caninator	MireilledOrnano
JillEvansMEP	EleonoraEvi	mady_delvaux	datirachida	SantiagoFisas	MonikaFlaBenova	Ashleyfoxmep	BasEickhout
JakopDalunde	RCorbettMEP	DianeDoddsMEP	LinneaEngstrom	lukeming	ErnstCornelia	TCornillet	FountoulisLampr
ArnaudDanjean	NikosChountis	cozzolino62	damiandraghici	AngeloCiocca	KarimaDelli	GeoffroyDidier	PDurandOfficiel
markdemesmaeker	NeenaGmep	sven_giegold	hudghtonmepSNP	Arne_Gericke	GrzybAndrzej	maryhoneyball	MariaGrapini
AnaGomesMEP	JFJalkh	graswanderhainz	brianhayesMEP	anjahazekamp	Jaakonsaari	EugenAFreund	IvanJakovcic
sylvieguillaume	MarianHarkin	CHansenEU	AnnaHedh	Sylvie_Goddyn	JarokaLivia	Sergio_GP	yjadot
JytteGutelaand	EGardini	peter_jahr	CharlesGoerens	JezekCZ	DJazlowiecka	JohnHowarth1958	TheresaMEP
thaendel	nadjahirsch	KGloanecMaurin	TaniaGonzalezPs	HansOlafHenkel	IratxeGarper	Gerbrandy	javorbenedek
thadjigeorgiou	RJ_lwaszkiewicz	DianeJamesMEP	elena_gentile	MariaHeubuch	fgambus_eu	enricogasbarra	Halla_aho
gualtierieurope	inge_graessle	AGabelic	MJRLdeGraaff	MartinHaeusling	brunogollnisch	Catalin_Ivan	NathanGillMEP
RomeoFranz1	IvetaGrigule	HeidiHautala	MonikaHohlmeier	gonzalezpons	EuropaJens	czeslawhoc	gimenezbarbat
GrosseteteF	Hetman_K	lidiageringer	mikehookemmep	AdamGierek	BeataGosiewska	DanielJHannan	m_giuffrida
EGardiazabal	ghokmark	michaelgahler	carlositurgaiz	RebHarms	BriceHortefeux	jaatteenmaki	DoruFrunzulica
danutahuebner	HolvenyiGyorgy	juliegirling	RJaureguiA	TonyGuoga	jhuitema	ConstanzeKrehl	Kalniete
ph_loiseau	AKRajewicz	WernerKuhnMdEP	ph_lamberts	blochbihler	GreenJeanMEP	MarcJoulaud	othmar_karas
olleludvigsson	andreykovatchev	SyedKamall	lepenjm	marekjurek	WajidKhanMEP	M_Kefalogiannis	ZdzKrasnodebski

KaufmannSylvia	SkaKeller	ckyenge	SteliosKoul	PatrickLeHyaric	elukacijewska	JLavrilleux	philippejuvin
ZbigniewKuzmiuk	Loekkegaard_MEP	giovannilavia	Konecna_K	langen_werner	SeanKellyMEP	jo_leinen	BLiberadzki
C_Lechevalier14	EduardKukan	adamkosamep	karinkadenbach	Gilles_Lebreton	krisjaniskarins	KellerHonza	b_kappel
BarbaraKudrycka	Jude_KD	kouroumbashev	kkuneva	KyllonenMerja	miltos_kyrkos	rinakari	berndlange
MonicaMacovei1	a_jongerius	KohlicekJaromir	SHKMEP	ArndtKohn	EvaKaili	miapetrakumpula	J_Lewandowski
profKarski	ALamassoure	TonoEPP	SvMalinov	JeppeKofod	EvaJoly	patricialalond2	peterliese
ileontini	KrystynaLybacka	GiorgosKyrtsos	palomalopezB	DdJong	JFLopezAguilar	MaleticIvana	jeroen_lenaers
fjavilopez	BerndLucke	SanderLoones	ArneLietz	Bernd_Koelmel	ElsiKatainen	ilhankyuchyuk	Esther_de_Lange
fulviomartuscie	biuroposelskie	Notis_Marias	EmmaMcClarkin	AngelikaMliar	JNicholsonMEP	cmonteiroaguiar	davidmcallister
alessiamosca	Norica_Nicolai	C_Nagtegaal	NagyJozsefEU	MeszericsT	RamonaManescu	DMartinFN	luigi_morgano
curziomaltesetw	Rory_Palmer	MassimoPaolucc6	LudekNie	davidmartinmep	SMuresan	georgmayermep	miromikolasik
UliMuellerMdEP	BarbaraMatera	Urmaspaet	younousomarjee	MrMesserschmidt	RMatthewsMEP	lukasmandl	ANiebler
AnneMarieMineur	Pabriks	MarianMarinescu	MaireadMcGMEP	ValentinasMazu1	ThomasMannEP	LiadhNiRiadaMEP	maitepagaza
Iskra_Mihaylova	LindaMcAvanMEP	oflynnmep	franzobermayr	mmatias_	RolandasPaksas	LouisMichel	GiuliaMoi_M5S
stefanomaullu	anthea_mcintyre	fmarcellesi	Bernard_Monot	LJManscour	MarusikMichal	Nuno_Melo_CDSPP	NosheenaM
gesine_meissner	RenaudMuselier	marinhopintoeu	Sophie_Montel	ClareMoodyMEP	MatthijsvMilt	MarleneMizzi	Ale_Mussolini_
andrejsmamikins	AntonioPanzeri	edouardmartinEU	DemPapadakis	AndreyNovakov	anamirandapaz	nadine__morano	Joerg_Meuthen
JiriMastalka	emorinchartier	LvNistelrooij	alexImayer	martina_michels	GabrielMatoA	JanOlbrycht	emmanuelmaurel
MomchilNekov	ClaudeMoraesMEP	sorinmoisa	NiedermullerMEP	RobertaMetsola	Europarl_GA	Europarl_HR	Europarl_PT
Europarl_HU	Europarl_CS	Europarl_ET	Europarl_FI	Europarl_MT	Europarl_SK	Europarl_NL	Europarl_IT
Europarl_ES	Europarl_SL	Europarl_BG	Europarl_FR	Europarl_da	Europarl_LV	Europarl_DE	Europarl_EL
Europarl_RO	Europarl_LT	Europarl_PL	Europarl_sv	PirkkoRL	GQuisthoudt	LilianaMEP	SantAlfred
Senficon	DominiqueRiquet	TomaszPoreba	cdallonnes	MaxSalini	gillespargneaux	lojzepeterle	MargotLJParker

Andreas_Schwab	CDPreda	OlgaSehnalova	MJRodriguesEU	PavelEmilian	rohde_jens	petrisarvamaa	HelmutSchoIzMEP
mauriceponga	DavidSassoli	SofiaSakorafa	schmidt_clau	julia_reid	AnnieSchreijer	papadimoulis	JPimentaLopes
jozorados	schopflinMEP	schulzeeuropa	PatricielloAldo	SaudargasA	Emil_Radev	ioanmirceapascu	pinapic
TPicula	fernandoruas	RodriguezPinero	TerryReintke	LolaPodemos	judithineuropa	spietikainen	SorayaPostFi
Evelyn_Regner	PediciniM5S	SchaldemoseMEP	PaulRuebig	PocheMEP	Frederiqueries	DacianaSarbu	markuspieperMEP
MarcusPretzell	clauderolin	GabrielePreuss	jasenkos	SernagiottoRemo	marek_plura	VRoziere	RadtkeMdEP
stanislavpolcak	Pospisil_Jiri	DariuszRosati	MarietjeSchaake	JTP07	Manuel___Santos	pavelpoc	franckproust
EvaMaydell	BronisRopeLT	RzvanPopa1	JSaryuszWolski	UlrikeRodust	ellyesse	TokiaSaifi	KatiPiri
Vincent_Peillon	marijana_petir	mortenhelveg	SofiaHRibeiro	LidiaSenra	JProcterMEP	CarolinaPunset	f_philippot
michelreimon	MicheleRivasi	ASanderMEP	LaurRebega	sylikiotis	THEOCHAROUSE	istvan_ujhelyi	SophieintVeld
StevensHelga	KaySwinburneMEP	GVOMEP	guyverhofstadt	NilsTorvalds	derekvaughan	JStarbatty	SmolkovaMonika
D_Sosnierz	szejnfeld	msojdrova	MartinSonneborn	MariaSpyraki	jordisolef	paultang	Troszczynski_FN
ivajgl	BirgitSippelMEP	hildevautmans	BartStaes	Isabel_thomasEU	turcanu2014	szanyitibor	anneleen_vb
renatosoru	TrebesiusMdEP	HelgaTruepel	Antonio_Tajani	YanaToom	bodilvalero	sabineverheyen	kmujazdowski
ernesturtasun	StetinaEP	TheodorStolojan	RL_Valcarcel	PatricijaSulin	Telicka	ElenaValenciano	MCVergiat
sionsimon	IvanStefanec	ViktorUspaskich	PeterSimonMEP	isoltesEP	JSeymourUKIP	MarcoValliM5S	MonikaVana
tamburrano	RSerraoSantos	DavorSkrlec	GreenKeithMEP	EvzenTosenovsky	dubravkasuica	SulikRichard	CharlesTannock
ClaudiaTapardel	AngelaVallina	BranoSkripek	SergeiStanishev	AdinaValean	rozathun	ramontremosa	Synadinos_Eleft
RomanaTomc	maritaulvskog	toiapatrizia	IneseVaidere	MiguelViegasPCP	CzSiekierski	csaba_sogor	etorrespodemos
marctarabella	indrektarand	mariepierrevieu	jmterricabras	RuzaTomasic	AlynSmith	OlafStuger	MiguelUrban
kvanbrempt	urutchev	1PavelSvoboda	vilimsky	tomvdkendelaere	MirjaVehkapera	AnnaZaborska	woelken
AxelVossMdEP	ManfredWeber	udovoigt	DamianoZofoli	MilanZver	flaviozanonato	Marcozanni86	MarcoZullo
jakob_eu	KosmaZlotowski	KristinaWinberg	j_wisniewska	czorrinho	Weidenholzer	LieveWierinck	TomZdechovsky

AndersVistisen	robertszile	gabriela_zoana	HennaVirkkunen	joachimzeller	vozemberg	GabiZimmerMEP	JanuszZemke
IuliuWinkler	MartinaWernerEU	BZdrojewski	TadeuszZwiefka	CeciliaWikstrom	julie4nw	WestphalKerstin	WalesaMEP
renateweber	Steven_Wolfe	JanaZitnanska	zalaboris	ZeljanaZovko	danieleviotti	FrancisZD	ZahradilJan
ep_emissions	EPSocialAffairs	EP_Development	EP_HumanRights	EP_Defence	EP_ForeignAff	EP_Legal	EP_BudgControl
EP_Transport	EPInstitutional	EP_GenderEqual	EP_Trade	EPCulture	EP_Fisheries	EP_Agriculture	EP_Economics
EP_Justice	EP_Budgets	EP_SingleMarket	EP_Regional	EP_Environment	EP_Industry	EP_Petitions	EuroParlPress
JKingEU	EBienkowskaEU	VeraJourova	TNavracsicsEU	GabrielMariya	VDombrovskis	EU_ecoinno	inea_eu
ECDC_EU	EU_ISS	eurogender	Cedefop	EFSA_EU	eurofound	EU_IPO	EU_OSHA
EUEnvironment	etfeuropa	EUinTajikistan	UEauSenegal	UeCongo	UEenRCA	UEauCameroun	UEauBurundi
UEenARG	UEauTchad	EUinEthiopia	EUinYemen	EUatOECD_UNESCO	UEenRDC	EUinNZ	EUinNigeria
EUinASEAN	EUinKazakhstan	EuropeInGhana	UEenEcuador	EUinSyria	EUinSA	UEauBenin	EUinSingapore
UEenElSalvador	euinzim	dueniger	EU_Maldives	EU_in_Sri_Lanka	UEenParaguay	EUOSCE	EUinEgypt
EUinMalawi	EUinJordan	DUeGabonGeStp	EU_in_Somalia	UEenCI	EUinTheGambia	EUinSwitzerland	EUinCanada
EUinAus	EU_Tashkent	UEenHonduras	EUintheUAE	EUinMalaysia	EU_SUDAN	UEenBolivia	UEaDjibouti
UeTunisie	EUinNepal	UEauMali	EUinCV	EUinUG	IraqDel	EU_InfoCentre	UnionEuropeaRD
EUinRussia	EUinJamaica	AmbUETogo	UEMauritanie	EUinTZ	EUinIsrael	EUinGeorgia	EUtoAU
EUDELtoLibya	UEenNicaragua	EUKosovo	EU_in_India	EUPakistan	EU2Namibia	UEGuatemala	DELGUYGEO
EUintheGCC	euffsg	UEenMexico	EUDELCoE	EU_UNGeneva	EUinLebanon	UEenPeru	UEenVenezuela
EUinAlbania	UEenChile	EUinKenya	EUpalestinians	euunvie	UEenColombia	EUinRW	UEnoBrasil
UEenCostaRica	EU_Armenia	EUinAfghanistan	EUDelegationVN	EUDelegationUA	euinkorea	EUDelegationTur	eudeleg_rome
UE_au_Maroc	EUinICELAND	EUmissionWTO	EUiNorge	eubih	EUinJapan	EUICBG	EUinthePH
uni_eropa	EUintheUS	EUatUN	EuSport	MEDIAprogEU	Energy4Europe	EUAgri	Food_EU

EU_Competition	EU_ScienceHub	europe_creative	EU_MARE	EU_H2020	Trade_EU	EU_Taxud	EUClimateAction
EuropeanYouthEU	EU_Health	ConnectCitiesEU	EU_ENV	Transport_EU	eu_near	MSCActions	eGov_EU
DSMeu	EU_Finance	EUdigitalblog	EUErasmusPlus	EU_Social	EU_opendata	translatores	EU_Growth
CORDIS_EU	EU_Consumer	ecfin	eHealth_EU				

German

EU-related Keywords in German

Brexit	EU	UE
Europäischen Union	Europäische Parlament	Europäischen Rat
Rat der Europäischen Union	Europäischen Gerichtshof	Binnenmarkt
Vertrag von Lissabon	Europäischen Kommission	Juncker
Tusk	Tajani	

Top 50 Accounts Mentioned in German Dataset

Twitter Account Mentioned (red accounts have since been suspended as of March 2019)	Number of Mentions
@welt (News)	1124
@spiegelonline (News)	456
@tagesschau (News)	354
@erdollum	341
@faznet (News)	306
@tagesspiegel (News)	169
Unknown (Hashed)	164
@doktordab (Journalist)	151
@stn_news (News)	133
Unknown (Hashed)	121
@sz (News)	112
Unknown (Hashed)	112
@zeitonline (News)	111
@larswienanD (Journalist)	101
@tejaadams (Journalist)	100
@dianagruberr	89
@stz_news (News)	88
@derspiegel (News)	82
@abendblatt (News)	82
@ntvde (News)	78
@keinewunder (Journalist)	75

@rolandtichy (Journalist)	73
@ilkomshop (Art)	73
Unknown (Hashed)	72
@morgenpost (News)	71
@cdu (Christian Democratic Union – Political Party)	70
Unknown (Hashed)	70
@zdf (Public Service TV Station)	69
@regsprecher (Federal Government Chief Press Officer)	69
@wdr (Public Service TV Station)	67
@bild (News)	63
@uniwave (Journalist)	63
@klauseck (Content Marketing)	62
@wznewsline (News)	60
@zdfheute (News)	59
@spiegeltv (TV Shows)	58
@sternde (News)	55
@focusonline (News)	54
@chrisstoecker (Journalist/Academic)	51
@martinschulz (Leader of the Social Democratic Party)	50
@tspleute (News)	50
@welt_politik (News)	50
@katjakipping (Leader of The Left party)	49
Unknown (Hashed)	48
@lorenzmaroldt (Journalist)	47
@tagesthemen (News)	47
@spdde (Social Democratic Party – Political Party)	46
@mopo (News)	46
@angieffehr	45
@juliakloeckner (Deputy Chairwoman of the Christian Democratic Party)	44

French

EU-related Keywords in French

Brexit	EU	UE	l'UE
Parlement européen	l'Union européenne	Conseil de l'UE	Conseil de l'Union européenne
Commission européenne	Comité économique et social européen	Comité européen des régions	Pierre Moscovici
Cour de justice de l'Union européenne	traité de Lisbonne	marché unique	Conseil européen
Juncker	Tusk	Tajani	

Top 25 Accounts Mentioned in French Dataset

Twitter Account Mentioned (red accounts have since been suspended as of March 2019)	Number of Mentions
@voltuan	135
@mlp_officiel (Marine Le Pen)	83
@opboycott (Boycott Israel)	43
@zombiaxx	38
@le_figaro (News)	34
@emmanuelmacron (Emmanuel Macron)	31
@paoegilles (Pro Trump and Israel)	27
@afpfr (Associated Press)	25
@elysee (Official Presidential Account)	24
@gabriellecluzel (Journalist)	24
@federicamog (Vice President of the EU Commission)	22
@lemondefr (News)	22
@carlosvfrvn	22
@c2017deboucracy	19
@kremlinrussi (Russian Kremlin)	18
@kremlinrussi (Russian Kremlin)	18
@whitehouse (US President)	18
@itele (News)	17
@bfmtv (News)	17
@antileftistsfas	17

@franceinfo (News)	16
@haussmannparis	16
@marion_m_le_pen (Marion Le Pen, niece of Marine Le Pen)	15
@thomaswieder (Journalist)	14
@rtenfrancais (Russia Today, France)	13

Italian

EU-related Keywords in Italian

Brexit	EU	UE
dell'UE	L'Unione europea	Consiglio europeo
Consiglio dell'UE	Parlamento europeo	Corte di giustizia dell'Unione europea
trattato di Lisbona	mercato unico	Commissione europea
Juncker	Tusk	Tajani

Top 25 Accounts Mentioned in Italian Dataset

Twitter Account Mentioned (red accounts have since been suspended as of March 2019)	Number of Mentions
@repubblica (News)	1763
@adnkronos (News)	1223
@repubblicait (News)	907
@agenzia_ansa (News)	656
@corriere (News)	612
@linkiesta (News)	512
@lastampa (News)	429
@ilpost (News)	352
@lettera43 (News)	245
@mattinodinapoli (News)	269
@ilmessaggeroit (News)	264
@giornalettismo (News)	255
@globalistit (News)	246
@huffpostitalia (News)	225

@radio1rai (Radio Channel)	213
@skytg24 (TV Channel)	209
@elena07617349	206
@agenzia_italia (News)	196
@wireditalia (News)	190
@repubblicatv (TV Channel)	174
@fattoquotidiano (News)	174
@gazzetta_it (News)	169
@sole24ore (News)	167
@internazionale (News)	156
@stati_generali (News)	145

FURTHER APPENDICES:
See here: https://docs.google.com/spreadsheets/d/1DSVOO7fWF0IovFG-wD7e6oAn-Uhd4i5JxUq9rXWHbvQ/edit#gid=1045125648

References

1. https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html
2. https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html
3. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html
4. https://uk.reuters.com/article/uk-myanmar-rohingya-un/u-n-calls-for-myanmar-generals-to-be-tried-for-genocide-blames-facebook-for-incitement-idUKKCN1LC0KL
5. https://motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent
6. https://gking.harvard.edu/files/gking/files/50c.pdf
7. https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet
8. https://shape.nato.int/resources/3/images/2018/upcoming%20events/mc%20draft_info%20ops.pdf
9. https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/sub-committee-on-disinformation/news/sub-committee-launch-report-publihed-17-19/
10. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation
11. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
12. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183
13. An approach to the risks of policy inaction in the face of human rights risks can be found here https://policyexchange.org.uk/publication/the-cost-of-doing-nothing-the-price-of-inaction-in-the-face-of-mass-atrocities/
14. 'Coordinated inauthentic behaviour' also appears in Facebook's definition of online behaviour which violates their terms of service https://www.buzzfeednews.com/article/pranavdixit/facebook-removes-indian-pakistani-political-accounts-pages
15. The time period that the case studies of information operations focused on, though the background research was broader in scope.
16. E.g. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf
17. Although we use the term 'information operations' in this report, which is broader than the categories of information warfare, disinformation or fake news, as these terms are very commonly used in the discourse in this area, they were judged to be suitable proxy search terms.
18. Others were used for background - see Bibliography
19. https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/
20. http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf
21. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf
22. https://mic.com/articles/191899/myanmar-military-members-fake-news-facebook#.ggl3PU9Of
23. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf
24. https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf

25. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf; https://rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf
26. https://news.sky.com/story/highly-likely-moscow-hacked-uk-agency-countering-russian-disinformation-11656539
27. https://www.nytimes.com/news-event/russian-election-hacking
28. CF. Shiffrin, Seana Valentine, 2014, Speech Matters: On Lying, Morality and the Law, Princeton University Press, Princeton
29. https://motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent
30. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf
31. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html; https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news
32. https://motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent
33. https://www.theguardian.com/commentisfree/2015/mar/02/guardian-view-russian-propaganda-truth-out-there
34. See bibliography for background reading e.g. https://www.washingtonpost.com/news/democracy-post/wp/2017/03/13/for-russian-tv-syria-isnt-just-a-foreign-country-its-a-parallel-universe/?utm_term=.38e82091e54c; https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/
35. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf
36. In the cases we reviewed in detail, the origin or whether there had been organisation of the information activity was not always clear. The numeric analysis in this section, for simplicity, considers only the cases with a clear organisational/intentional element.
37. See also analysis of citizen involvement in information operations in the Ukraine/Russia conflict: https://journals.sagepub.com/doi/abs/10.1177/0163443716686672; https://academic.oup.com/ia/article/94/5/975/5092080
38. https://www.bbc.co.uk/news/world-us-canada-45294192
39. https://www.firstpost.com/tech/news-analysis/viral-fake-video-shared-via-facebook-causes-political-upheaval-in-cameroon-5505611.html
40. Hence here we have treated the government amplification as an instance of information operations
41. https://edition.cnn.com/2019/03/27/europe/paris-fake-kidnapping-scli-intl/index.html
42. See e.g. https://www.bbc.co.uk/news/world-europe-47800418
43. https://motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent
44. https://mic.com/articles/191899/myanmar-military-members-fake-news-facebook#.bbK9wXAkb
45. Such as Cuban state-run media sharing stories about the US being responsible for giving Chavez cancer.https://www.miamiherald.com/news/nation-world/world/americas/cuba/article166582192.html
46. As we show below, mass amplification of true news can be carried out as part of an information operation.
47. https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia

48. As in Bahrain https://www.westminsterpapers.org/articles/abstract/10.16997/wpcc.167/
49. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf
50. https://www.bbc.co.uk/news/world-europe-47488267?ocid=socialflow_twitter
51. https://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war
52. https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet
53. 5 displayed a combination of the types
54. https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far
55. https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf
56. As in Nigeria, Myanmar
57. https://www.westminsterpapers.org/articles/abstract/10.16997/wpcc.167/
58. https://www.westminsterpapers.org/articles/abstract/10.16997/wpcc.167/
59. See e.g. https://www.thetimes.co.uk/article/1a6f281e-412c-11e9-aa0a-30b9d78dd63b
60. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf
61. (Although this case may not qualify as 'coordinated') https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news; https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html
62. This not mean that the information activities were conclusively carried out by or on behalf of a government (although many were), but rather that their aims seemed to be broadly supportive of the government.
63. 'Aligned with a government' includes cases of operations by one government against another
64. 'Deepfakes' counted as both for and against government, as a tactic which hasn't yet been employed on a wide basis but could be employed on either side.
65. Discussed in more detail above
66. See e.g. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf
67. Although both kinds would likely have secondary effects in the other space.
68. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf
69. https://motherboard.vice.com/en_us/article/z4maww/how-mexican-twitter-bots-shut-down-dissent
70. https://mic.com/articles/191899/myanmar-military-members-fake-news-facebook#.ggl3PU9Of
71. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper-121718.pdf
72. See e.g. https://www.vox.com/policy-and-politics/2017/11/2/16588964/america-epistemic-crisis; https://www.washingtonpost.com/news/democracy-post/wp/2017/03/13/for-russian-tv-syria-isnt-just-a-foreign-country-its-a-parallel-universe/?utm_term=.38e82091e54c; https://www.vox.com/policy-and-politics/2017/3/22/14762030/donald-trump-tribal-epistemology; https://www.theguardian.com/commentisfree/2018/apr/20/trump-us-syria-truth-tribal-robert-mueller-white-helmets-factse?CMP=Share_iOSApp_Other; https://www.theguardian.com/books/2018/jul/14/the-death-of-truth-how-we-gave-up-on-facts-and-ended-up-with-trump; https://www.theatlantic.com/international/archive/2014/09/russia-putin-

revolutionizing-information-warfare/379880/ https://www.nytimes.com/2017/04/17/opinion/has-trump-stolen-philosophys-critical-tools.html; https://www.nytimes.com/2016/11/05/opinion/beyond-lying-donald-trumps-authoritarian-reality.html
73. See https://www.nytimes.com/2015/06/07/magazine/the-agency.html
74. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump
75. https://scholarspace.manoa.hawaii.edu/bitstream/10125/59711/0271.pdf, p.2743'
76. https://www.theguardian.com/world/2017/jan/05/five-star-movement-beppe-grillo-putin-supporters-west
77. https://www.nato.int/docu/Review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm; https://scholarspace.manoa.hawaii.edu/bitstream/10125/59711/0271.pdf
https://www.bloomberg.com/news/articles/2018-06-07/who-you-gonna-call-postal-police-is-italy-s-fake-news-fix
https://www.euractiv.com/section/elections/video/wed-the-modest-impact-of-fake-news-on-the-2018-italian-elections/; https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/; https://theconversation.com/in-italy-fake-news-helps-populists-and-far-right-triumph-92271;
78. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf
79. https://www.nytimes.com/2015/06/07/magazine/the-agency.html
80. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper-121718.pdf
81. https://www.nato.int/DOCU/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm
82. A framework used in the case of atrocity crimes by Protection Approaches https://www.protectionapproaches.org/our-approach.html

Licence to publish

Demos – License to Publish
The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions
a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.
b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this License.
c 'Licensor' means the individual or entity that offers the Work under the terms of this License.
d 'Original Author' means the individual or entity who created the Work.
e 'Work' means the copyrightable work of authorship offered under the terms of this License.
f 'You' means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from Demos to exercise rights under this License despite a previous violation.

2 Fair Use Rights
Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 License Grant
Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:
a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions
The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:
a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.
c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer
a By offering the Work for public release under this License, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:
i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder
and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;
ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.
b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability
Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination
a This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.
b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other licence that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8 Miscellaneous
a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this License.
b If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.
c No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.
d This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of Demos and You.