Trends in Online Foreign Influence Efforts[*]

Diego A. Martin[†] Jacob N. Shapiro[‡]

Version 1.2
July 8, 2019

Abstract

Information and Communications Technologies (ICTs) create novel opportunities for a wide range of political actors. In particular, foreign governments have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation. This report describes a new database of such 53 such foreign influence efforts (FIE) targeting 24 different countries from 2013 through 2018. FIEs are defined as: (i) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, (ii) through media channels, including social media, by (iii) producing content designed to appear indigenous to the target state. The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization. Our data draw on more than 460 media reports to identify FIEs, track their progress, and classify their features.

[*] We are grateful to a range of colleagues including Laura Courchesne, Nick Feamster, Andy Guess, Hans Klein, and Brendan Stewart for helpful comments and feedback on our coding scheme. Will Lowe provided invaluable advice on data structure and data entry. Arya Goel, Janette Lu, Imane Mabrouk, Matthew Merrigan, Kamila Radjabova, and Nina Sheridan provided excellent research assistance. This work was possible thanks to generous funding from the Bertelsmann Foundation and Microsoft. All errors are our own.

[†] Princeton University, Woodrow Wilson School of Public and International Affairs, 323 Bendheim Hall, Princeton, NJ 08544. E-mail: diegoam@princeton.edu.

[‡] Princeton University, Woodrow Wilson School of Public and International Affairs, Princeton, NJ 08544. Email: jns@princeton.edu.

Contents

1 Introduction

Information and Communications Technologies (ICTs) have increased the productivity, wage, and demand for capital factors in the developed and developing world (Krueger 1993, Acemoglu & Autor 2011, Benavente et al. 2011, Martin 2018). Additionally ICTs have changed the way people communicate about politics and access information on a wide range of topics (Foley 2004, Chigona et al. 2009). Social media, for example, revolutionizes communication between leaders and voter by enabling direct politician-to-voter communications outside the structure of traditional speeches and press conferences (Ott 2017). In the 2016 US presidential election campaign, social media platforms were more widely viewed than traditional editorial media and were central to the campaigns of both Democratic candidate Hillary Clinton and Republican candidate Donald Trump (Enli 2017). These new platforms create novel opportunities for a wide range of political actors. In particular, foreign actors have used social media to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation.

This report describes a new database of such foreign influence efforts (FIEs). FIEs are defined as: (i) coordinated campaigns by one state to impact one or more specific aspects of politics in another state, (ii) through media channels, including social media, by (iii) producing content designed to appear indigenous to the target state. To be included in the data an FIE must meet all three criteria. The objective of such campaigns can be quite broad and to date have included influencing political decisions by shaping election outcomes at various levels, shifting the political agenda on topics ranging from health to security, and encouraging political polarization. In contrast to traditional information operations, when state-supported media outlets promote specific narratives, FIEs disguise the origin of the content (though many FIEs appear to be coordinated with such traditional propaganda efforts).

Our data draw on a wide range of media reports to identify FIEs, track their progress, and classify their features. We identified 53 FIE, in 24 targeted countries, from 2013 through 2018.[1] Two of the cases were ongoing as of April 2019. In total, 72% of the campaigns were conducted by Russia, with China, Iran, and Saudi Arabia accounting for most of the remainder. In five cases press reports did not reliably report the origin of the campaign. We also identified and studied more than 40 distinct influence efforts which met some, but not all of our inclusion criteria.[2]

The Russian government has a long history of influence operations against its own citizens, including using various social media platforms to distract citizens from political issues in the country (Zhegulev 2016, Sobolev 2019). Similar tools and techniques have been used to attack democratic elections and day-to-day politics elsewhere, as is well-documented

[1] An excellent recent review by the Australian Strategic Policy Institute focuses more tightly on foreign influence efforts against elections in democracies (Hanson et al. 2017). Examining 97 elections and 31 referendums from November 2016 through April 2019, the authors "...find evidence of foreign interference in 20 countries: Australia, Brazil, Colombia, the Czech Republic, Finland, France, Germany, Indonesia, Israel, Italy, Malta, Montenegro, the Netherlands, North Macedonia, Norway, Singapore, Spain, Taiwan, Ukraine and the US."

[2] In 2016, for example, Pro-Kremlin and Russian state-funded media wrote negative stories against NATO's operation in Estonia (Nimmo 2017). This information operation was not an FIE under our definition because the content was not meant to appear as though it were produced in Estonia.

in the press and prior reports (e.g. Watts & Weisburd 2016, Kroet 2017, Watts 2017, Karp 2018, Nimmo & Brookie 2018*a*, Yourish et al. 2018, Zaveri & Fortin 2019). FIE by other countries are less sophisticated. Iran has used similar strategies as Russia in an attempt to undermine political systems in its regional neighbors. But, in comparison to Russian efforts, there is less evidence of coordination between different campaigns and the participation of the Iranian government is less clearly documented. Saudi Arabia seems to have conducted an influence effort against Iran recently, but on a much smaller scale.

The report proceeds as follows. Section 2 describes the coding rules, inclusion criteria, and process for creating our database. Section 3 provides descriptive statistics and highlights trends over time. Section 4 discusses potential future research directions. For a more granular look at the specific tactics used in Russian FIEs we recommend the excellent New Knowledge report published in late-2018 (DiResta et al. 2018).

2 Foreign Influence Effort Database

The primary objective of this project is to compile a list of distinct FIEs. An FIE is defined as an attacker-target-political goal triple (e.g. the Russian campaign to polarize American politics (Howard et al. 2018, Shane 2018, Aceves 2019) was distinct from the one intended to discredit conservative critics of President Trump (Poulsen & Ackerman 2018*b*)). Our goal in doing so is to summarize evidence regarding trends in these operations, provide baseline information about a wide range of FIEs, and offer high-level context for the growing literature about disinformation campaigns. We do not collect data on traditional propaganda (e.g. political information provided by country X about country Y in ways which do not seek to mask its origin) nor local political activity (i.e. disinformation about country X produced by political actors in country X and spread on social media).[3]

To be included in the database, an influence effort must involve: (i) action by one state against another in the media;[4] (ii) an identifiable political goal; and (iii) producing content that is meant to appear as being produced organically in the target state (e.g. fake accounts, fake press organizations, trolls posing as citizens of the target state). FIEs may involve promoting true content as well as false or misleading information.[5]

The database was built in three steps following standard practices for constructing such

[3] FIEs are distinct from the broader category of disinformation campaigns which can include purely domestic activity as well as content clearly labeled as being produced in the influencing state.

[4] Broadly defined to include social media.

[5] In our definition the deception is over the origin of the content, not necessarily its content, though that too is often untrue.

data:[6]

1. *Develop a coding schema.* Our database structure and features are intended to reflect strategic decisions by the influencer as well as operational choices which must be made in managing multiple distinct influence campaigns over time, as the Russian Internet Research Agency (IRA) did from mid-2014 through at least 2018 (Mueller 2019, p. 4 - 8, p. 14 - 35).[7] To organize such campaigns, an attacking organization needs to articulate strategies for each country along several dimensions including: the topics to be pursued, platforms to use, specific tactics, etc. We elicited feedback on our schema from scholars and technologists working on disinformation challenges in private industry. Figure 1 presents the final relational database which incorporates their feedback. The database contains the following: basic identifying information about the attacker and target as well as the timing of the attacks, types of actors employed, platforms used, strategy, approach, tactics, and topics.

2. *Identify candidate influence efforts.* Once the coding scheme was developed we examined 463 stories about influence efforts from 41 countries across a range of sources. We first reviewed material from the following news outlets: ABC News, BBC News, Politico, Reuters, The Economist, The Guardian, The Independent, The Mirror, The New York Times, The Telegraph, The Wall Street Journal, The Washington Post, and Wired Magazine.[8] We then searched for additional information on media websites and expert blogs including: Al-Monitor, Buzzfeed, Freedom House, Human Rights Watch, Medium (including the excellent series of reports by DFRLabs), Quartz, The Atlantic, The Daily Beast, The Daily Dot, The Hill, The Intercept, The New Republic, The Observer, The New Statesman, The Register, and The Verge. Finally, we reviewed all working papers and articles by the Computational Propaganda Project of Oxford University and the Social Media and Political Participation (SMaPP) Lab of New York University.

3. *Code values for all FIEs.* We identified 93 candidate FIEs across the sources above. Of the 93 we determined that 53 met our inclusion criteria based on both English language sources and reporting in Arabic, French, Spanish, and Russian as appropriate. Each FIE was reviewed and evaluated by one of the authors as well as two

[6] Bradshaw & Howard (2018), for example, report on domestically-produced propaganda, coding cases where political parties or governments use social media to manipulate public opinion. As in this report, they focus on coordinated campaigns and not lone actors, identifying 48 cases around the world. Their methodology is similar to ours. They look for information in the news, review the cases with research assistants, and check the results with experts.

A different approach is used in Woolley & Howard (2017) who study approaches to computational propaganda. They examine both purely domestic influence campaigns and ones targeting foreign countries by analyzing tens of millions of posts on seven different social media platforms during political elections between 2015 and 2017 in Brazil, Canada, China, Germany, Poland, Taiwan, Russia, Ukraine, and the United States.

[7] The most granular analysis of IRA activity during this period is DiResta et al. (2018) who analyze "an expansive data set of social media posts and metadata provided to SSCI by Facebook, Twitter, and Alphabet, plus a set of related data from additional platforms..." on the group's operations in the US from 2014 to 2017. They find that the Russian campaign exploited political and social division between American voters through a combination of disinformation, hate speech, and promoting true-but-divisive contetn.

[8] The following link provides a list of all articles reviewed.

student research assistants – one who did the original coding and a second student who had not previously worked on the case. The final 53 cases were reviewed by at least three people. The 53 cases from 2013 through the end of 2018 represent a lower bound on the number of FIEs to date as it is possible there are FIEs we did not capture. Readers who know of such efforts should contact the authors. The database and report will be periodically updated.

Many key database fields are not self-explanatory, so we provide some additional information here. Appendix A-1 provide a detailed description of each variable with specific examples.

- Each FIE is identified as an attacker-target-political goal triple. This design allows us to draw inferences about changes over time in tactics and about the allocation of effort by attacking organizations, which have to make tradeoffs between time spent on different political goals.
- The political goal of an effort is a broad description of the objective of the effort. While we did not choose a fixed set of potential values, we did look for homogeneity across countries so that we could compare the FIEs around the world. Polarizing domestic politics, for example, has been a political goal of attacks against Australia, Canada, German, Latvian, South Africa, and the US.
- Information on attacking parties is recorded in two ways. In the "Attacker" table we identify organizations by name and record key people and organizations mentioned as being part of the effort. In the "Actor" table we record a series of 0/1 variables for whether particular types of organizations were engaged in the effort (e.g. fake grassroots organizations created as part of the influence effort, known colloquially as "astroturf"). We do not distinguish between principals, those who order the attacks, and agents, those who execute them, because it is rarely possible to disentangle lines of authority with the available information.
- The platform table records a series of 0/1 variables for which media are involved in each FIE (e.g. Facebook, Twitter, etc.). We make no judgment about the extent to which different platforms are used.[9]
- The source table records a short description of the event and provides URLs for the main articles, news, reports, and working papers, relevant to that case. Only cases with at least three sources are included in the final database.
- The strategy table records the overarching method or methods used including defamation, persuasion, polarization, agenda shifting, or undermining political institutions.
- The topic table records the various topics discussed for each attack. As with political goals it is an open-ended field in which we sought to use the same terminology for broadly-similar topics. Topic and Strategy are at the same level in the relational database.

[9] Boulianne (2015) shows a positive relationship between social media use and participation in civic and political life, using 36 studies.

- The approach table records the measurable actions made by actors to achieve the strategy. These include amplifying existing content, creating new content, and producing distorted information about verifiable facts.

- The tactic table identifies concrete actions that actors can take to pursue an approach, such as use of bots, fake accounts, stealing information, and trolling.

We also provide a complementary lightly annotated bibliography of 305 references containing research about online propaganda, influence operations and media consumption of voters.[10]

3 Trends in Foreign Influence Efforts

The 53 FIEs since 2013 targeted 24 different countries: 38% of the FIEs targeted the US; 9% Great Britain; 6% Germany; Australia, France, Netherlands, and Ukraine 4% each; with Austria, Belarus, Brazil, Canada, Finland, Israel, Italy, Lithuania, Poland, Spain, South Africa, South Saudi, Sweden, Taiwan, and Yemen received each being targeted once.[11]

3.1 Attackers and Timing

These efforts have engaged a number of different types of actors, platforms, strategies, approaches, and tactics, as illustrated in table 1 which presents summary statistics of the database.

The first FIE in our data began in 2013 when Russian trolls launched a campaign to discredit Ukraine in the Polish Internet space (Savytskyi 2016). Fully 70% of the attacks started between 2015 and 2017. Attacks last for an average of 2.2 years.[12] There are at least two FIEs which began in earlier periods ongoing in 2019, including Russia undermining the Belarus government, and Russia working to reduce support for the Donbass conflict among Ukrainian citizens.

Private companies (47%), media organization (39%), and intelligence agencies (22%) are the most common actors. Media reporting was insufficiently detailed to clearly identify the responsible actors in one fourth of FIEs.[13]

[10] The following link provides the annotated bibliography updated on June 27, 2019.

[11] Determining the targeted country is not always straightforward. In the FIE aimed at discrediting the White Helmets, for example, the Twitter accounts, behind the campaign, suggested they are tweeting independently from London, Berlin, Barcelona, Istanbul, New York, Chicago, Marseille, and many other places (Jindia et al. 2017). For this effort, we recorded “multiple” targeted countries because the effort attacked many liberal democratic states whose governments supported the White Helmets.

[12] The median duration is 2 years.

[13] In the 2017 German federal election, for example, anonymous online trolls and extremist agitators meddled in Germany’s election. One researcher found a large number of posts which appeared superficially to be by right-wing social media users in the US, but claimed that it is possible that some of these accounts were connected to Russian interference (Hjelmgaard 2017). Therefore, it is unknown which actor is behind this effort.

3.2 Strategies and Tactics

FIEs have employed a wide range of strategies and we do not see clear trends over time.[14] The most commonly-used strategy is defamation, defined as attempts to harm the reputation of people or institutions, which is used in 65% of FIEs. Persuasion, which we define as trying to move the average citizen to one side of an issue, is used in 55% of FIEs. Only 15% of FIEs used polarization—defined as trying to move opinion to the extremes on one or more issues. These findings contradict the idea that FIEs most often work to polarize public opinion Stewart et al. (2018, see e.g.).[15]

There is much less heterogeneity in which approaches have been used over time. Three in five cases include all three approaches—amplify, create, and distort—in the same operation. 99% of the cases use creation of original content, 78% amplification of pre-existing content, and 73% distortion of objectively verifiable facts.[16]

When it comes to tactics, there is a great deal of variance, but few distinct trends over time. Fully 9 out of 10 cases use trolls. Half of the attacks used automation to spread their message, and the share doing so has been fairly stable since 2014, as we see in figure 6, panel B. Similarly, just over half of the FIEs used fake accounts, a number which has remained stable since 2014. Since it is often not possible to determine whether the accounts involved in an attack are real or not based on media reporting, we record that a fake account was involved only if one of the sources directly make that claim.

Twitter has been the most commonly-used platform (83%), followed by news outlets (66%), and Facebook (50%).[17] This pattern may reflect these platforms' market share as well as the fact that both platforms offer free access and have historically had low capacity to screen content, making them ideal platforms for sending propaganda masked as indigenous political activism. However, the pattern may also be an artifact of these platforms' transparency. Both Twitter and Facebook have released a great deal of data about the Russians operation in the 2016 US presidential election (NewsWhip 2018), making it easier to report on how FIEs have used them, which in turn leads them to be represented in our data.

3.3 Combinations Across Fields

Table 2.1 shows the percentage of cases that combine two strategies. Defame and persuade (47%) is the most commonly-used combination, followed by undermine institutions and

[14] The most detailed analysis of the various strategies and tactics used in Russian FIEs to date is DiResta et al. (2018).

[15] Relatedly, Eady et al. (2019) do not find strong evidence of "echo chambers" in which people choose news sources which reinforce their biases. Using a sample of Americans on Twitter they find most people consume media from multiple perspectives.

[16] Stewart et al. (2018) provide a number of specific examples of how different approaches were used in Russian FIE targeting the US.

[17] Both Facebook and Twitter are commonly used by political supporters to distribute junk news. Narayanan et al. (2018) analyze Twitter and Facebook groups three months before President Donald Trump's first State of the Union Address in 2018. They find that on Twitter, the Trump Support Group shared 95% of the junk news sites on their watch list, and accounted for 55% of junk news traffic in the sample. On Facebook, the Hard Conservative Group shared 91% of the junk news sites on their watch list, and accounted for 58% of junk news traffic in the sample. Other groups shared content from these junk news sources, but at much lower rates.

shift the political agenda (33%). Table 2.2, analogously, shows that trolling, bots, and hashtag hijacking (97%) are typically used together. Finally, table 2.3 displays Twitter, Facebook, Instagram and e-mail are used together most of the time.

Creation of new content has been the most common approach in every year, as figure 2 shows. Since 2016 amplification has been more commonly used than distortion.

3.4 Attacker Patterns

Russia has been the main country using FIEs to date, as figure 3 shows. In 2017 we estimate that Russia was engaged in 29 distinct campaigns around the world. Iran was involved in 2 cases between 2014 and 2015, but steadily increased their activity through 2018 when they targeted 8 other nations. China, Iran, and Saudi Arabia each initiated FIEs during our study period.[18]

Panel A in figure 4 presents the number of attacks involving each type of actor from 2013 through 2018. Astroturf, cyber espionage groups, real NGOs, and wealthy individual were involved in fewer than five cases each year. Most attacks involved companies, foreign government officials, intelligence agencies, and media organizations. Their relative shares remained fairly stable after 2015, as Panel B shows, with the exception of the shift from identified firms being involved to unknown actors. This may reflect increasing proficiency among FIE actors in masking their responsibility.

Figure 5, panel A, presents total number of attacks employing each strategy during the study period. Defame and persuade were used in a majority of FIEs throughout the period. Although the number of cases involving polarization is modest, only 8 cases by 2018, they have been an increasing share of active efforts over time, as Panel B shows. Efforts to shift the political agenda and undermine institutions have been relatively rare.

The share of attacks using different tactics has been relatively consistent since 2014, as figure 6, panel B shows. Trolling is present in almost all FIEs (94% overall), but bots and fake accounts have only been used approximately half of the attacks in most years. There does appear to be a steady increase in the use of hashtag hijacking over time, but even in the most recent years it is only used in 20% of FIEs.

Facebook, Twitter, and news outlets are the most common platforms used in FIEs, as figure 7 shows. Twitter was involved in 32 cases, news outlets 27, Facebook 19, and other platforms 18.[19] Instagram and Youtube have been used in an increasing share of attacks over time, as Panel B shows. Despite these apparent trends, it is important to note that the use of platforms in furtherance of FIEs is distinct from an assessment of interaction of FIE content on those platforms. Assessing the latter requires approaches asking to those deployed in Allcott et al. (2019) who find that interaction with false content increased on both Facebook and Twitter between 2015 and 2016. Interactions with false content

[18] Vilmer et al. (2018) analyzes information manipulations using a broader definition that includes propaganda (i.e. where one country directly attacks another using official media as opposed to campaigns which pretend to be organic from the targeted country). They report that European authorities attribute 80% of influence efforts to Russia, with the remaining 20% coming from China, Iran, and ISIS, a non-state actor.

[19] Other platforms include email, Google, fake websites, Line, other media which includes radio, TV, and newspapers, Reddit, Whatsapp, and Wikipedia.

continued to increase on Twitter in the following two years but fell on Facebook.

3.5 Attacking countries

China and Russia both have large state-run media organizations that spread propaganda locally and conduct influence operations on their own citizens (see e.g. King et al. 2017, Zhuang 2018, Stukal et al. 2019). The Russian government has long interfered on Russian social networks to divert attention from the social and economic problems (Sobolev 2019). We suspect that this prior experience served as the basis for initiating campaigns around the world, as others have noted.[20] Based on media reporting, those managing Russian FIEs organize their workers in a hierarchical manner. Workers at the Internet Research Agency, for example, reportedly received subjects to write about each day and were divided into groups, where those with best writing skills in English were at a higher level of the hierarchy (Troianovski 2018). The group also had systems to react quickly to daily events, such as new policies, diplomatic events between governments, and various kinds of accidents.

China has not been as active as Russia in conducting FIEs, perhaps because their citizens do not commonly use the same platforms as Westerners (e.g. Twitter and Facebook), which may make the organizational challenges of running foreign operations relatively higher. [21]

When it comes to partisanship, Russian efforts are most-often associated with driving right-wing parties. In Germany, for example, Russian efforts supported the Alternative for Germany (AfD) party in recent national elections, and in Italy Russian managed accounts helped the Five Star Movement (M5S) and far-right Lega Nord party. There are, however, cases where Russia supports left-wing parties, such as in Spain where they have been pushing Catalonia independence. Instead of following a fixed political ideology, Russian FIEs appear to be quite pragmatic and sophisticated when it comes to what kinds of changes will support their geopolitical goals.

Overall Russia has conducted 14 distinct FIEs in the US; three each in Great Britain, two each against Australia, Germany, Netherlands, and the Ukraine (one of which has been ongoing since 2015); and one FIE in each of the following countries: Austria, Belarus, Brazil, Canada, Finland, France, Italy, Lithuania, Poland, Sweden, South Africa, Spain and Syria (the latter involving efforts to hide responsibility chemical weapons attacks by the Syrian-government). Their political goals have been diverse, as summarized below:

- Discredit and attack: American institutions, conservative critics of Trump, the Democratic party in the US Presidential (2016) and midterm elections (2018), Em-

[20] Watts (2017), for example, argues that Soviet Active Measures strategy and tactics have been reborn and updated for the modern Russian regime and the digital age. He also adds that Russia's Active work far better than that of their Soviet ancestors. During the Cold War, Russians had to infiltrate the West, recruit agents, and suborn media organizations to promote communist parties and spread propaganda. Social media, on the other hand, provides Russia's new Active Measures access to US audiences without setting foot in the country. Blank (2013) also claims that Russia, because of its historical experience and the legacy of Soviet thinking about information warfare, sees social media as a new means to conduct large-scale campaigns to reshape the thinking of entire political communities.

[21] Consistent with that interpretation, there have been campaigns targeting Chinese communities in Australia using Line and WeChat.

manuel Macron in the 2017 French elections, Hillary Clinton in the 2016 US Presidential election, the White Helmets, Theresa May, and US military operations in various locations around the world.[22]

- Polarize: American politics (by e.g. simultaneously supporting the Black Lives Matter movement and the White Lives Matter counter-movement), Australian politics, Brazilian politics, Canadian politics, and South African politics.
- Support: Alt-right movements in the US, Alternative for Germany (AfD) in the German Federal Elections (2017), Brexit referendum, Catalonia independence vote, Donald Trump in the 2016 US Presidential election, Donald Trump's nominees for the US Supreme Court, the Five Star Movement (M5S) and far-right party the League (La Lega) in Italy, fringe movements for independence in California and Texas,[23] and the Annexation of Crimea by the Russian Federation.[24]
- Undermine and reduce support for: Angela Merkel and her political decisions, the Belarus government, Sebastian Kurz after 2017 Presidential elections in Austria, the Australian government, Barack Obama, the relationship between Poland and Ukraine.
- Other political goals include: criticizing U.K. participation in the Syrian conflict, discrediting people identifying Russian propaganda, distorting perceptions of the relationship between Lithuania and Belarus, influencing Brazilian elections,[25] influence public opinion on various issues, promote Russian propaganda, reduce support in Ukraine and Europe for Ukrainian action in the Donbass conflict, spreading false reports about a wide range of topics including a chemical plant explosion in Louisiana, an Ebola outbreak and a police shooting in Atlanta during the first half of 2011.

In the 2016 US presidential elections, for example, Russian trolls promoted and attacked both Donald Trump and Hillary Clinton. Then-candidate Trump received more support and fewer attacks compared with Clinton (Nimmo & Karan 2018). During the same election and afterward, Russian-managed bots and trolls pushed voters in opposite directions about subjects such as race, immigration, healthcare policy (mostly around vaccinations), police violence, and gun control, among others. This strategy appears to have inspired Iranian trolls who followed a similar mix of strategies, though no evidence has come to light of a company running operations as the Internet Research Agency did

[22] Some platforms have taken action to combat such efforts. During the 2018 US midterm election, for example, Facebook employed a large team to analyze different types of media information, identify what they termed "coordinated inauthentic activity" (mostly from Russia), and reduce viewership of that content in the run up to the election (Kist 2018).

[23] Russian-origin tweets supporting the YesCalifornia group and Russian-created Facebook pages supporting Texas Independence

[24] Although "Democratic tech experts" in the US used Russian-style disinformation tactics during Alabama's 2017 special election in an attempt to splinter support for Roy Moore (Shane & Blinder 2018), the cyber security research project Hamilton 68 found that 600 Twitter accounts linked to Russian influence operations pushed out more than 20,000 tweets daily in support of Roy Moore using the hashtag #alabamasenaterace in 2018 (Clifton 2017, Schafer 2017).

[25] Primarily through polarization: spreading messages involving Jair Bolsonaro, Luiz Inácio Lula da Silva and fake news about pedophilia involving prominent politicians.

for Russia.[26] Unlike Russian FIEs, Iranian trolls have attacked President Trump, the Republican party, and Secretary of State Mike Pompeo, though both have produced content supporting Brexit.

In the MENA region both Russian and Iranian trolls have worked to obscure responsibility for violence by the Syrian government and to push narratives favorable to the Syrian armed forces, as well as, pushing their own agendas (Barojan 2018*b*, Nimmo & Brookie 2018*b*). Iranian trolls have also attacked both the Israeli and Saudi Arabian governments (Kanishk et al. 2019).[27] In Latin America, we found some evidence of influence efforts, but not with the level of coordination seen in the US, Europe, and the MENA region (Nimmo 2018*a*).

Appendix B provides summaries of each of the foreign influence efforts included in the final database.

4 Conclusion

Foreign Influence Efforts (FIEs) have targeted countries around the world since 2014. While Russia has been the most active user of this new form of statecraft, other countries are following suit. Iran and China have deployed similar tactics beyond their own borders and even democratic states such as Mexico have adapted these techniques for internal purposes (Melendez 2018, Love et al. 2018, Linthicum 2018)

We hope this report and data will provide useful background for those studying these trends. Our underlying data and this report will be updated regularly.

[26] Nimmo (2018*d*) presents evidence that the cluster of websites known as International Union of Virtual Media (IUVM) laundered Iranian state messaging by claiming it as their own and passing it on to other users. Those users then reproduced the information without referencing its ultimate origin.

[27] Lim et al. (2019) reported 72 fake domains that impersonated legitimate media outlets using a variety of typosquatting and domain spoofing techniques (e.g., bloomber**q**.com instead of bloomber**g**.com). This operation was linked to Iran by FireEye which traced back registration information and other indicators to Iranian origins.

5 Figures and tables

Table 1: Summary statistics

Variable	Freq.	Variable	Freq.
First sighting		Last sighting	
2013	1	2013	0
2014	9	2014	1
2015	10	2015	1
2016	15	2016	7
2017	12	2017	12
2018	6	2018	32
Variable	Mean	Variable	Mean
Actor		Platform	
Astroturf	0.08	Email	0.08
Company	0.40	Facebook	0.57
Cyber espionage group	0.08	Fake websites	0.15
Foreign government	0.17	Google	0.17
Intelligence Agency	0.19	Instagram	0.21
Real NGO	0.04	Line	0.02
Wealthy individual	0.06	News outlets	0.64
Unknown	0.26	Other media	0.15
		Reddit	0.09
Strategy		Twitter	0.83
Defame	0.64	Whatsapp	0.04
Persuade	0.57	Wikipedia	0.02
Polarize	0.15	Youtube	0.26
Shift agenda	0.06		
Undermine institutions	0.06	Tactic	
		Bot	0.53
Approach		Fake account	0.55
Amplify	0.77	Hashtag hijacking	0.17
Create	0.98	Other tactics	0.23
Distort	0.72	Steal information	0.13
		Troll	0.85

Foreign influence efforts (FIEss) are defined as coordinated campaigns by one state to impact politics in another state through media channels, including social, in a manner which involves producing content that appears indigenous to the target state. In total, 53 FIEs. Each category is not mutually exclusive.

Table 2.1: Strategy combination

	Defame	Persuade	Polarize	Shift agenda	Undermine
Defame	100				
Persuade	47	100			
Polarize	9	3	100		
Shift agenda	6	7	12	100	
Undermine	9	3	25	33	100

Notes: The table shows the percentage of foreign influence efforts (FIEs) that use the strategy of the row at the same time as the strategy of the column. Numbers are percentage. Each category is not mutually exclusive. 53 FIEs.

Table 2.2: Tactic combination

	Bots	Fake account	#Hijacking	Other tactics	Steal info.	Trolls
Bots	100					
Fake account	68	100				
#Hijacking	21	14	100			
Other tactics	25	17	11	100		
Steal info.	14	17	22	0	100	
Trolls	93	90	100	58	86	100

The table shows the percentage of foreign influence efforts (FIEs) that use the tactic of the row at the same time as the tactic of the column. Numbers are percentage. Each category is not mutually exclusive. 53 FIEs.

Table 2.3: Platform combination

	e-mail	Facebook	Fake websites	Google	Instagram	Line	News outlets	Other media	Reddit	Twitter	Whatsapp	Wikipedia	Youtube
e-mail	100												
Facebook	75	100											
Fake websites	50	20	100										
Google	25	30	12	100									
Instagram	0	30	25	44	100								
Line	0	0	0	0	0	100							
News outlets	50	60	25	78	73	100	100						
Other media	0	13	12	11	9	0	18	100					
Reddit	0	10	0	33	18	0	12	12	100				
Twitter	100	87	100	89	91	0	79	75	100	100			
Whatsapp	0	7	0	0	0	0	3	12	0	5	100		
Wikipedia	0	0	0	0	0	0	3	0	20	2	0	100	
Youtube	0	30	12	56	45	0	29	50	80	32	100	0	100

The table shows the percentage of foreign influence efforts (FIEs) that use the platform of the row at the same time as the platform of the column. Numbers are the percentage rounded to the closest integer. Each category is not mutually exclusive. 53 FIEs.

Figure 1: Relational database structure

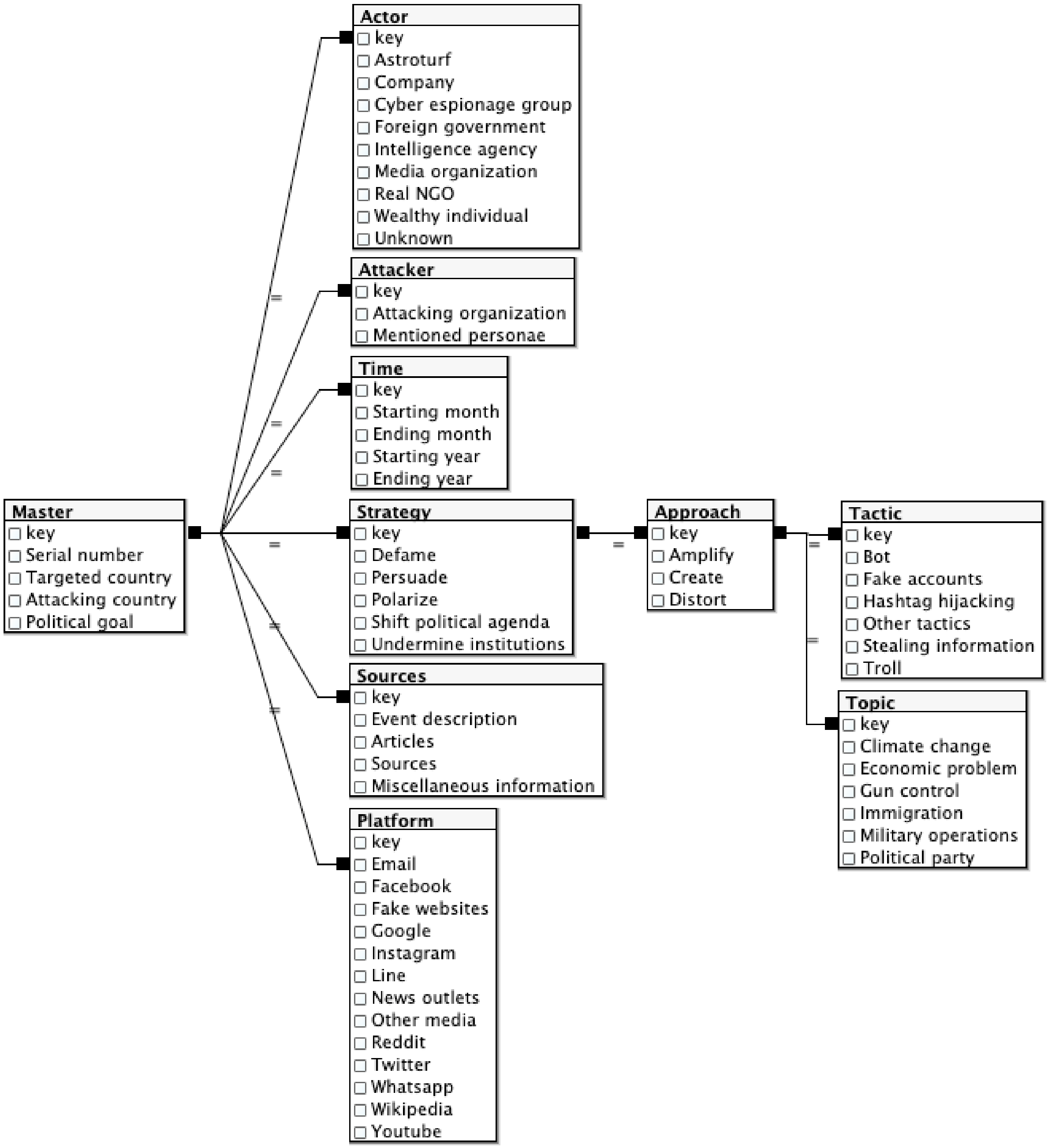


Figure 2: Approach

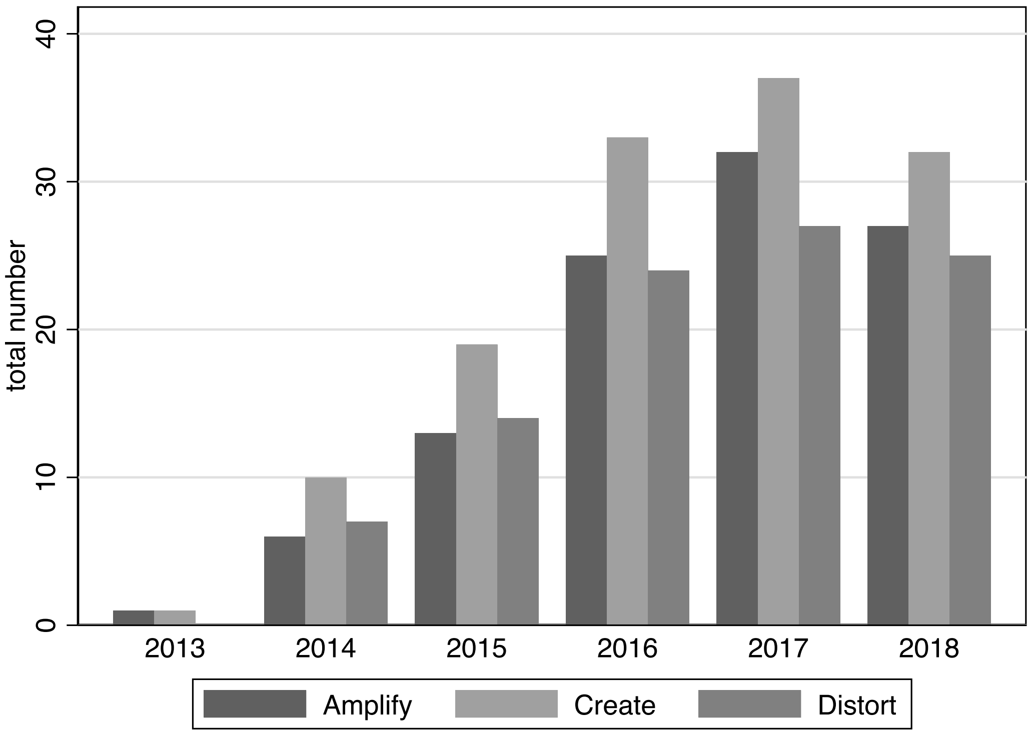


Figure 3: Origin of the attacks

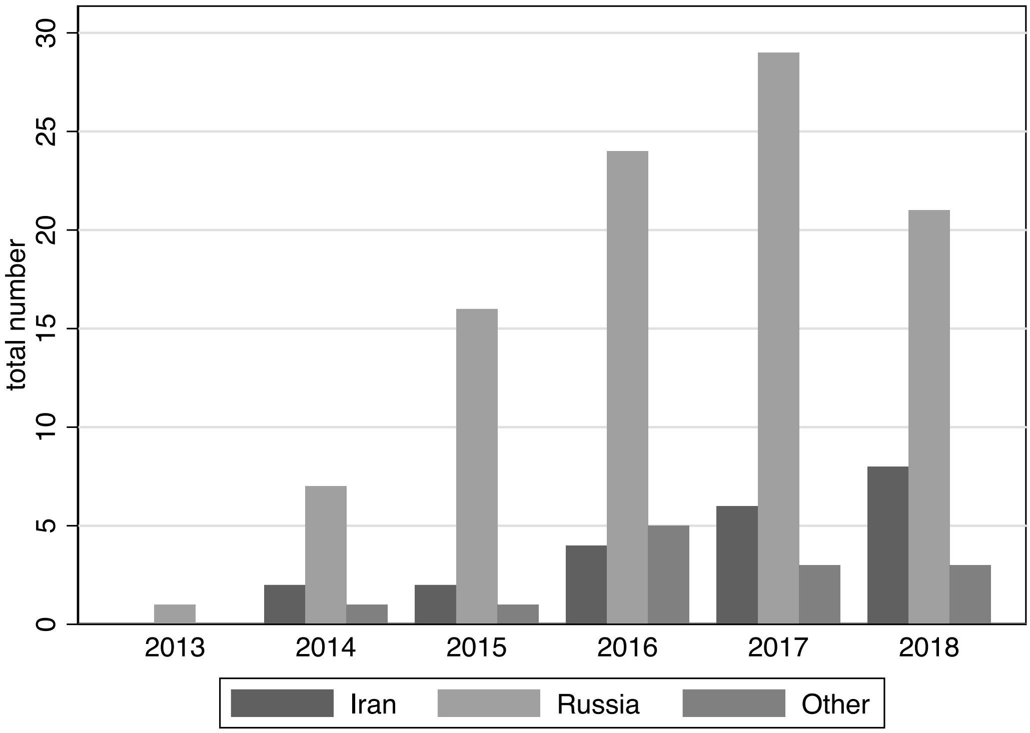
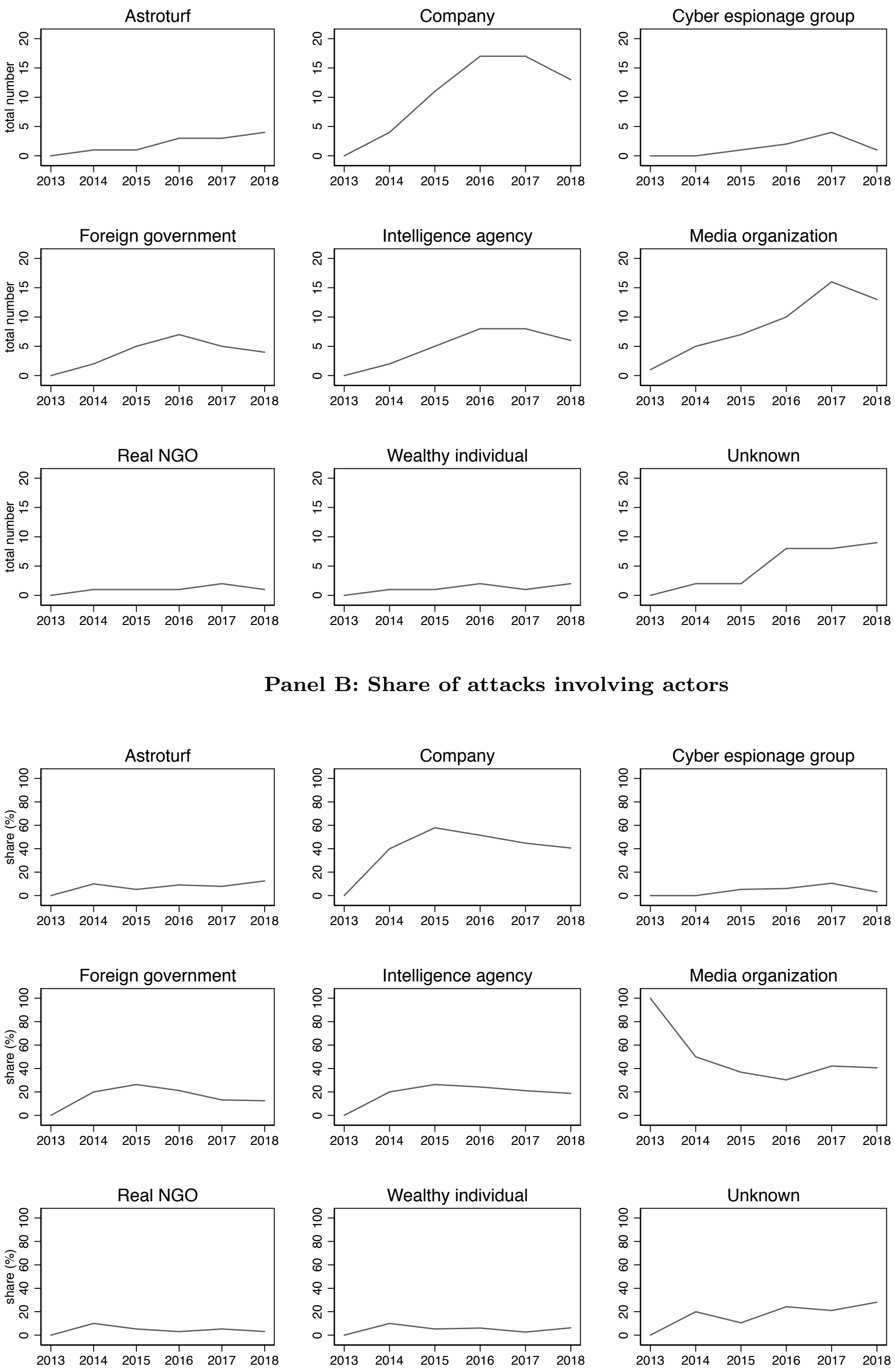


Figure 4: Actors

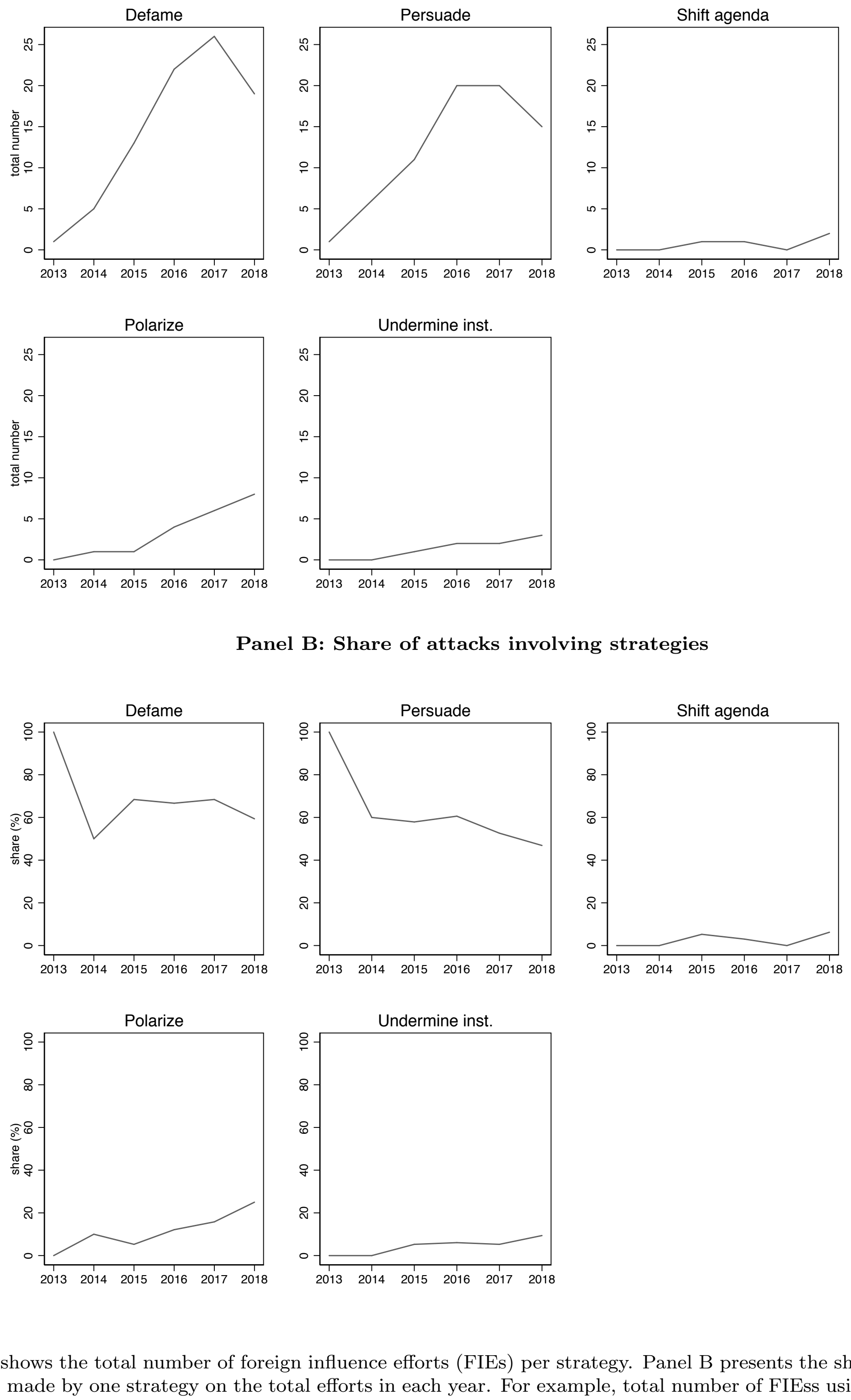


Panel A: Total number of attacks per actor

Panel B: Share of attacks involving actors

Panel A shows the total number of foreign influence efforts (FIEs) per actor. Panel B presents the share of the number of efforts made by one actor on the total efforts in each year. For example, total number of FIEss using company in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive

Figure 5: Strategy

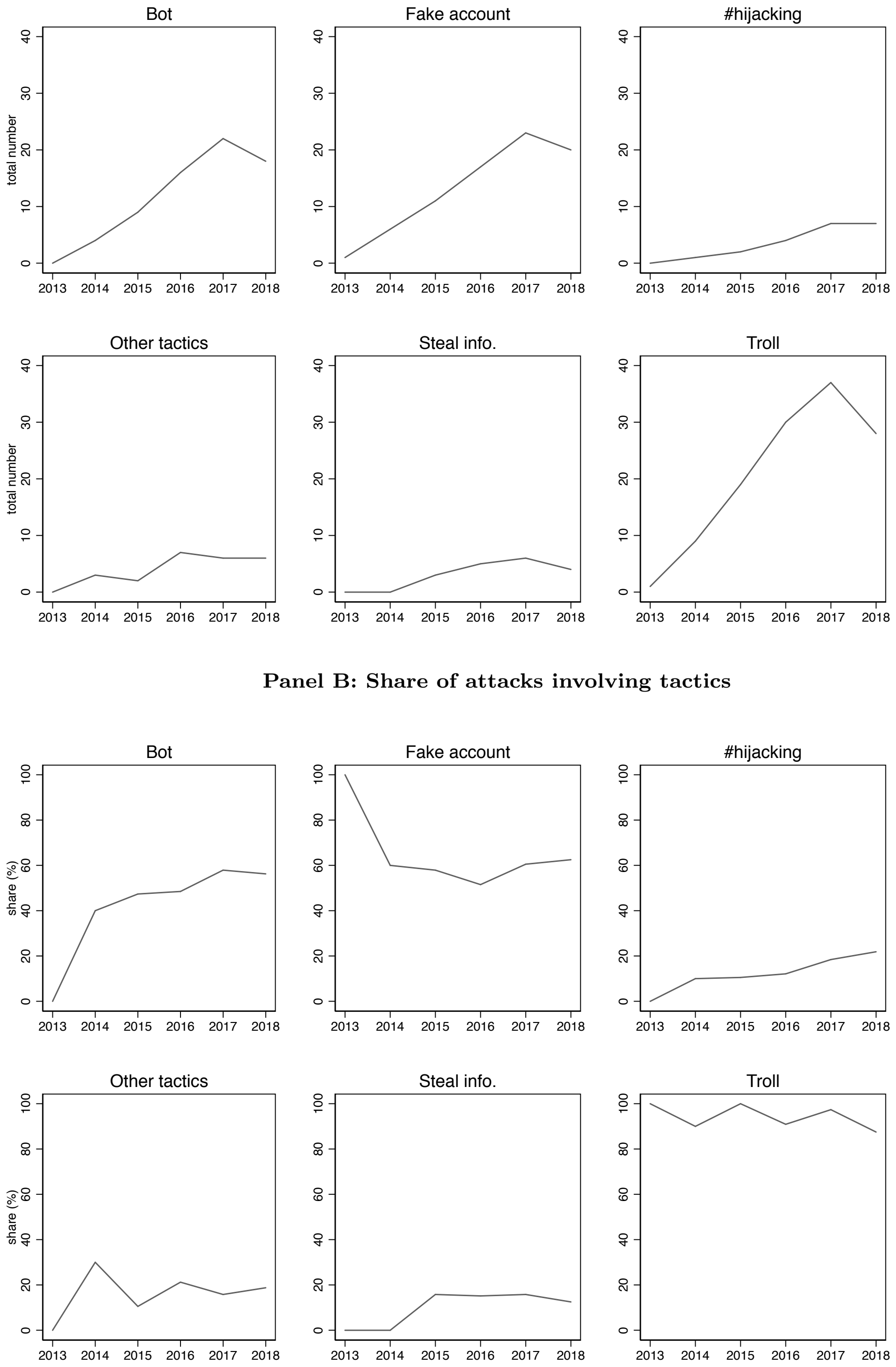


Panel A: Total number of attacks per strategy

Panel B: Share of attacks involving strategies

Panel A shows the total number of foreign influence efforts (FIEs) per strategy. Panel B presents the share of the number of efforts made by one strategy on the total efforts in each year. For example, total number of FIEss using defame in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive.

Figure 6: Tactic

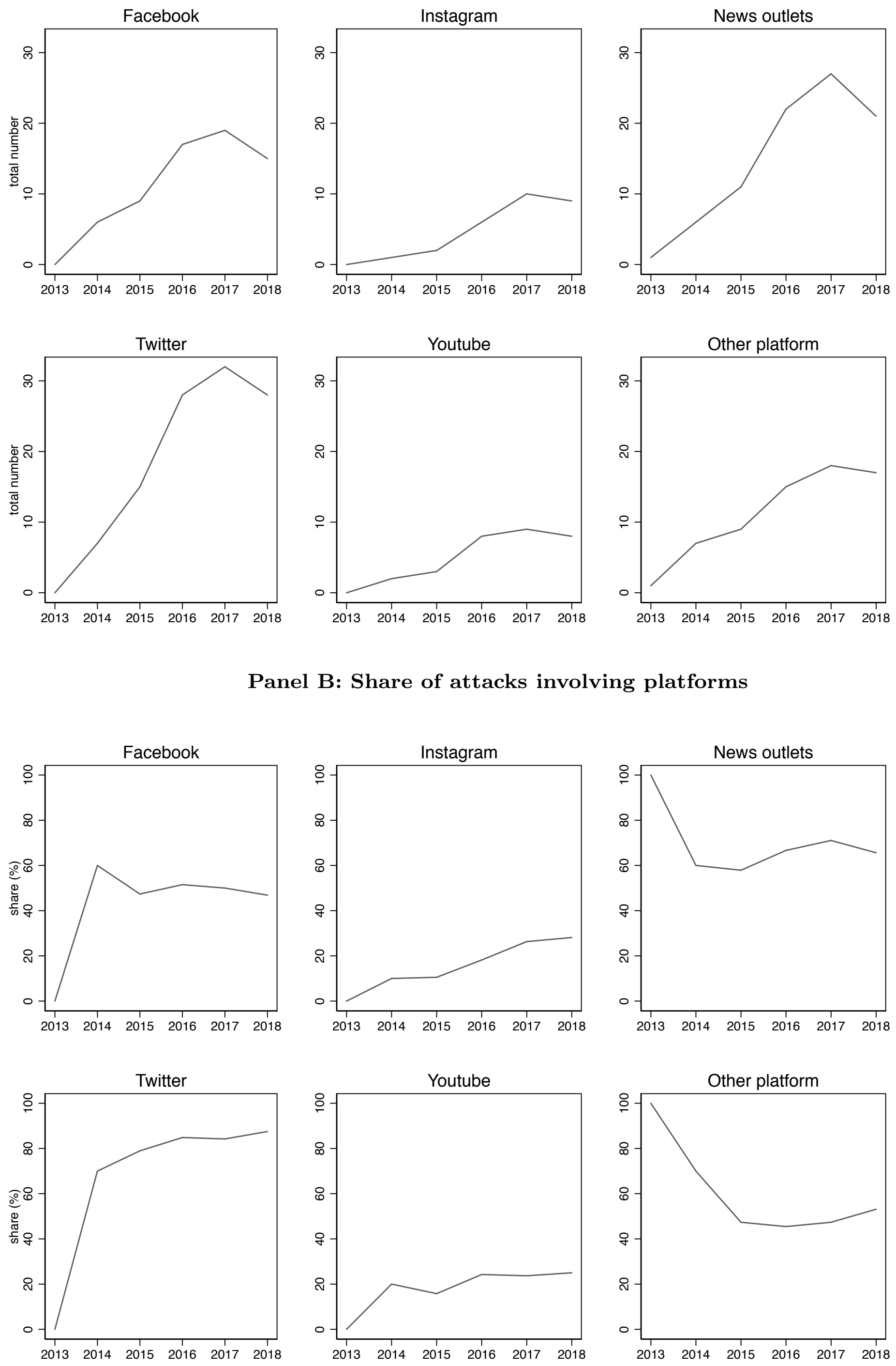


Panel A: Total number of attacks

Panel B: Share of attacks involving tactics

Panel A shows the total number of foreign influence efforts (FIEs) per tactic. Panel B presents the share of the number of efforts made by one tactic on the total efforts in each year. For example, total number of FIEss using trolls in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive.

Figure 7: Platform



Panel A: Total number of attacks per plarform

Panel B: Share of attacks involving platforms

Notes: Panel A shows the total number of foreign influence efforts (FIEs) per platform. Panel B presents the share of the number of efforts made by a platform on the total efforts in each year. For example, total number of FIEss using Twitter in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive. Other platforms category includes email, Google, fake websites, Line, other media which includes radio, TV, and news papers, Reddit, Whatsapp, and Wikipedia

A Codebook

Table A-1: Codebook

Variable	Definition	Example
	Master	
Serial number	Fourth digit code	0001 is the first identified effort against a country. The serial number starts again from 0001 for a new targeted country
Targeted country	Country under attack	Russia has an FIE in 2014 Crimea referendum, the 2016 U.S. presidential elections, Brexit referendum in 2016, 2017 France elections. Write the three letters code used by the World Bank. We include a category called multiple for the liberal Western states.
Attacking country	The country which planned and/or ordered the attack. In cases where a country sends the attack, but the plan and the orders come from another country, this variable shows who orders the attack.	Russia hired people in Macedonia for creating fake news of U.S. In this case, the attacks come from Russia, not Macedonia. Write the three letters code used by the WB. Code UKN means unknown country.
Political Goal	Open-text field describing the broad political objective of the effort. This is the primary thing the attacker wants to accomplish as best can be inferred from the preponderance of the reporting on that effort	Changing US policy in Syria/Ukraine/Balkan/etc. Make people distrust the political system. With Brexit the political objective was to get the UK to vote to leave the EU. With many 2016 U.S. presidential elections efforts it was get President Trump elected or with Roy Moore it was to support Roy Moore's reelection campaign in the Sep. '17 special election in Alabama.

	Time	
Starting month	The earliest month where the attack started.	The earliest attack seen was in January.
Ending month	The latest month where the attack started.	The latest attack seen was in December.
Starting year	The earliest year where the influence effort was made.	Document methods employed by Internet Research Agency (IRA) to influence the political agenda of the U.S. from June 19, 2015 to December 31, 2017. For this example, the start year is 2015.
Ending year	The latest year where the influence effort was made.	Document methods employed by IRA to influence the political agenda of the U.S. from June 19, 2015 to December 31, 2017. For this example, the end year is 2017.
	Attacker	
Mentioned personae	Name of websites, Facebook profiles, Twitter accounts or people, which are mentioned by the news as possible creators and amplifiers of misinformation and fake news. NA means that the sources do not have information from the organization in charge of the attack	Yevgeny Prigozhin is considered by the U.S. as one of the heads in the Russian media attack to elections in 2016.
Attacking organization	Name of the primary organization responsible for the attacks. NA means that the sources do not have information from the organization in charge of the attack.	IRA is widely considered to be the main organization producing propaganda in favor of Donald Trump during the 2016 Presidential Election.

Actor		
Astroturf	Equal to 1 when a false organization or social movement is being created as part of the attack.	A mysterious group used the death of Philando Castile, shot by a police officer, to create a movement called Don't Shoot and organized protests outside the police department where the responsible officer works. When people from CNN and Black Lives Matter tried to look for the origin of Don't Shoot they found that it was a fake website run from Russia.
Company	Equal to 1 when a person working for a corporation (e.g. Yevgeny Prigozhin) or company orders or directs operation to influence political decisions in a foreign country in pursuit of corporate goals	IRA is a Russian company based in Saint Petersburg. Yevgeny Prigozhin, a Russian businessman with ties to Russian president Vladimir Putin, controls "a network of companies", including three accused of interference in the 2016 United States elections.
Cyber espionage group	Equal to 1 when an attack is conducted by a group that engages in a range of cyber activities, e.g. is on Fireye's list of Advanced Persistent Threats	According to Microsoft, APT28, a group in the list of Fireye and publicly linked to a Russian intelligence agency, creates websites to steal information from conservative groups which criticized of U.S. President Donald Trump.
Media organization	Equal to 1 when an attack is conducted by an established company, with an installed capacity in terms of employment and buildings. It is not a news web page working for just a short period of time or closed after the Influence effort was done. Must be a for-profit concern or one whose main business is breaking news.	RT (formerly Russia Today) is a Russian International television network, as well as providing Internet content in English, funded by the Russian Government. It operates directed to audience outside of Russia.

Intelligence agency	Equal to 1 when an attack was conducted by an intelligence agency of a country or subsidiary directly controlled organization	Main Intelligence Directorate of the General Staff (GRU). Bots from the "troll army" tweet using hashtag Brexit in favor of Brexit. Press reports suggest this activity was directed by GRU.
Foreign government	Equal to 1 when politicians order the effort to influence political decisions in a foreign country or when they are part of the strategy.	The Grand Jury for the District of Columbia said the Russian Federation operated a military intelligence agency called the GRU. This is evidence that a foreign government is the actor of this FIE.
Real NGO	Equal to 1 when an attack is executed by an activist group that is neither government nor for-profit corporation. This category includes Wikileaks, Openleaks, AJTransparency.com, Globalleaks.com, Balkanleaks.eu, etc.	Maria Katasonova launched the hashtag dislikeMacron. She is a Russian nationalist who works for a high-ranking politician, heading up the "Women for Marine" movement and she is part of a Russian patriotic artists' collective.
Wealthy individual	Equal to 1 when a rich individual order a campaign to influence political decisions in a foreign country. It is not 1 when the wealthy individual mentioned is the CEO of a company conducting the campaign.	Russians businessmen create media propaganda to reduce the prices of land in South Africa, where apparently, they are interested in buying and build a nuclear plant.
Strategy		
Defame	Equal to 1 when there is a direct attack against a person, intended to discredit him or her.	IRA create fictitious social-media personas to spread falsehoods and promote messages against Hillary Clinton.
Persuade	Equal to 1 when there is an influence effort with which goal appears to be directly shift political views about an issue or actor in an identifiable direction. This affects the median voter in one direction.	Trolls create blogs and fake news to incentive people to vote in favor of Donald Trump. These trolls do not push the Hillary Clinton campaign at the same time.

Polarize	Equal to 1 when an attack aims to create polarization on issues. This is persuasion on both sides of an issue to move individuals to the extremes. This affects the variance of the decision because it looks for pushing one political goal in two opposite directions.	Nearly 600 Russia-linked accounts tweeted about the US Affordable Care Act - ObamaCare. The majority of the nearly 10,000 tweets on the Affordable Care Act seemed intended to pit one side against the other, not to advance a particular policy with respect to the ACA.
Shift political agenda	Equal to 1 when the efforts add something new in the political agenda.	Russia plans to eliminate the American energy threat, as an exporter of this source, and to do so by influencing social media users, American voters, and public officials.
Undermine institutions	Equal to 1 when the objective is to reduce the credibility/reputation of one or more institutions in the target country. This category includes Armed Forces (including the FBI), the national congress (but individual parties are not institutions), and system justice (including courts).	Russian media outlets circulated a false story about a state prosecutor in Berlin failing to prosecute an alleged rape by immigrants.

Platform

Email	Equal to 1 when an attack involves email with misinformation or looking for stealing information.	Phishing emails to access to conversations between Hillary Clinton and her team in the elections.
Facebook	Equal to 1 when an attack involves Facebook.	The IRA posts divisive American issues, including race, religion, gun laws and gay rights, particularly during the 2016 presidential election on Facebook
Google	Equal to 1 when an attack involves Google platforms.	Using Google accounts, Iranian trolls attack against Donald Trump
Fake websites	Equal to 1 when an attack involves the creation of fake websites to steal information or send a message pretending to be a different persona or institution. This category does not include news pages in other platforms.	GRU cloned the access web page to the official site of the Democratic Party, and when the participants of this political party entered their personal data, the hackers stole their information.

Instagram	Equal to 1 when an attack involves activity on Instagram	The official Instagram account of Angela Merkel, Chancellor of Germany, received a coordinate attack from Russian trolls, who post negative comments in every picture in the account, except for those ones with Vladimir Putin.
News outlets	Equal to 1 when an attack involves the creation of news websites. This category does not include news pages in other platforms.	Trolls in Macedonia create news websites against the Hillary Clinton campaign in the U.S election.
Other media	Equal to 1 when an attack uses TV, newspapers and Radio.	News providers in Ukraine with Russian shareholder are more restrained in their criticism of Russia than comparable news providers without support of Moscow.
Reddit	Equal to 1 when an attack involves Reddit platform.	Reddit accounts were involved spreading message against Hillary Clinton and in favor of Donald Trump in the 2016. Presidential elections.
Twitter	Equal to 1 when an attack involves Twitter.	Twitter released more than 10 million tweets that had been circulated by propaganda farms and their associated puppet accounts.
WhatsApp	Equal to 1 when an attack involves WhatsApp platform.	Using WhatsApp, Russia spread rumors saying that Hillary Clinton was in favor of White Americans.
Wikipedia	Equal to 1 when an attack involves manipulating Wikipedia	Russian Trolls create Wikipedia web pages about conservative critics of Trump, such as Marco Rubio, saying that they were fake conservatives.
YouTube	Equal to 1 when an attack involves YouTube.	Iranian Trolls create YouTube propaganda against Donald Trump saying that Trump wastes the public resources of the United States.

Source

Event description	Succinct 1-3 sentence description about the objective, political goal, and topic of the attack.	People in the troll factory create fake social media accounts and writes blog posts meant to show divisions in the U.S. and turn Russians against Americans.
Miscellaneous information	Relevant information about classification of any variables.	The fake profile Melvin Redick was used by Russians to spread the stolen emails from Hilary Clinton campaign.
Source	Provide link to where news and media sources related to the influence effort can be found. Include at least three sources per FIE	`https://www.justice.gov/file/1080281/download`
Articles	Provide full citation to articles related to the influence effort. Each effort will have multiple associated articles.	Boatwright, B. C., Linvill, D. L., & Warren, P. L. Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building. `http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf`

Approach

Amplify	Equal to 1 when an individual (Trolls or Bots) work to promote specific content, whether real or fake.	A suspected network of 13,000 Twitter Bots retweeted and share media in favor of Brexit before the referendum.
Create	Equal to 1 when the effort is to create an entirely new narrative around a set of events. May or may not include creating false information.	Aleksei, the troll from St. Petersburg, said the first task assigned to all new employees was to create three identities on Live Journal, a popular blogging platform. The main thread running through the blog posts and the commentary was that "life was good in Russia under Putin and it was bad in the U.S. under Obama.
Distort	Equal to 1 when a person or a group creates false information about objectively verifiable facts. This includes promoting conspiracy theories.	A well-known Russian twitter account said "Muslim woman pays no mind to the terror attack, casually walks by a dying man while checking phone". This message was amplified by a Russian network in the same social media. The woman denied this version.

Tactic		
Bot	Equal to 1 when an automatic is used. Retweet or share misinformation or fake news on a preset schedule or in response to identifying specific signals.	Bot-like accounts are those with number and ratio of tweet to retweets much higher than the average accounts. An account tweeted 3,176 times, at an average rate of 453 a day. Of those tweets, 3,122 were retweets, a rate of 98%.
Fake accounts	Equal to 1 when the effort creates fictitious personas, or if there is misuse of a real person's identity. Record in notes if ambiguous.	Creation of an account in someone's name that is not controlled by them
Hashtag hijacking	Equal to 1 when an attack uses hashtag to amplify their propaganda	Russian accounts on Twitter amplified the hashtag NotInMyNameTheresaMay, after Rachael Swindom, a prominent Labor party campaigner, tweeted out a poll asking if Twitter users support Theresa May's plans to "bomb Syria".
Other tactics	Equal to 1 when an attack uses a different tactic from trolls, bots, hashtag hijacking, stealing information and fake accounts	A network of websites and social media pages which have been traced to Iran posted pro-Tehran articles mixed in with content taken from bona fide websites, and shared content attacking Saudi Arabia. It is unclear if trolls are behind these pages
Stealing information	Equal to 1 when a person tries to steal sensitive data	Phishing emails to access to conversations between Hillary Clinton and her team in the elections.
Troll	Equal to 1 when a person (or people) create a large volume of content for executing influence operations. Can be independent or contractor. The distinguishing characteristic is the volume of content and focus of the content and the fact that it is produced and disseminated manually.	Lyudmila Savchuk spent most of her time at the troll farm writing as an imaginary Russian woman on the LiveJournal blogging platform, widely used in Russia today.

	Topic (selected list)	
Economic problem	Equal to 1 when an attack exploits an economic issue	Russian trolls use the Keystone XL pipeline in Canada to generate division in the country
Gun control	Equal to 1 when an attack exploits gun control	Russian media organization create posts claiming that Sweden sells weapons to Islamic state
Immigration	Equal to 1 when an attack exploits immigration	In the Brexit Referendum, trolls post several tweets claiming that many people would migrate to England if the United Kingdom did not leave the Europe Union
Military operations	Equal to 1 when an attack exploits military operations	Russian trolls use the NATO's military exercises in Estonia to claim that the country prepared an attack against Russia.
Political party	Equal to 1 when an attack exploits politicians and political parties	Russian trolls attack Hillary Clinton, while they support Donald Trump.

Notes: For each attack we code both the principal ordering the attack and the agent(s) responsible for carrying it out in the table Actor. In the future we may seek to make a distinction between principles and agents. Strategy is the approach taken to achieve the goal or the things one needs to do to achieve a political goal. Topic, can be multiple topics per attack, each strategy in a given attack gets the topics employed in that strategy assigned to it. Approach is a measurable thing you do to achieve a strategy. Tactics are the tool, the implementation, the concrete actions that people or organizations can take.

B Annotated List of Foreign Influence Efforts

This section summarizes key details of all 53 foreign influence efforts included in the database. The references and details are not exhaustive. For full details please consult this link. Each FIE has a unique identifier which combines the ISO3 code for targeted country, the ISO3 code for the attacking country, and a sequential serial number based on the order in which we found the FIE[28]. The following annotated list is organized by this code.

AUSRUS0001. Targeted country **Australia**. Attacking country **Russia**. Political goal **Undermine the Australian government**:

The Internet Research Agency (IRA), a Russian "troll factory", targeted Australian politics on social media between 2015 and 2017, according to the 3 Million Russian Troll Tweets released by Linvill & Warren (2018). As in the US elections and Brexit referendum, Russian trolls leveraged events in the news. 5,000 of their tweets, for example, mentioned the terms "#auspol" or "MH17" (Linvill & Warren 2018, Sear & Jensen 2018). The activity focuses on the downing by pro-Russian forces in the Ukraine of Malaysia Air flight MH17 correlated with the Australian government's deployment of fighter aircraft to operate in Syrian airspace where Russian aircraft were also operational. During this period, the Australian Defence Forces (ADF) were also confronted by Russian military

[28] AUSRUS0001, for example, is the first FIE we identified in which Australia was taregted by Russian actors.

cyber operations (Mason 2018).

AUSRUS0002. Targeted country **Australia**. Attacking country **Russia**. Political goal **Polarize Australian politics**:

Russian Twitter trolls, belonging to the Internet Research Agency, targeted Australian politics, primarily through attempts to stoke anti-Islamic sentiment. According to Michael Jensen, an associate of the News and Media Research Centre and senior fellow at the Institute for Governance and Policy Analysis, Russia-linked accounts seemed "interested in amplifying social divisions, in particular distinctions between Muslims and the rest of the population" and they "emphasize links to terrorism extensively". (Karp 2018). Russian trolls touched on a range of other hot-button issues such as the 2014 downing by Russian-supported rebels of Malaysian Air Flight 17 (Sear & Jensen 2018). These and other activities led to the passage of the "Foreign Influence Transparency Scheme Bill" by the Australian parliament in June 2018.

Russian trolls linked to Internet Research Agency (IRA) also targeted the 2016 Australian federal elections (Bogle 2019). Around 3,841 Twitter accounts in the sample of 3 million tweets collected and released by Linvill & Warren (2018), attempted to exploit anti-Islamic sentiment in the Australian population. One Russian account called PidgeonToday, for example, posted: "I wonder why #ReclaimAustralia is racist and bigoted and Muslims calling for beheading are just offended protesters?" (Owens 2018, Sear & Jensen 2018). Researchers from Canberra University in Australia claim that Russian trolls aimed at amplifying social divisions, as in the 2016 US presidential elections (Karp 2018).

AUTRUS0001. Targeted country **Austria**. Attacking country **Russia**. Political goal **Undermine Sebastian Kurz in the 2017 Austrian Presidential election**:

The campaign involved a range of actions on social media. Two Facebook sites, for example, posted photo-shopped images and video clips that accused Sebastian Kurz of supporting immigration from Islamic countries, and of being part of the "dubious political network" of the Hungarian-American financier Soros (Oltermann 2017). After Sebastian Kurz became chancellor designate in Austria, YourNewsWire.com, a site "used by the Russians as a proxy site to spread disinformation" (Oltermann 2017), amplified false information that Kurz wanted to expel Open Society Foundations, the philanthropic organization founded by Soros, from the country. This item was spread on social media and through other sites claiming to fight "the new world order" (Stojanovski 2017).

BLRRUS0001. Targeted country **Belarus**. Attacking country **Russia**. Political goal **Undermine Belarus government**:

In Fall-2018, Russian media began promoting a number of narratives targeting Belarus and its leader Alexander Lukashenka (Belsat 2018). As part of the campaign, the Russian government allegedly paid bloggers in Belarus small amounts on a per-item basis to make it appear there was strong support in Belarus for union with Russia (Goble 2019).

BRARUS0001. Targeted country **Brazil**. Attacking country **Russia**. Political goal **Polarize Brazilian elections**:

A study of the spread of misinformation in Brazil from August to September 2018 showed an effort on Twitter, Facebook and Whatsapp to influence Brazilian elections(Ruediger

2018, Benevides 2018). Analysts identified a group of 232 profiles previously active in other countries which spread messages involving Jair Bolsonaro, Luiz Inácio Lula da Silva and fake news about pedophilia. The group produced 8,185 Twitter posts related to Brazilian politics in Portuguese between August 1 and September 26, 2018 (Ruediger 2018).

CANRUS0001. Targeted country **Canada**. Attacking country **Russia**. Political goal **Polarize Canadian politics**:

Of the 3 million English-language tweets which Twitter identified as being produced by Russian trolls in 2018, close to 8,000 mentioned Canadian issues such as asylum seekers, the Quebec City mosque shooting, and the Keystone XL pipeline (Linvill & Warren 2018). The strategy seems to have been to sow division within Canadian politics (Rocha 2018). Russian trolls even tried to get Canadians exercised about US football players kneeling during the playing of the National Anthem to protect police violence. Some of the more active accounts that tweeted about Canadian issues had between 2,300 and 44,000 followers. Most were categorized by the researchers as "Right Trolls," who tweet inflammatory views with a right-wing slant (Linvill & Warren 2018).

ESPRUS0001. VBVTargeted country **Spain**. Attacking country **Russia**. Political goal **Support Catalonia independence in 2017 referendum**:

Russian-based groups used online social media to heavily promote Catalonia's independence referendum last month in an attempt to destabilize Spain, according to Spanish government sources in 2017 (Emmott 2017). Spain's defense and foreign ministers said they had evidence that state and private-sector Russian groups used Twitter, Facebook and other Internet sites to massively publicize the separatist cause (Emmott 2017). Germany's intelligence chief also accused Russia of seeking to destabilize Spain by backing separatists in Catalonia, claiming it was "very plausible" that Moscow had carried out a campaign of disinformation before the secession referendum in October 2017 (Keeley 2018).

FINRUS0001. Targeted country **Finland**. Attacking country **Russia**. Political goal **Promote Russian Propaganda**:

After the Finnish government imprisoned two pro-Kremlin individuals, Ilja Janitskin and Johan Backman, Russian trolls started a campaign against the government, calling the procedure "unlawful" and "targeted at Russians" (Szymański 2018, BBC 2018*a*). They cited the head of MV-Lehti, an "anti-immigrant, racist, pro-Russian news source", to argue the imprisonment violated human rights (Higgins 2018). The campaign also used similar tactics as in the Baltic countries to persuade Finns to oppose plans for Finland to join NATO (Rosendahl & Forsell 2016). The trolls, for example, suggested that joining NATO would be the end of Finnish Independence from foreign actors (Withnall 2018).

FRARUS0001. Targeted country **France**. Attacking country **Russia**. Political goal **Attack Emmanuel Macron in the 2017 French elections**:

President Emmanuel Macron said many times that "Russia and Sputnik" spread fake news about him during the 2017 Presidential Campaign (Tait 2017, Michel & Dyomkin 2017). One such incident included a cache supposedly containing a plethora of confidential information about Macron being leaked on several internet platforms, mostly in a peer-to-peer manner. Websites and handles that spread the information were tied to Russian addresses, and many scholars claim that the primary perpetrators were from a group known as Fancy Bear, Pawn Storm, or APT28 (Auchard & Felix 2017).

Facebook suspended over 30,000 accounts 10 days before French Elections on April 23, 2017, that they suspected were automated and linked to Russia (Auchard & Menn 2017).

Another signal pointing to Russia the attacking country was the fact that information stolen from Macron was edited in a Russian-language version of Microsoft Excel before being released to the public (Brewster 2017). Bots and Twitter accounts linked to WikiLeaks spread the fake documents using the hashtag #MacronLeaks, including by some US far-right activists, who had previously attacked the Democratic Party to help Donald Trump in the 2016 US Presidential Elections (Volz 2017*a*, Mohan 2017).

FRAUNK0001. Targeted country **France**. Attacking country **Unknown**. Political goal **Attack Emmanuel Macron in the 2017 French elections**:

A network of accounts on Facebook spread propaganda, mostly in French, from mid-2017 to November 2018 attacking Emmanuel Macron (Nimmo & Francois 2018, Gleicher 2018*b*). Macron Leaks had similarities to Russia's 2016 US interference. Most of the material came from the hacked Gmail accounts of people connected to Emmanuel Macron's campaign, and they were promoted breathlessly on social media by Twitter bots (Volz 2017*b*). While there are sources saying that Russia is behind the attack, there is no concrete evidence to prove this statement. The French government said it could find no evidence that Russia was behind the hacks. "It really could be anyone," a French cybersecurity official said at the time (Poulsen 2018).

GBRIRN0001. Targeted country **Great Britain**. Attacking country **Iran**. Political goal **Support Brexit referendum in 2016**:

Individuals with ties to Iranian state media set up social media accounts with fake names in an effort to influence Britain's vote to leave the European Union. These Facebook accounts also posted content backing Jeremy Corbyn, leader of Britain's opposition Labour Party (Guynn 2018*b*).

In 2018 Facebook announced that it had removed 82 accounts, groups, and pages since 2016 which had Iranian origins but were pretending to be Americans or British (Gleicher 2018*c*). The accounts were removed for "engaging in coordinated inauthentic behavior on Facebook and Instagram" (Gleicher 2018*a*). Twitter was also used to encourage people to vote in favor of the Brexit referendum, with 770 distinct Iranian-managed accounts spreading disinformation and intensifying their activity on June 26, 2016, the day of the Brexit vote (Field & Wright 2018). The campaign was complemented by attacks on politicians, such as former UK Independence Party (UKIP) leader Nigel Farage and former Foreign Secretary Boris Johnson, while praising others, e.g. Labour leader Jeremy Corbyn (Field & Wright 2018).

GBRIRN0002. Targeted country **Great Britain**. Attacking country **Iran**. Political goal **Support Scottish succession**:

Among the 654 accounts taken down by Facebook in 2018, several promoted a page called Free Scotland 2014. With more than 20,000 followers, the Iranian-backed page was one of several pages connected to fake "news" sites, including one linked to Iran's main propaganda source, Press TV (Dick 2018). Nearly 1,000 Twitter and YouTube profiles linked with Iran were eventually taken down (Michel 2018).

GBRRUS0001. Targeted country **Great Britain**. Attacking country **Russia**. Political goal **Support Brexit referendum in 2016**:

Thousands of Russia-linked Twitter bots promoted messages in favor of Brexit in the weeks leading up to the June 2016 referendum (Burgess 2017). More than 13,000 bot accounts re-tweeted and shared messages that contained racist and anti-immigrant rhetoric. 400 Russian trolls using fake Twitter accounts also produced divisive and racist rhetoric to persuade voters in favor of leaving the Europe Union. Many of these accounts were tracked back to the Internet Research Agency (IRA). Some of these accounts promoted anti-immigrant sentiments and shared posts aiming to incite political discord between those in favor of Brexit and those opposed (Burgess 2017). The pro-Brexit campaign continued for some time after the referendum. And, as in the case of the US 2016 presidential elections, the Russian trolls opportunistically used real events to promote their pro-Brexit message. After the June 2017 terror attack on London Bridge for example, an account linked to the Russian effort used a photograph of a Muslim woman looking at her phone walking along the bridge to stir anti-Islamic sentiment, claiming that the woman ignored the injured (Ball 2017, Hern 2017).

GBRRUS0002. Targeted country **Great Britain**. Attacking country **Russia**. Political goal **Criticize U.K. participation in the Syrian conflict**:

Russian troll activity in the U.K. picked up after the British government accused Russia of "illegal use of force" in the attempt to poison former spy Sergei Skripal on March 4, 2018 (Nimmo 2018*b*). Following the April 7, 2018 chemical weapons attack in Douma, Syria, the U.K. announced plans to join the US in a military response. British social media users launched a campaign under hashtag #NotInMyNameTheresaMay, which asked Prime Minister to not get involved in the Syrian conflict. The poll was amplified by pro-Kremlin users (Baroja 2018). The British government later reported that there was a 4,000 percent increase in activity by bots and trolls linked to Kremlin after the strikes as part of the larger Russian effort (Staff 2018).

GBRRUS0003. Targeted country **Great Britain**. Attacking country **Russia**. Political goal **Attack Theresa May's decision about military intervention in Syria in 2018**:

In 2018, Russia-linked Twitter accounts amplified and created content criticizing UK Prime Minister Theresa May's decision to support military action with the US against Syria after the April 2018 chemical weapons attack in Douma. This campaign included both re-tweeting and posting comments using the hashtag #NotInMyNameTheresaMay. These trolls, for example, pushed an online poll started by prominent Labour party campaigner Rachael Swindon (who has 68K followers on Twitter (Di Stefano 2018)) asking if Twitter users support May's plans to "bomb Syria". The hashtag was also promoted by Russian-run media organizations. Sputnik News, for example, wrote an article entitled "Not in my name, Theresa May: Social Media users oppose UK strikes in Syria" and published it using the same hashtag in social media. RT also used the poll's result in an article entitled "43% of Britons lack appetite for war in Syria" (Baroja 2018), an exemplar of the links between content promoted on social media and that in state-supported outlets.

GERRUS0001. Targeted country **Germany**. Attacking country **Russia**. Political goal **Support Alternative for Germany (AfD) for the Federal Elections in 2017**:

Efforts by the Russian government to influence the 2017 German Federal Election began in May 2017. Material from German-language news outlets connected to the Russian government—such as RT Deutsch, Sputnik Deutsch, and NewsFront Deutsch—was used by pro-Russian activists such as AnnaLenaDo and Ollissya to justify support for the right-of-center Alternative für Deutschland (AfD) party (Neuman 2018). Other attempts to influence the German electorate include; the specific targeting of Russian-speaking Germans through pro-AfD messages in Russian; social media accounts amplifying a fake anti-migrant story where a 13-year old Russian-German girl falsely claimed she was raped and kidnapped by migrants; and bots and trolls tied to Russia defaming the Merkel-led government and accusing it of not punishing migrant crime (Snegovaya 2017).

GERRUS0002.Targeted country **Germany**. Attacking country **Russia**. Political goal **Undermine Angela Merkel and her political decisions**:

Russia targeted German Prime Minister Angela Merkel in 2015 in a manner similar to their actions against Hillary Clinton in the 2016 US presidential election. According to German officials, the cyber espionage group APT28 tried to steal information from Germany's lower house of parliament, the Bundestag, and Angela Merkel in 2015 (Neuman 2018). Just days after Angela Merkel set up her Instagram account, thousands of Russian trolls began insulting the people in Merkel's pictures. One of the comments tells Merkel that the Russians "will soon be in Berlin again." A picture of the Chancellor meeting Ukrainian president Petro Poroshenko received several comments, comparing the two leaders to Nazis, making personal insults about Merkel's appearance, and using aggressive sexual threats. The only positive comments in Russian were added to an image of Merkel and Russian President Vladimir Putin (Griffin 2015). The campaign also included the creation of around 2,500 fake news posts, aiming to contradict Merkel's policy toward refugees (Kroet 2017). These posts were coordinated with content on Russian media outlets that systematically challenged key decisions of Merkel's CDU party, especially by calling into question her controversial decision to allow thousands of refugees to enter Germany in August 2015 (Brattnerg & Maurer 2018). At least some of the onslaught of anti-Merkel content on Twitter came from bot accounts and trolls that previously backed Donald Trump in the 2016 US election (Snegovaya 2017).

The campaign was complemented by creating and spreading false stories about immigrants in Berlin who kidnapped and raped a Russian-German girl. This fake scandal mobilized the Russian-speaking German population against Merkel's government. The protests were not publicly announced or indexed on search engines, with word spreading instead via personal invitation through social networks like Facebook, and through encrypted messaging services like WhatsApp and closed groups on VKontakte (Snegovaya 2017).

GERUNK0001. Targeted country **German**. Attacking country **Unknown**. Political goal **Polarize German politics**:

Anonymous online trolls and extremist agitators were active in the 2017 German federal election. Some of the content they used originated among right-wing social media users in the US, and there is some evidence that American users were directly active in promoting right-wing groups in Germany (Hjelmgaard 2017). Some of the anti-Merkel content on

Twitter came from bot accounts and trolls that shifted from bolstering Donald Trump to trying to tear down Angela Merkel (Silverman 2016).

ISRIRN0001. Targeted country **Israel**. Attacking country **Iran**. Political goal **Attack Israeli government and promote Iranian view**:

As in Saudi Arabia, Iranian accounts promoted anti-Israel content on Facebook, Twitter and Google Plus (Dave & Bing 2018). News outlets managed from Iran posted articles in Hebrew which appeared designed to influence public opinion in Israel. Tel Aviv Times Hebrew and at least two other sites, for example, carried fake news about the Israeli government (Yaron 2018). They also amplified content from Canadian-based site globalresearch.ca, a known hub of false stories, including one accusing Israeli Prime Minister Benjamin Netanyahu of producing disinformation propaganda targeting Iranians (Nimmo 2018*a*).

ITARUS0001. Targeted country **Italy**. Attacking country **Russia**. Political goal **Support Five Star Movement (M5S) and far-right party the League (La Lega)**:

The Internet Research Agency managed thousands of Twitter profiles active in Italy during the 2018 Italian elections. These accounts mostly re-tweeted messages in support of two populist parties, the Five Star Movement and the League. Reporting by Milan-based dailer newspaper *Corriere della Sera* suggests that the trolls did not produce "original content", but instead retweeted content from prominent accounts sympathetic with the populist parties (Fubini 2018) Both parties have pro-Russia factions, oppose EU sanctions on Russia, and have appeared on Kremlin-backed media including RT and news agency Sputnik (News 2018).

LITRUS0001. Targeted country **Lithuania**. Attacking country **Russia**. Political goal **Distort relationship between Lithuania and NATO**:

Russia engaged in an extended campaign to discredit NATO in Lithuania and other Baltic states.[29]

The Russian campaign against European countries that are hosting NATO's operation in their territory has included spreading content intended to look like it was created in the targeted countries. Barojan (2018*a*), for example, describe how Pro-kremlin hackers placed an English article in the Lithuanian news outlet Kas Vyksta Kaune (What is Happening in Kaunas in English) on October 25, 2018. The article, an exact translation from the pro-Kremlin blogger, claimed that Anakonda 2018, a NATO exercise in Lithuania, aimed at occupying Belarus Kronitis (2018). Fake accounts and news outlets such as Black (2018) and The Russophile or Russia News Now spread the article. Kas Vyksta Kaune pulled down the article when it learned it had been hacked.

MULRUS0001.[30] Targeted country **Multiple**. Attacking country **Russia**. Political

[29] Russia publicly announced that The North Atlantic Treaty Organization (NATO), a military alliance between 29 countries including the US, is a threat to Russian security (Kuczynski 2019). In 2016, president Vladimir Putin updated a national security strategy document from 2009 that complains about the expansion of NATO in Europe and the military operations close to Russian borders (Farchy 2016). RT and Sputnik News Agency, two Russian-state media organizations, have written many articles opposing NATO's military actions (Aleksejeva 2019) and arguing Russians dissatisfaction for NATO (RT 2018).

[30] In cases where there were multiple targeted countries in one FIE on a particular political issue we created the 3-letter code MUL, which is not assigned to any country in the ISO3 list.

goal **Discredit the White Helmets Syrian civil defense organization**:

The Syrian civil defense (SCD) group known as the White Helmets, was targeted over many years by a disinformation campaign (di Giovanni 2017). Russian trolls and bots linked to the Internet Research Agency (IRA) began creating content and amplifying disinformation against SCD in 2015, the year when Russia began its military intervention in Syria (Solon 2017). These operations aimed at discrediting the group by, for example, blaming the White Helmets for the chemical attack in Khan Sheikhoun, on April 4, 2017 (Chulov 2017, Jazeera 2017), and the nerve gas attack in Douma, on April 7, 2018 (BBC 2018*b*), among other cases.

In the Khan Sheikhoun gas attack, around 6,0000 Twitter accounts covering the attack were directly related to Kremlin. In some cases, the tweets called the chemical attacks a "false flag." One account, for example, posted "CW used by #AlQaeda not by #Assad #Khansheikun was falseflag of alqaeda linked fake aid organisation #whitehelmets" (Jindia et al. 2017). In other cases these accounts blamed SCD or other organizations with a low probability of working together (Bellingcat 2018). Bots also amplified the misinformation campaign against the White Helmets with almost 150 tweets per day (Solon 2017). The profiles suggest the accounts were tweeting independently from London, Berlin, Barcelona, Istanbul, New York, Chicago, Marseilles, and other places (Jindia et al. 2017).

The Twitter accounts, as well as Russian media, strategically raised the status and credibility of select journalists writing on the Syrian conflict. For example, Vanessa Beeley, who tweeted "White Helmets are not getting. We know they are terrorists. Makes them a legit target" and strongly criticized the UN report blaming the Syrian regime for the gas attack in Khan Sheikhoun, received coordinated re-tweets from a number of pro-Kremlin profiles (Jindia et al. 2017). Other people reportedly backed by these networks are Eva Bartlett, who claimed that the "White Helmets staged rescues using recycle victims" and Timothy Anderson, "who said the 2017 attack in Syria was a hoax" (Solon 2017).

This social media campaign was complemented by traditional propaganda. At least 22 articles written by between September and November accused the SCD of transporting chemical weapons in Idlib, a city in the same governorate as Khan Sheikhoun. Eight of the 22 were written by a pro-Kremlin organization called, Russian Centre for Reconciliation of Opposing Sides in Syria (RCROSS), the rest of them came directly from Sputnik, Russian-state media, and representatives of the Russian government (Solon 2017, Bellingcat 2018).

MULRUS0002. Targeted country **The United States**. Attacking country **Multiple**. Political goal **Discredit individuals raising awareness about Russian propaganda efforts**:

In several cases, individuals who drove important public awareness campaigns about Russian disinformation efforts were specifically targeted.

In September 2017, for example, American actor Morgan Freeman fronted a video warning that Russia had started an information war against the United States (Mele 2017, BBC 2017). In response, an account linked to the Internet Research Agency (IRA) called AgitPolk accused Freeman of "manipulating the facts of modern Russian history and openly slandering our country" on VKontakte, the Russian Facebook-equivalent, and amplified the attack using the hashtag #StopMorganLie on Twitter. The hashtag received 10,000 tweets, by Russian bots and accounts using profile pictures from a Soviet film. Russian-run RT News then ran a lengthy article claiming that "Twitterati" were "disappointed" with Freeman's comments, headlining the fact that the hashtag was getting a lot of attention on Facebook (Nimmo 2018*c*).

Finnish journalist Jessikka Aro was similarly targeted after her research on the location of IRA's headquarters was released in 2015 (Aro 2015). This campaign was highly responsive, with participating trolls posting immediately after Aro's appearance on TV or radio (Blanco 2019).[31]

In a broad study, the Associated Press found that at least 200 journalists have been targeted by Fancy Bear, a cyber espionage group associated with Russia (Satter et al. 2017) Approximately one quarter of those targeted worked at The New York Times and another quarter were correspondents in Moscow. The strategy aimed at stealing personal information and releasing it to the public, commonly known as "doxing". The remaining journalists worked on other countries and regions such as Ukraine Moldova and the Baltics (Satter et al. 2017). This hacked information was often spread using social media. Personal messages were stolen from Journalist Pavel Lobkov by Fancy Bear, for example, were spread to almost 300 Facebook pages (Satter et al. 2017).

NDLRUS0001. Targeted country **Netherlands**. Attacking country **Russia**. Political goal **Influence public opinion in 2017 Dutch parliamentary elections**:

Trolls working for the Russian Internet Research Agency (IRA) posted more than 200,000 tweets aimed at trying to influence political debate in the Netherlands (Kist & Wassens 2018). The trolls posted in Dutch with spelling and grammatical errors criticizing Islam, using hashtags such as "IslamKills". The trolls also supported the far-right politician Geert Wilders and called on Dutch voters to support the Party for Freedom (PVV, Partij voor de Vrijheid in Dutch) in the 2017 parliamentary elections (NWS 2018).

NDLRUS0002. Targeted country **Netherlands**. Attacking country **Russia**. Political goal **Undermine the trade agreement with Ukraine**:

The Netherlands held a referendum in April 2016 to approve a trade deal between the EU and Ukraine. Prior to the referendum Russian media outlets spread the false story that the Ukrainian military had shot down Flight MH17, which killed 193 Dutch citizens (Yong 2018). Online investigative group Bellingcat identified a range of similar content being promoted on other platforms. The YouTube channel called "Patriot" (in Ukrainian), for example, uploaded a video threatening the Netherlands entitled "Appeal of AZOV fighters to the Netherlands on a referendum about EU – Ukraine." The video depicted six soldiers, supposedly from the notorious far-right ultra-nationalist Azov Battalion, speaking in Ukrainian before burning a Dutch flag. A range of analysis suggests this video was initially spread and likely created by the network of accounts and news sites operated by the Internet Research Agency and the Federal News Agency (FAN) (Bellingcat 2016).

POLRUS0001. Targeted country **Poland**. Attacking country **Russia**. Political goal **Undermine the relationships between Poland and Ukraine**:

Shortly after the Maiden protests began in Kiev, a wave of anti-Ukrainian propaganda started to appear on the web in 2013 as noted by analysts from Poland (Savytskyi 2016).

[31] In 2018, two of the most aggressive and persistent trolls in the campaign, Ilja Janitskin and Johan Backman, were sentenced to 22 and 12 months, respectively, on 16 criminal courts (Higgins 2018).

The trolls consistently repeated the views of Russian authorities on places such as the internet forum of the Russian-Polish Radio Sputnik Polska. Their posts in autumn-2013 were primarily aimed at agreeing with and amplifying anti-Ukrainian stories (Savytskyi 2016).

SAIRN0001. Targeted country **Saudi Arabia**. Attacking country **Iran**. Political goal **Attack Saudi government**:

A number of websites and troll accounts that posted pro-Iranian articles and news clippings in Saudi Arabia were traced back to Iran (Nimmo 2018*a*). Foreign influencers "masquerading as domestic accounts" posted tens of thousands of times relating primarily to foreign and international relation problems, which indicates that trolls were attempting to politicize international relations as opposed to polarize solely domestic issues (Lake 2018). English posts were often written in clearly "non-native" English, and assaulted the Saudi state for its handling of relations with Iran. Attacks were also made prominent Saudis and Saudi state policy against terrorism from an Iranian perspective. Trolls were used to amplify many of these narratives (Boylan 2018).

Whereas Facebook and Twitter made efforts to remove more than 300 pages, many were still active after the announced removals (Prentis 2018).

Pro-Tehran articles were posted mixed in with content taken from established websites on a network of websites and social media pages that were all traced to Iran. One story posted on August 23rd, 2018 promoted a story that Saudi Arabia was "extending the ideology of terror with the support of the United Kingdom." Without mentioning its affiliation, this article quoted an interview that was conducted by Iranian state outlet PressTV. Another apparently original article reported that Saudi Arabia had been defeated in an assault on Hodeidah, Yemen on June 14, 2018 (Nimmo 2018*a*).

The two main websites which internet security firm FireEye identified as part of the effort were libertyfrontpress.com and InstitutoManquehue.org. Both of these websites were still functional as of August 22, 2018, and the output in English language seemed to be authentic. It was often written in non-native English, and focused on issues from the Iranian state point of view. 3 out of the top 4 posts concerned a profile of a Bahraini ayatollah, a hostile view of Saudi influence in Bahrain, and an interview which claimed that "Iran's democratic system is far more fair-minded to their voters than the American system" (Nimmo 2018*a*). The operation was also conducted on Twitter, where Iranian accounts posted 89,995 times about Saudi Arabia (Nimmo et al. 2018*b*).

SWERUS0001. Targeted country **Sweden**. Attacking country **Russia**. Political goal **Undermine the Swedish government**:

In 2018 Swedish officials stated they were seeing an increase in hacking and dissemination of fake news with the goal of undermining the stability of Swedish society (Brattberg & Maurer 2018). They highlighted misleading media reports that were being used to "frame NATO as an aggressor and military threat, the EU as in terminal decline, and Russia as under siege from hostile Western governments" (Brattberg & Maurer 2018). There is also evidence identifying "troll armies" targeting Swedish journalists and academics, hijacked Twitter accounts, and pro-Kremlin NGOs operating in Sweden (Henley 2017). According to the Swedish Security Service, Russian tactics ranged from online trolls and disinformation campaigns to efforts to demonize Swedish politicians and authorities

(Radio 2016).

TWNCHN0001. Targeted country **Taiwan**. Attacking country **China**. Political goal **Undermine Taiwanese government**:

Several bot and troll accounts linked to mainland China were discovered to be promoting information unfavorable to the Taiwanese government (Hsiao 2018, Corcoran et al. 2019). The campaign has touched on a number of domestic political issues in Taiwan, including the status of pension payments. Accounts promoting such content were traced to "bot farms" based in China. The activity appears designed to discredit the secessionist movement, which advocates formal separation from mainland China, and to encourage unity with the People's Republic of China. Specific operations have included exposing dissidents' activities, exacerbating political tensions and strife, and raising suspicions against leading military and political figures (Cole 2017).

UKRRUS0001. Targeted country **Ukraine**. Attacking country **Russia**. Political goal **Support the Annexation of Crimea to Russian Federation**:

After the fall of the Ukraine's pro-Russian president Viktor Yanukovych in 2014 and the annexation of Crimea by Russia, the GRU, the Russian military intelligence agency, embarked on a campaign creating fake accounts on Facebook and VKontakte – a Russian social media website (Peisakhin & Rozenas 2018). These accounts pretended to be pro-Russia Ukrainian citizens pushing anti-Ukrainian nationalist messages – for example by calling those in the Ukraine who were protesting Russian annexation of Crimea zapadentsy (westerners). Furthermore, the GRU bought ads and tried to enhance the popularity of its fake pro-Russia Ukrainian groups on Facebook (Summers 2017).

UKRRUS0002. Targeted country **Ukraine**. Attacking country **Russia**. Political goal **Reduce support for Donbass conflict**:

Since 2014, Russian information operations have supported the country's military activities in Ukraine. The operation included common propaganda aimed at discrediting the Ukrainian government—through, for example, claims that Ukraine is ruled by "successors of the Nazis" (Sazonov et al. 2016, EUvsDisinfo 2019)–alongside a campaign pretending to be organic from Ukraine, where Russian trolls used social media to blame Ukrainian government for the Donbass conflict (Andrusieczko 2019).[32]

Russian trolls also blamed Ukraine for shooting down Malaysia Airlines Flight 17 (MH17) on July 17, 2014. The airplane was attacked above territory held by Russian-backed separatists in eastern Ukraine, closed to the Donbass region. The Internet Research Agency (IRA) posted at least 65,000 tweets about MH17 one day after the crash and 111,486 posts from July 17 through 19. They use three hashtags: "Kiev shot Boeing", "Kiev Provocation" and "Kiev Tell the Truth". The tweets ended on July 19, after which the trolls continued to write about this topic, but with less frequency and without the hashtags (Knight 2019, van der Noordaa & van de Ven 2019).

UNKSAU0001. Targeted country **Unknown**. Attacking country **Saudi Arabia**. Political goal **Deny Saudi government responsibility for the murder of journalist Jamal Khashoggi**:

[32] For example, a group called the Russian Liberation Movement linked with a Russian "troll factory" produced a series of fake videos on YouTube about pro-Russian rebels in Ukraine and Russia (Soshnikov 2017).

Twitter banned a network of accounts attempting to sow doubt on Riyadh's involvement in the murder of Washington Post journalist Jamal Kahshoggi. These automated accounts promoted content countering evidence of Saudi Arabia's involvement (Elliot 2018, Collins & Wodinsky 2018). Many posted tweets in both Arabic and English with identical pro-Saudi hashtags (Barojan 2018*b*). This FIE has "unknown" as the targeted country because the campaign targeted populations around the world that speak English and/or Arabic.

USAIRN0001. Targeted country **The United States**. Attacking country **Iran**. Political goal **Polarize American politics**:

Iranian trolls worked to polarize American politics by creating and distributing divisive content on a range of topics on Facebook, Instagram, Twitter, and YouTube (Nimmo & Brookie 2018*b*, Guynn 2018*b*). The account @INeedJusticeNow, for example, which had 61,507 followers and around 13 million video views, focused on issues of police brutality. The account @nornowar, with almost half-million followers and likes, posted a range of content to drive people towards pro-Iranian propaganda designed to look like real news reporting (Wong & Hautala 2018). Other examples include Michelle Obama holding a sign saying "An Immigrant Took My Job" referring to Slovenia-born First Lady Melania Trump (Guynn 2018*b*), while another page created and amplified conspiracy theories related to the 9/11 terrorist attack with a video arguing that 9/11 was an "inside job" executed by the US Government (Bell 2018). One of the most viewed videos, around 1.5 million views, showed US soldiers laughing at Iraqi children (Nimmo et al. 2018*a*). Another group of 147 Facebook pages and 76 Instagram accounts related to Iranian state media engaged in hacking accounts and spreading malware (Guynn 2018*a*).

USAIRN0002. Targeted country **The United States**. Attacking country **Iran**. Political goal **Attack Donald Trump after 2016 US presidential elections**:

More than 600 accounts and groups were taken down by Facebook in 2018 for "coordinated inauthentic behavior that originated in Iran and targeted people in the US and UK." In the US, these accounts often posed as left-wing activists, attacking Republican politicians and praising Democratic ones (Nimmo & Brookie 2018*b*).

By comparison to the Russians, the Iranian hackers were unsophisticated and relatively inept at imitating Americans Sanger (2018). One ad showed a frowning Mr. Trump, and declared him "The Worst, Most Hated President in American History," and another showed two men shaking hands above a conference table and passing money below it and with text: "We call it bribery — they call it lobbying" (examples cited in Sanger 2018).

USAIRN0003. Targeted country **The United States**. Attacking country **Iran**. Political goal **Attack Republican Party after 2016 US presidential election**:

FireEye, a cyber-security firm, warned Facebook in July 2018 about "Liberty Front Press", a network of Facebook pages and Instagram accounts with Iranian origins (Intelligence 2018). On August 21 Facebook, drawing on the report, removed 652 users linked to Iranian state media, including accounts, groups and pages. The companies tracked the origin of the accounts using website registration information and IP addresses (Gleicher 2018*c*). "Quest 4 Truth", for example, was linked to Press TV, a news channel affiliated with Iranian media (Gleicher 2018*c*, Price 2018).

Nimmo & Brookie (2018*b*) analyzed the content of the Iranian accounts and found that posts mainly focused on attacking Donald Trump and the Republican Party. They often used distorted images or memes, such as President Trump hugging Kim Jong-un, Supreme Leader of North Korea, with a caption saying "The Nukebook".

Elements of this FIE were broadly similar to the Russia campaign against Hillary Clinton in the 2016 US Presidential ElectionsNimmo & Brookie (2018*b*). However, the Iranian network of fake websites and accounts reported by Lim et al. (2019) also aimed at amplifying geo-political tensions between the United States and countries in the Middle East.

USARUS0001. Targeted country **The United States**. Attacking country **Russia**. Political goal **Attack Hillary Clinton in the US 2016 presidential election**:

Russian tolls targeted the 2016 US presidential election by defaming Hillary Clinton and trying to persuade voters not to choose her. The campaign included three main tactics: stealing information, using bots to amplify stories, and deploying trolls to distort verifiable facts.

First, a team of 14 Russians indicted by a federal grand jury for interfering in the American election, hacked the email accounts of volunteers along with employees of the U.S presidential campaign of Hillary Clinton (the "Clinton Campaign"), including the email account of the Clinton Campaign's chairman. Mr. Prigozhin and his team, posing as Guccifer 2.0, contacted a U.S reporter with an offer to provide stolen emails from "Hillary Clinton's staff." They then sent the reporter the password to "access a nonpublic, password-protected portion of Dcleaks.com containing emails stolen from Hillary" in or around March 2016 (Muller 2018).

Second, Mr. Prigozhin also controlled the entity that financed the troll factory, known as the Internet Research Agency (IRA). This company created fictitious social-media personas, spreading falsehoods and promoting messages criticizing Hillary Clinton (Muller 2018). Troll factory tactics included applauding Donald Trump's candidacy while trying to undermine Hillary Clinton's (MacFarquhar 2018). Workers for the organization, a number of whom now face US criminal charges, allegedly placed Facebook and Twitter ads carrying fake or harshly critical news about Hillary Clinton. The impact of some of those ads was amplified via automated systems, known as "bots", whose activity reached millions of Americans (Gordon 2018).

USARUS0002. Targeted country **The United States**. Attacking country **Russia**. Political goal **Attack Democratic party in the 2016 and 2018 US elections**:

The Main Intelligence Directorate of the General Staff (GRU) engaged in a concerted long-term effort to damage the political prospects of Democratic Party candidates in two elections cycles. A key method in 21016 was releasing documents stolen through computer intrusions. A group of at least 13 Russians, including Yevgeny V. Prigozhin businessman with ties to President Vladimir Putin, was indicted for their efforts to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The attackers used the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page, to steal DCCC credentials and modify the DCCC website, redirecting visitors to the actblues.com domain. They stole approximately 2.5 gigabytes of data, including donor records and personal identifying information from more than

2,000 Democratic donors. This information was transferred to registered state lobbyists, as well as senior members of the Trump presidential campaign and online sources of political news (Muller 2018).

The campaign was complemented Russians accounts on social media trying to persuade voters to not choose the Democratic Party.[33] A Russian-created Twitter account, for example, tweeted in February 2018: "The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals and dead voters." Another account, tweeted instructions for Americans to donate money to defeat Democratic candidates such as Maxine Waters, Elizabeth Warren, and Nancy Pelosi. Russian trolls also defame Democrats with tweets, using the term "rapefugees", to associate democratic candidates with cases of sexual assault by migrants (Nimmo et al. 2018*c*).

USARUS0003. Targeted country **The United States**. Attacking country **Russia**. Political goal **Undermine Barack Obama's image**:

Russian trolls produced a large volume of tweets defaming President Obama and pushing negative hashtag on Twitter. They also wrote blog posts claiming that "life was good in Russia under Putin and it was bad in the US under Obama" (MacFarquhar 2018). As in other cases, these trolls were opportunistic and used bots to try and widely spread organic public expressions against Obama. For example, these accounts promoted on Twitter and Facebook the case of a fan at a University of Wisconsin football game who came dressed as then President Barack Obama with a noose around his neck (Stein 2018).

USARUS0004. Targeted country **United States**. Attacking country **Russia**. Political goal **Discredit American institutions**:

A coordinated campaign discredited the US Federal Bureau of Investigations (FBI) from 2017 onwards, especially its research on Russian influence operations, as part of a larger campaign to discredit American institutions (Linvill & Warren 2018). For example, Russian trolls promoted the effort to force the release of classified documents which allegedly show bias against President Donald Trump at the Justice Department by promoting the hashtag #releasethememo in early-2018 (e.g. by driving a thousandfold increase in the hashtag's prominence on January 19, 2018) (RFE 2018).

Russian trolls also tried to reduce the trust in US institutions using Twitter accounts related to Internet Research Agency (IRA) (Nimmo et al. 2018*a*). They specifically targeted African-Americans and Mexican-Americans in an apparent effort to reduce their respect for government institutions (Howard et al. 2018).

USARUS0005. Targeted country **The United States**. Attacking country **Russia**. Political goal **Support Donald Trump before and after the US 2016 presidential elections**:

Private firms in Russia, i.e. 'troll factories' were paid by the Russian government to spread pro-Trump propaganda on social media (Chen 2015*a*, Bertrand 2016). The trolls, for example, use Facebook to organize more than a dozen pro-Trump rallies in Florida during the 2016 election, which were then promoted online by local pro-Trump activists (Poulsen et al. 2017). A typical post by a Kremlin troll called "Bertha Malone", who had at least 400 posts on Facebook, said on this: "if only media had been as bothered

[33] See DiResta et al. (2018) for a detailed analysis of the specific content behind this campaign and other Russian ones targeting the US.

by Obama's ties to the Muslim Brotherhood as they are by Trump's fake ties to Russia" (Poulsen & Ackerman 2018*a*). Using data from Facebook, Google, Instagram, Twitter and Youtube between 2015 and 2016 Howard et al. (2018) concludes that the messages created by the IRA were primarily designed to benefit the Republican Party and then-candidate Donald Trump.

USARUS0006. Targeted country **The United States**. Attacking country **Russia**. Political goal **Attack Conservative critics of Donald Trump after 2016 US presidential elections**:

A hacking attack created websites to steal information from conservative groups critical of US President Donald Trump. The 'think tanks' attacked were former supporters of President Donald Trump, but now they were enemies who had called for more sanctions for Russia. Microsoft points out that these online sites were created by the group of hackers APT28, which has been publicly linked to a Russian intelligence agency and actively interfered in the 2016 presidential election, according to US researchers (Sanger & Frenkel 2018).

This campaign was complemented by online article attacking Conservative critics of Donald Trump. An article, for example, titled "Paul Ryan Opposes Trump's immigration Cuts, Wants Struggling American Workers to Stay Poor." Another article titled "Pro-Amnesty Sen. Marco Rubio: Trump's immigration Bill Will not Pass the Senate" (Holt 2017).

The Russian influence campaign pretended to be on both the left or the right. Enemies of Donald Trump – and Russia – were targeted by Project Lakhta, the broader Russian campaign to influence politics in the US and EU (Holt 2017).

USARUS0007. Targeted country **The United States**. Attacking country **Russia**. Political goal **Polarize American Politics**:

Russian trolls and bots promoted discord within the American political landscape over many years. Twitter discovered that nearly 600 Russian-linked troll accounts were promoting conservative, anti-Obama messages from 2014 to 2018 (Weixel 2018). Russian troll accounts also posted both pro-Affordable Care Act (ACA) and anti-ACA content in 2016. Scholars believe some of that activity was an effort to incite discord between Hillary Clinton and Bernie Sanders supporters in the 2016 Democratic primary election (Penzenstadler et al. 2018).

Russia-linked accounts also posted about police violence and brutality. Russian bots participated in rhetoric concerning the death of a young black man by police and the Black Lives Matter movement at large (Ackerman 2018, O'Sullivan et al. 2018). Russian accounts were linked with tweets concerning taking the knee during the National Anthem, immigration (of all varieties), gun control, and the NRA (Beaton & Simon 2018). Russian addresses were found to be pushing and creating Facebook pages on both sides of the immigration issue. Russian trolls also tried to incite physical protest, by tweeting that people "must take to the streets" if Trump fired Robert Mueller (Hern 2018, Penzenstadler et al. 2018). With regards to gun control, Russian bot accounts tweeted both for and against gun control (Mak 2018, Frenkel & Wakabayashi 2018). There is little consistency in ideology across these various efforts, leading many observed to conclude that a key Russian goal was to promote political discord and polarization.

Russian efforts also pushed on environmental issues. For example, Russian trolls exploited the hashtag #NoDAPL and targeted US energy policy from 2015 to 2017 through the use of Facebook, Twitter, and Instagram accounts controlled by the Internet Research Agency (Blacktivist 2016). An investigation by the Republican majority staff on the House Committee on Science, Space and Technology found more than 9,000 posts produced by 4,334 Russian accounts that dealt with climate and energy issues (Timberg & Romm 2018). In particular, for more than a week in October 2016, hundreds of accounts tweeted the #NoDAPL hashtag every six hours. #NoDAPL refers to the opposition movement against the Dakota Access Pipeline, which has long been a source of political division in the United States. The #NoDAPL tweets also played up racial and ethnic tensions associated with the pipeline (Hindman & Barash 2018).

USARUS0008. Targeted country **The United States**. Attacking country **Russia**. Political goal **Discredit US operations in Syria**:

After the April 2018 Douma chemical weapons attack in Syria, there was a campaign of Russian-administered social media activity by accounts claiming to be from the US (Nassetta & Fecht 2018). Analysts observed a large increase in the rate of Twitter accounts being opened immediately after the attack, many of which were found to be part of a Russian disinformation campaign against American participation in the Syrian conflict Nassetta & Fecht (2018). These accounts used pro-Assad rhetoric and blamed terrorists for attacks on the Syrian people (Nassetta & Fecht 2018). Russian news agencies such as Sputnik were also found to have reported fake stories about the United States backing Daesh (ISIS) soldiers in Syria in order to fight Assad (Nassetta & Fecht 2018). These stories were later confirmed to be false by Combined Joint Task Force - Operation Inherent Resolve (Barojan 2017).

USARUS0009. Targeted country **The United States**. Attacking country **Russia**. Political goal **Support Movement for the Independence in California and Texas**:

Russian trolls supported the "YesCalifornia" secessionist movement. The group, founded by Luis Marinelli and Marcus Evans, pushed a message of Californian independence. Marinelli previously lived in Russia and opened an 'embassy' for his movement there with funding from a Russian NGO (Friedersdorf 2017). Hours after the 2016 presidential elections, the #calexit movement was mentioned over 100,000 times by Russian bots (Wendling 2017). Russian bots and trolls also supported the Texas secession movement through the Heart of Texas Facebook page created by the Internet Research Agency (IRA). This page supported the secession of Texas from the US by pushing an event called "Get Ready to Secede" and by using anti-Muslim and anti-Hillary Clinton rhetoric to persuade its audience (Gomez 2017).

USARUS0010. Targeted country **The United States**. Attacking country **Russia**. Political goal **Support Donald Trump's judicial nominees**:

Russian bots and trolls on Twitter distorted evidence against then Supreme Court nominee Brett Kavanaugh in the case of sexual harassment claims by three women. The state-funded news outlet RT highlighted White House claims that there was insufficient proof of sexual misconduct by the judge (Maza 2018).

USARUS0011. Targeted country **The United States**. Attacking country **Russia**. Political goal **Support Republican candidate to US Senate, Roy Moore**:

In the 2017 Alabama special election for a US Senate seat, Kremlin-linked news sites and trolls supported Roy Moore, the Republican candidate accused of sexual misconduct against multiple women (Clifton 2017). More than 20,000 to 25,000 tweets were sent out every single day using the hashtag #alabamasenaterace from approximately 600 twitter accounts. These accounts were being monitored by the cyber security research project Hamilton 68. It was reported that "Among pro-Moore articles, close to 70% attacked the credibility of the accuser(s), 38% attacked the media, the Washington Post in particular, and one story attacked Lindsey Graham for not defending Moore" (Schafer 2017). Not all the support that Moore received on the Internet cames from Russia. The New York Times reported that a group of "Democratic tech experts" used Russian-style disinformation tactics during Alabama's 2017 special election in an attempt to splinter support for Moore (Shane & Blinder 2018). The Washington Post also reported that Facebook has suspended accounts used by five people involved in the project (Romm & Timberg 2018). Although the tactics are similar to those used by Russian trolls, they were not part of this FIE.

USARUS0012. Targeted country **The United States**. Attacking country **Russia**. Political goal **Support Alt-right movements after the US 2016 presidential election**:

Russian trolls worked for a number of years to polarize American politics by pushing both complaints by actors on both the political right and the political left in the social media. However, these accounts re-tweeted voices in the American "alt-right" — significantly more than their left-wing rivals (Nimmo & Karan 2018). This activity looks to have had a distinct political goal from the broader polarization effort and is therefore coded as a distinct campaign.

USARUS0013. Targeted country **The United States**. Attacking country **Russia**. Political goal **Spread false reports of Chemical explosion in Louisiana, Ebola outbreak and police shooting in Atlanta**:

According to a report in The New York Times Magazine, in 2014 Russian trolls from the IRA spread false reports about a chemical explosion at the Columbian Chemicals plant in Centerville, Louisiana. The FIE used "YouTube videos of fake CNN tweet[ed] directed at local journalists" and "text alerts sent to nearby residents" according to Szal (2015). The source field on Twitter showed that the tweets sent about #ColumbianChemicals were posted using a tool called Mass Post, which is associated with a nonworking page on the domain Add1.ru (Szal 2015, Chen 2015*b*). False reports such as a police shooting in Atlanta and an outbreak of Ebola were also spread using similar approaches in 2015 (Szal 2015).

USAUNK0001. Targeted country **The United States**. Attacking country **Unknown**. Political goal **Attack Hillary Clinton 2016 in the US Presidential election**:

The campaign to target then-candidate Hillary Clinton involved substantial activity from contractors funded by an unknown country. Veles, a small town in Macedonia, hosted at least 100 websites creating fake stories against Hillary Clinton (Subramanian 2017). For example, a story titled "Hillary Clinton In 2013: 'I Would Like To See People Like Donald Trump Run For Office; They're Honest And Can't Be Bought."' was written by ConservativeState.com. The post received 480,000 shares, reactions, and comments on Facebook. This number of shares is high relative to some New York Time's posts about the US presidential elections, which receive around 175,000 shares in the same social network (Silverman & Lawrence 2016). There is some evidence suggesting that one group of the Macedonian trolls received orders from Internet Research Agency and they were allegedly financed by Ben Goldman and Paris Wade, the co-founders of the US conservative site Liberty Writers News (Silverman et al. 2018). In aggregate, however, it is not clear whether the operation was initiated by Macedonians seeking to produce clickbait to drive ad revenues, Russians seeking to advance Clinton's electoral prospects, or American campaign operatives.

USAUNK0002. Targeted country **The United States**. Attacking country **Unknown**. Political goal **Support Donald Trump in 2016 US presidential elections**:

The Guardian identified more than 150 domains registered in Veles, Macedonia, that published political news about the United States. Headlines included "Hillary's Illegal Email Just Killed Its First American Spy", "This is How Liberals Destroyed America", and "This Is Why We Need Trump in the White House" Petreski & Kanishk (2019). Articles on the website appeared to use sensationalist headlines to obtain traffic, similar to clickbait. The websites received some engagement on social media platforms Twitter and Facebook, but most traffic to the website was direct (Petreski & Kanishk 2019, Subramanian 2017). It is unclear from reporting whether these sites were paid for by foreign actors or were intended to generate ad revenue by drawing traffic from politically interested users.

USAUNK0003. Targeted country **The United States**. Attacking country **Unknown**. Political goal **Distribute conspiracy theories about religion and immigration in American Midterms elections**:

Websites administered from Macedonia were active in purveying a range of low-reliability political content before and during the 2018 US midterm election, albeit less so than in 2016 (Petreski & Kanishk 2019). These sites included: usapatriotsvoice.com which contained race and ethnicity-based content; and wuc-news.com, which posted conspiracy theories and anti-immigration. content (Petreski & Kanishk 2019). It is unclear from reporting whether these sites were paid for by foreign actors or were intended to generate ad revenue by drawing traffic from politically interested users.

YEMIRN0001.Targeted country **Yemen**. Attacking country **Iran**. Political goal **Reduce support for Saudi Arabian government in Yemen**:

News outlets pretending to come from Yemen, but with address and fax numbers in Iran, posted content critical of Saudi actions in Yemen (Kanishk et al. 2019). Reuters found a number of Iranian-run sites targeting Yemen, e.g. the self-styled, misspelled "Yemen Press Agecny" which claimed to have a running update of Saudi "crimes against Yemenis during the past 24 hours," as well as sites targeting Egypt and Sudan (Stubbs & Bing 2018).

ZAFRUS0001. Targeted country **South Africa**. Attacking country **Russia**. Political goal **Polarize South African politics**:

The Rhodes Must Fall and Fees Must Fall Movements in South Africa resemble The Black Lives Matter movement in America. Russian operatives engaged both movements in a minor way. Of the 3 million tweets written by Russian trolls identified by Twitter in 2018, there were some tweets consisted of info-graphics that misrepresented land or race facts in

South Africa (Linvill & Warren 2018). The accounts also spread a white genocide meme, with the intent to polarize opinions over race (Superlinear 2018). Yevgeny Prigozhin has reportedly opened technology centers in Central Africa, where his team will research and send out social media messages about the upcoming elections to try and make people vote for Pro-Russian relations in Africa (Pertsev 2018).

C References

Acemoglu, D. & Autor, D. (2011), 'Skills, tasks and technologies: Implications for employment and earnings', *Handbook of labor economics* **4**, 1043–1171.

Aceves, W. (2019), 'Virtual hatred: How russia tried to start a race war in the united states', *Michigan Journal of Race & Law* **24**(1).

Ackerman, S. (2018), 'Russia is exploiting american white supremacy over and over again'.
URL: `https://www.thedailybeast.com/how-russia-exploits-american-white-supremacy-over-and-over-again?ref=author`

Aleksejeva, N. (2019), 'Balticbrief: Sputnik takes aim at a russian-speaking audience'.
URL: `https://medium.com/dfrlab/balticbrief-sputnik-takes-aim-at-a-russian-speaking-audience-6f7668e6cc23`

Allcott, H., Gentzkow, M. & Yu, C. (2019), Trends in the diffusion of misinformation on social media, Technical report, National Bureau of Economic Research.

Andrusieczko, P. (2019), 'Ukraine in the sights of russian trolls and propagandists - soon presidential and then parliamentary elections'.
URL: `http://wyborcza.pl/7,75399,24353939,ukraina-na-celowniku-rosyjskich-trolli-i-propagandzistow-wkrotce.html?disableRedirects=true`

Aro, J. (2015), 'Yle kioski traces the origins of russian social media propaganda – never-before-seen material from the troll factory'.

Auchard, E. & Felix, B. (2017), 'French candidate macron claims massive hack as emails leaked'.
URL: `https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ`

Auchard, E. & Menn, J. (2017), 'Facebook cracks down on 30,000 fake accounts in france'.
URL: `https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G`

Ball, J. (2017), 'A suspected network of 13,000 twitter bots pumped out pro-brexit messages in the run-up to the eu vote'.
URL: `https://www.buzzfeed.com/jamesball/a-suspected-network-of-13000-twitter-bots-pumped-out-pro`

Baroja, D. (2018), 'Troll tracker: Pro-kremlin trolls deployed ahead of syria strikes'.
URL: `https://medium.com/dfrlab/trolltracker-pro-kremlin-trolls-deployed-ahead-of-syria-strikes-e49acc68c8ff`

Barojan, D. (2017), 'Questionable sources on syria. how kremlin-backed and fringe media spread a false story claiming the u.s.-led coalition evacuated isis from the front lines'.
URL: `https://medium.com/dfrlab/questionable-sources-on-syria-36fcabddc950`

Barojan, D. (2018*a*), 'Balticbrief: Nato not planning to invade belarus'.
URL: https://medium.com/dfrlab/balticbrief-nato-not-planning-to-invade-belarus-d694d34f04ba

Barojan, D. (2018*b*), 'Syriahoax part two: Kremlin targets white helmets'.
URL: https://medium.com/dfrlab/syriahoax-part-two-kremlin-targets-white-helmets-c6ab692d4a21

BBC (2017), 'Russia turns on morgan freeman over election 'war' video'.
URL: https://www.bbc.com/news/world-europe-41348749

BBC (2018*a*), 'Jessikka aro: Finn jailed over pro-russia hate campaign against journalist'.
URL: https://www.bbc.com/news/world-europe-45902496

BBC (2018*b*), 'Syria war: What we know about douma 'chemical attack''.
URL: https://www.bbc.com/news/world-middle-east-43697084

Beaton, A. & Simon, S. (2018), 'Russian trolls tried to influence debate over nfl players kneeling during anthem'.
URL: https://www.npr.org/2018/10/27/661313336/russian-trolls-tried-to-influence-debate-over-nfl-players-kneeling-during-anthem

Bell, C. (2018), 'The people who think 9/11 may have been an 'inside job'.
URL: https://www.bbc.com/news/blogs-trending-42195513

Bellingcat (2016), 'Behind the dutch terror threat video: The st. petersburg "troll factory" connection'.
URL: https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video/

Bellingcat (2018), 'Chemical weapons and absurdity: The disinformation campaign against the white helmets'.
URL: https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets/

Belsat (2018), 'Top 5 fake stories about belarus spread by russian media'.
URL: https://belsat.eu/en/news/top-5-fake-stories-about-belarus-spread-by-russian-media/

Benavente, J. M., Bravo, D. & Montero, R. (2011), 'Wages and workplace computer use in chile', *The Developing Economies* **49**(4), 382–403.

Benevides, B. (2018), 'Russian hackers are trying to interfere in brazilian elections, cybersecurity firm says'.
URL: https://www1.folha.uol.com.br/internacional/en/world/2018/10/russian-hackers-are-trying-to-interfere-in-brazilian-elections-cybersecurity-firm-says.shtml

Bertrand, N. (2016), 'It looks like russia hired internet trolls to pose as pro-trump americans'.
URL: https://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7

Black, P. (2018), ‘Shocking anakonda 2018 exercise’s scenario’.
URL: `https://medium.com/@paulblackjournalist/shocking-anakonda-2018-exercises-scenario-b8e58c1399ee`

Blacktivist (2016), ‘Republican investigation links russian trolls to nodapl movement’.
URL: `https://www.indianz.com/News/2018/03/01/republican-investigation-links-russian-t.asp`

Blanco, P. (2019), ‘Así arruinaron los ‘trolls’ rusos la vida de jessikka aro’.
URL: `https://elpais.com/internacional/2017/12/07/actualidad/1512655209-165226`

Blank, S. (2013), ‘Russian information warfare as domestic counterinsurgency’, *American Foreign Policy Interests* **35**(1), 31–44.

Bogle, A. (2019), ‘Twitter cracking down on political posts ahead of australian election’.
URL: `https://www.abc.net.au/radio/programs/am/twitter-cracks-down-on-political-posts-ahead-of-election/10828096`

Boulianne, S. (2015), ‘Social media use and participation: A meta-analysis of current research’, *Information, communication & society* **18**(5), 524–538.

Boylan, D. (2018), ‘Fake news: Iranian propaganda reports of death of saudi crown prince spark conspiracy theories’.
URL: `https://www.washingtontimes.com/news/2018/may/29/iran-propaganda-reports-mohammed-bin-salman-death-/`

Bradshaw, S. & Howard, P. N. (2018), ‘Challenging truth and trust: A global inventory of organized social media manipulation’, *The Computational Propaganda Project* .

Brattberg, E. & Maurer, T. (2018), ‘How sweden is preparing for russia to hack its election’.
URL: `https://www.bbc.com/news/world-44070469`

Brattnerg, E. & Maurer, T. (2018), ‘Russian election interference: Europe’s counter to fake news and cyber attacks’.
URL: `https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435`

Brewster, T. (2017), ‘Did russia hack macron? the evidence is far from conclusive’.
URL: `https://www.forbes.com/sites/thomasbrewster/2017/05/08/macron-emails-leaked-and-russia-is-the-chief-suspect/#6ec43ef168f4`

Burgess, M. (2017), ‘Here’s the first evidence russia used twitter to influence brexit’.
URL: `https://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency`

Chen, A. (2015*a*), ‘The agency’.
URL: `https://www.nytimes.com/2015/06/07/magazine/the-agency.html`

Chen, A. (2015*b*), ‘The agency’.
URL: `https://www.nytimes.com/2015/06/07/magazine/the-agency.html?`

Chigona, W., Beukes, D., Vally, J. & Tanner, M. (2009), ‘Can mobile internet help alleviate social exclusion in developing countries?’, *The Electronic Journal of Information Systems in Developing Countries* **36**(1), 1–16.

Chulov, M. (2017), ‘Sarin used in april syria attack, chemical weapons watchdog confirms’.
URL: `https://www.theguardian.com/world/2017/jun/30/sarin-was-used-in-syria-khan-sheikhun-attack-says-chemical-weapons-watchdog`

Clifton, D. (2017), ‘Russian propagandists are pushing for roy moore to win’.
URL: `https://www.motherjones.com/politics/2017/12/russian-propagandists-are-pushing-for-roy-moore-to-win/`

Cole, M. J. (2017), ‘Banking on structural weaknesses in today’s media, beijing has succeeded in broadcasting a false narrative about taiwan, often on a global scale’.
URL: `https://sentinel.tw/china-disinformation-tw/`

Collins, B. & Wodinsky, S. (2018), ‘Twitter pulls down bot network that pushed pro-saudi talking points about disappeared journalist’.
URL: `https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871`

Corcoran, C., Crowley, B. J. & Davis, R. (2019), Disinformation threat watch. the disinformation landscape in east asia and implications for us policy, Technical report.

Dave, P. & Bing, C. (2018), ‘Facebook, twitter dismantle disinformation campaigns tied to iran and russia’.
URL: `https://www.reuters.com/article/us-facebook-russia-usa/facebook-twitter-remove-pages-promoting-iranian-propaganda-idUSKCN1L62FD`

di Giovanni, J. (2017), ‘Why assad and russia target the white helmets’.
URL: `https://www.nybooks.com/daily/2018/10/16/why-assad-and-russia-target-the-white-helmets/`

Di Stefano, M. (2018), ‘Here’s the woman behind britain’s most divisive twitter account’.
URL: `https://www.buzzfeed.com/markdistefano/heres-the-woman-behind-britains-most-divisive-twitter`

Dick, S. (2018), ‘Fake pro-independence facebook page that originated in iran is taken down’.
URL: `https://www.heraldscotland.com/news/16592877.fake-pro-independence-facebook-page-that-originated-in-iran-is-taken-down/`

DiResta, R., Shaffer, D., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, D. & Johnson, B. (2018), ‘The tactics & tropes of the internet research agency’.
URL: `https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf`

Eady, G., Nagler, J., Guess, A., Zilinsky, J. & Tucker, J. A. (2019), ‘How many people live in political bubbles on social media? evidence from linked survey and twitter data’, *SAGE Open* **9**(1).

Elliot, H. (2018), ‘Twitter reportedly suspends network of bots pushing pro-saudi disinformation on suspected khashoggi murder’.
URL: `https://slate.com/news-and-politics/2018/10/twitter-reportedly-suspends-network-of-bots-pushing-pro-saudi-disinformation-on-suspected-khashoggi-murder.html`

Emmott, R. (2017), ‘Spain sees russian interference in catalonia separatist vote’.
URL: `https://www.reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalonia-separatist-vote-idUSKBN1DD20Y`

Enli, G. (2017), ‘Twitter as arena for the authentic outsider: exploring the social media campaigns of trump and clinton in the 2016 us presidential election’, *European journal of communication* **32**(1), 50–61.

EUvsDisinfo (2019), ‘Results of 2018 “eu versus disinformation” screening: Ukraine remains under fire through disinformation’.
URL: `https://www.euneighbours.eu/en/east/stay-informed/news/results-2018-eu-versus-disinformation-screening-ukraine-remains-under-fire`

Farchy, J. (2016), ‘Putin names nato among threats in new russian security strategy’.
URL: `https://www.ft.com/content/6e8e787e-b15f-11e5-b147-e5e5bba42e51`

Field, M. & Wright, M. (2018), ‘Russian trolls sent thousands of pro-leave messages on day of brexit referendum, twitter data reveals’.
URL: `https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/`

Foley, P. (2004), ‘Does the internet help to overcome social exclusion’, *Electronic Journal of e-government* **2**(2), 139–146.

Frenkel, S. & Wakabayashi, D. (2018), ‘After florida school shooting, russian ‘bot’ army pounced’.
URL: `https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html`

Friedersdorf, C. (2017), ‘Is russia behind a secession effort in california?’.
URL: `https://www.theatlantic.com/politics/archive/2017/03/is-russia-behind-a-secession-effort-in-california/517890/`

Fubini, F. (2018), ‘Tweet populisti dalla russia sulla politica italiana. come negli usa’.
URL: `https://www.corriere.it/politica/18_agosto_01/tweet-populisti-russia-voto-italiano-come-usa-f33df26c-95cc-11e8-819d-89f988769835.shtml?refresh_ce-cp`

Gleicher, N. (2018*a*), ‘Coordinated inauthentic behavior explained’.
URL: `https://newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/`

Gleicher, N. (2018*b*), ‘More information about last week’s takedowns’.
URL: `https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/`

Gleicher, N. (2018*c*), 'What we've found so far'.
URL: `https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/`

Goble, P. (2019), 'Belarus already under russian troll attack designed to give moscow a base for further aggression'.
URL: `http://euromaidanpress.com/2019/01/02/belarus-already-under-russian-troll-attack-designed-to-give-moscow-a-base-for-further-aggression/`

Gomez, L. (2017), 'A russian twitter bot promoted california secession, or calexit'.
URL: `https://www.sandiegouniontribune.com/opinion/the-conversation/sd-russian-bot-pushed-calexit-movement-20171102-htmlstory.html`

Gordon, G. (2018), 'Fake, misleading social media posts exploding globally, oxford study finds'.
URL: `https://www.mcclatchydc.com/news/nation-world/national/national-security/article215188910.html`

Griffin, A. (2015), 'Angela merkel's instagram bombarded with abuse from russian troll army'.
URL: `https://www.independent.co.uk/life-style/gadgets-and-tech/news/angela-merkels-instagram-bombarded-with-abuse-from-russian-troll-army-10303425.html`

Guynn, J. (2018*a*), 'Facebook foils political influence campaigns originating in iran, russia ahead of u.s. midterms'.
URL: `https://www.usatoday.com/story/tech/2018/08/21/facebook-foils-political-influence-campaigns-originating-iran-russia-ahead-u-s-midterms/1058233002/`

Guynn, J. (2018*b*), 'These are the liberal memes iran used to target americans on facebook'.
URL: `https://www.usatoday.com/story/tech/news/2018/08/24/how-iran-targeted-u-s-facebook-youtube-and-twitter-liberal-memes/1079882002/`

Hanson, F., O'Connor, S., Walker, M. & Courtois, L. (2017), Hacking democracies: Cataloguing cyber-enabled attacks on elections, Technical report, The Australian Strategic Policy Institute.
URL: `https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Hacking%20democracies.pdf`

Henley, J. (2017), 'Russia waging information war against sweden, study finds'.
URL: `https://www.theguardian.com/world/2017/jan/11/russia-waging-information-war-in-sweden-study-finds`

Hern, A. (2017), 'How a russian troll soldier stirred anger after the westminster attack'.
URL: `https://www.theguardian.com/uk-news/2017/nov/14/how-a-russian-troll-soldier-stirred-anger-after-the-westminster-attack`

Hern, A. (2018), 'Vast archive of tweets reveals work of trolls backed by russia and iran'.
URL: `https://www.theguardian.com/technology/2018/oct/17/vast-archive-of-tweets-reveals-work-of-trolls-backed-by-russia-and-iran`

Higgins, A. (2018), 'Three internet trolls convicted of systematic defamation against journalist in finland'.
URL: `https://www.nytimes.com/2018/10/19/world/europe/finland-internet-trolls-defamation.html`

Hindman, M. & Barash, V. (2018), 'Disinformation, 'fake news' and influence campaigns on twitter'.

Hjelmgaard, K. (2017), 'There is meddling in germany's election — not by russia, but by u.s. right wing'.
URL: `https://www.usatoday.com/story/news/world/2017/09/20/meddling-germany-election-not-russia-but-u-s-right-wing/676142001/`

Holt, D. (2017), 'Criminal complaint'.
URL: `https://assets.documentcloud.org/documents/5011321/Khusyaynova-Complaint.pdf`

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J. & François, C. (2018), *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, University of Oxford.

Hsiao, R. (2018), 'Ccp propaganda against taiwan enters the social age'.
URL: `https://jamestown.org/program/ccp-propaganda-against-taiwan-enters-the-social-age/`

Intelligence, F. (2018), 'Suspected iranian influence operation leverages network of inauthentic news sites and social media targeting audiences in u.s., uk, latin america, middle east'.
URL: `https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html`

Jazeera, A. (2017), 'Syria forces behind khan sheikhoun gas attack: Un probe'.
URL: `https://www.aljazeera.com/news/2017/09/syria-forces-khan-sheikhoun-gas-attack-probe-170906115601017.html`

Jindia, S., Graphika & TSC (2017), Killing the truth: How russia is fuelling a disinformation campaign to cover up war crimes in syria, Technical report, The Syria Campaign.

Kanishk, K., Barojan, D., Hall, M. & Brookie, G. (2019), 'Trolltracker: Outward influence operation from iran'.
URL: `https://medium.com/dfrlab/trolltracker-outward-influence-operation-from-iran-cc4539684c8d`

Karp, P. (2018), 'Russian twitter trolls stoking anti-islamic sentiment in australia, experts warn'.
URL: `https://www.theguardian.com/australia-news/2018/nov/20/russian-twitter-trolls-stoking-anti-islamic-sentiment-in-australia-experts-warn`

Keeley, G. (2018), 'Russia meddled in catalonia independence referendum, says german intelligence boss'.
URL: `https://www.thetimes.co.uk/article/russia-meddled-in-catalonia-vote-p6g5nttpm`

King, G., Pan, J. & Roberts, M. E. (2017), 'How the chinese government fabricates social media posts for strategic distraction, not engaged argument', *American Political Science Review* **111**(3), 484–501.

Kist, R. (2018), 'The fight against the trolls hardens'.
URL: `https://www.nrc.nl/nieuws/2018/10/29/de-strijd-tegen-de-trollen-verhardt-a2753190`

Kist, R. & Wassens, R. (2018), 'Russian troll army also active in the netherlands'.
URL: `https://www.nrc.nl/nieuws/2018/07/15/de-russische-trollen-zijn-anti-islam-en-voor-wilders-a1610155`

Knight, A. (2019), 'Russia deployed its trolls to cover up the murder of 298 people on mh17'.
URL: `https://www.thedailybeast.com/mh17-russia-deployed-its-trolls-to-cover-up-the-murder-of-298-people?ref=home`

Kroet, C. (2017), 'Russian fake news campaign targets merkel in german election'.
URL: `https://www.politico.eu/article/russian-fake-news-campaign-targets-merkel-in-german-election/`

Kronitis, R. (2018), 'Shocking anakonda 2018 exercise's scenario, the fourth stage (creation of a buffer zone)'.
URL: `https://9gag.com/u/rudiskronitis`

Krueger, A. B. (1993), 'How computers have changed the wage structure: Evidence from microdata', *The Quarterly Journal of Economics* **108**(1), 33–60.

Kuczynski, G. (2019), Nato-russia relations: The return of the enemy, Technical report.

Lake, E. (2018), 'Iran's fake news is a fake threat'.
URL: `https://www.bloomberg.com/opinion/articles/2018-08-31/iran-s-fake-news-is-not-a-real-threat`

Lim, G., Maynier, E., Scott-Railton, J., Fittarelli, A., Moran, N. & Deibert, R. (2019), Burned after reading: Endless mayfly's ephemeral disinformation campaign, Technical report, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto.

Linthicum, K. (2018), 'Mexico has its own fake news crisis. these journalists are fighting back'.
URL: `https://www.latimes.com/world/la-fg-mexico-fake-news-20180415-story.html`

Linvill, D. L. & Warren, P. L. (2018), 'Troll factories: The internet research agency and state-sponsored agenda building'.

Love, J., Menn, J. & Ingram, D. (2018), 'In mexico, fake news creators up their game ahead of election'.
URL: `https://www.reuters.com/article/us-mexico-facebook/in-mexico-fake-news-creators-up-their-game-ahead-of-election-idUSKBN1JO2VG`

MacFarquhar, N. (2018), 'Inside the russian troll factory: Zombies and a breakneck pace'.
URL: `https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html`

Mak, T. (2018), 'Russia's divisive twitter campaign took a rare consistent stance: Pro-gun'.
URL: `https://www.npr.org/2018/09/21/648803459/russias-2016-twitter-campaign-was-strongly-pro-gun-with-echoes-of-the-nra`

Martin, D. A. (2018), 'U-shaped wage curve and the internet: The colombian case', *Estudios de Economía* **45**(2), 173–202.

Mason, M. (2018), 'Intelligence officials plan to repel fake news in australian federal election'.
URL: `https://www.afr.com/business/media-and-marketing/advertising/intelligence-officials-plan-to-repel-fake-news-in-australian-federal-election-20180907-h151y2`

Maza, C. (2018), 'Brett kavanaugh has huge opposition in the u.s.—but russian state propaganda loves donald trump's nominee'.
URL: `https://www.newsweek.com/brett-kavanaugh-has-huge-opposition-us-russian-state-propaganda-loves-donald-1155046`

Mele, C. (2017), 'Morgan freeman angers russians over video about 2016 election'.
URL: `https://www.nytimes.com/2017/09/22/world/europe/morgan-freeman-russia-video.html`

Melendez, S. (2018), 'To see the future of social media manipulation in politics, look to mexico'.
URL: `https://www.fastcompany.com/40531308/to-see-the-future-of-social-media-manipulation-in-politics-look-to-mexico`

Michel, C. (2018), 'It turns out russia is not the only country turning facebook and twitter against us'.
URL: `https://www.washingtonpost.com/news/democracy-post/wp/2018/08/23/it-turns-out-russia-isnt-the-only-country-turning-facebook-and-twitter-against-us/`

Michel, R. & Dyomkin, D. (2017), 'After talks, france's macron hits out at russian media, putin denies hacking'.
URL: `https://www.reuters.com/article/us-france-russia-idUSKBN18P030`

Mohan, M. (2017), 'Macron leaks: the anatomy of a hack'.
URL: `https://www.bbc.com/news/blogs-trending-39845105`

Mueller, R. S. (2019), 'Report on the investigation into russian interference in the 2016 presidential election', *U.S. Department of Justice* pp. p. 4 – 8, p. 14 – 35.

Muller, R. (2018), 'Conspiracy to commit an offense against the united states'.
URL: `https://www.justice.gov/storage/report.pdf`

Narayanan, V., Barash, V., Kelly, J., Kollanyi, B., Neudert, L.-M. & Howard, P. N. (2018), 'Polarization, partisanship and junk news consumption over social media in the us', *The Computational Propaganda Research Project* .

Nassetta, J. & Fecht, E. (2018), All the world is staged: An analysis of social media influence operations against us counterproliferation efforts in syria, Technical report, Middlebury Institute of International Studies at Monterey.
URL: `https://www.nonproliferation.org/wp-content/uploads/2018/09/op37-all-the-world-is-staged.pdf`

Neuman, S. (2018), 'Russia's 'fancy bear' reportedly hacks german government network'.
URL: `https://www.npr.org/sections/thetwo-way/2018/03/01/589787931/russias-fancy-bear-reportedly-hacks-german-government-networks`

News (2018), 'Russian 'troll factory' tweets tried to influence italian voters'.
URL: `https://www.thelocal.it/20180802/russian-troll-factory-tweets-attempted-influence-italian-elections`

NewsWhip (2018), 'Navigating the facebook algorithm change: 2018 report.'.
URL: `http://go.newswhip.com/rs/647-QQK-704/images/FacebookAlgorithmMarch18.pdf`

Nimmo, B. (2017), 'Russian narratives on nato's deployment. how russian-language media in poland and the baltic states portray nato's reinforcements'.
URL: `https://medium.com/dfrlab/russian-narratives-on-natos-deployment-616e19c3d194`

Nimmo, B. (2018*a*), 'Iran is suspected information operation. assessing the main pages and accounts traced to tehran by fireeye'.
URL: `https://medium.com/dfrlab/trolltracker-irans-suspected-information-operation-153fc7b60126`

Nimmo, B. (2018*b*), 'Putinatwar: Trolls on twitter'.
URL: `https://medium.com/dfrlab/putinatwar-trolls-on-twitter-5d0bb3dc30ae`

Nimmo, B. (2018*c*), 'Russia is full spectrum propaganda'.
URL: `https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970`

Nimmo, B. (2018*d*), 'Trolltracker: An iranian messaging laundromat'.
URL: `https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193`

Nimmo, B. & Brookie, G. (2018*a*), 'Trolltracker: Criminal complaint filed against russian troll farm'.
URL: `https://medium.com/dfrlab/trolltracker-criminal-complaint-filed-against-russian-troll-farm-5b751953de06`

Nimmo, B. & Brookie, G. (2018*b*), 'Trolltracker: Facebook uncovers iranian influence operation iranian narratives buried in divisive content target united states and united kingdom'.
URL: `https://medium.com/dfrlab/trolltracker-facebook-uncovers-iranian-influence-operation-d21c73cd71be`

Nimmo, B., Brookie, G. & Karan, K. (2018*a*), 'Trolltracker: Twitter troll farm archives. part one — seven key take aways from a comprehensive archive of known russian and iranian troll operations'.
URL: `https://medium.com/dfrlab/trolltracker-twitter-troll-farm-archives-8d5dd61c486b`

Nimmo, B., Brookie, G. & Karan, K. (2018*b*), 'Trolltracker: Twitter troll farm archives part three — assessing an covert iranian social media influence campaign'.
URL: `https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-17a6d5f13635`

Nimmo, B., Brookie, G. & Karan, K. (2018*c*), 'Trolltracker: Twitter troll farm archives. part two — how the internet research agency regenerated on twitter after its accounts were suspended'.
URL: `https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-8be6dd793eb2`

Nimmo, B. & Francois, C. (2018), 'Trolltracker: Glimpse into a french operation'.
URL: `https://medium.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924`

Nimmo, B. & Karan, K. (2018), 'Trolltracker: Favorite russian troll farm sources. measuring the websites and accounts the internet research agency shared most'.
URL: `https://medium.com/dfrlab/trolltracker-favorite-russian-troll-farm-sources-48dc00cdeff`

NWS (2018), 'Russian trolls active in belgium and the netherlands'.
URL: `https://www.vrt.be/vrtnws/en/2018/07/16/russian-trolls-active-in-belgium-and-the-netherlands/`

Oltermann, P. (2017), 'Conservative sebastian kurz on track to become austria's next leader'.
URL: `https://www.theguardian.com/world/2017/oct/15/sebastian-kurz-on-track-to-become-austrias-next-leader-projections-show`

O'Sullivan, D., Guff, S., Quinones, J. & Dawson, M. (2018), 'Her son was killed — then came the russian trolls'.
URL: `https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/`

Ott, B. L. (2017), 'The age of twitter: Donald j. trump and the politics of debasement', *Critical studies in media communication* **34**(1), 59–68.

Owens, J. (2018), 'Twitter cracking down on political posts ahead of australian election'.
URL: https://www.theaustralian.com.au/national-affairs/foreign-affairs/russias-tweet-troll-factory-meddled-in-australian-politics/news-story/24674946dab18d03ec6055a675b66856

Peisakhin, L. & Rozenas, A. (2018), 'When does russian propaganda work — and when does it backfire?'.
URL: https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/03/when-does-russian-propaganda-work-and-when-does-it-backfire-heres-what-we-found/

Penzenstadler, N., Heath, B. & Guynn, J. (2018), 'We read every one of the 3,517 facebook ads bought by russians. here's what we found'.
URL: https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/

Pertsev, A. (2018), 'Russian political consultants discover africa'.
URL: https://www.kommersant.ru/doc/3607961#comments

Petreski, V. & Kanishk, K. (2019), 'Election watch: Macedonian memes, american midterms'.
URL: https://medium.com/dfrlab/electionwatch-macedonian-memes-american-midterms-b1f35f9df2ee

Poulsen, K. (2018), 'Mueller finally solves mysteries about russia's 'fancy bear' hackers'.
URL: https://www.thedailybeast.com/mueller-finally-solves-mysteries-about-russias-fancy-bear-hackers

Poulsen, K. & Ackerman, S. (2018*a*), 'The most shocking moments of the new russia complaint, from civil war to fake rubio to colored lgbt'.
URL: https://www.thedailybeast.com/the-most-shocking-moments-of-the-new-russia-indictment-from-civil-war-to-fake-rubio-to-colored-lgbt

Poulsen, K. & Ackerman, S. (2018*b*), 'The most shocking moments of the new russia complaint, from 'civil war' to 'fake' rubio to 'colored lgbt''.
URL: https://www.thedailybeast.com/the-most-shocking-moments-of-the-new-russia-indictment-from-civil-war-to-fake-rubio-to-colored-lgbt

Poulsen, K., Ackerman, S., Collins, B. & Resnick, G. (2017), 'Exclusive: Russians appear to use facebook to push trump rallies in 17 u.s. cities'.
URL: https://www.thedailybeast.com/russians-appear-to-use-facebook-to-push-pro-trump-flash-mobs-in-florida

Prentis, J. (2018), 'Facebook and twitter say iran propaganda pages deleted'.
URL: https://www.thenational.ae/world/mena/facebook-and-twitter-say-iran-propaganda-pages-deleted-1.762801

Price, R. (2018), ‘Facebook says iran-backed accounts pretended to be news organizations to spread information and to launch cyber attacks’.
URL: https://www.businessinsider.sg/facebook-detects-information-campaigns-russia-iran-2018-8/

Radio, S. (2016), ‘Russia’s propaganda efforts underscored in sapo report’.
URL: https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6391875

RFE (2018), ‘Russian trolls found amplifying u.s. republican charge against fbi’.
URL: https://www.rferl.org/a/russian-trolls-amplify-us-republican-charge-anti-trump-bias-at-fbi-/28986362.html

Rocha, R. (2018), ‘Data sheds light on how russian twitter trolls targeted canadians’.
URL: https://www.cbc.ca/news/canada/russian-twitter-trolls-canada-targeted-1.4772397

Romm, T. & Timberg, C. (2018), ‘Facebook suspends five accounts, including that of a social media researcher, for misleading tactics in alabama election’.
URL: https://www.washingtonpost.com/technology/2018/12/22/facebook-suspends-five-accounts-including-social-media-researcher-misleading-tactics-alabama-election/?utm_term=.8c4df3c6ce55

Rosendahl, J. & Forsell, T. (2016), ‘Finland sees propaganda attack from former master russia’.
URL: https://www.reuters.com/article/us-finland-russia-informationattacks/finland-sees-propaganda-attack-from-former-master-russia-idUSKCN12J197

RT (2018), ‘Russians view us, ukraine and eu as country’s main enemies – survey’.
URL: https://www.rt.com/russia/415487-russians-us-ukraine-eu-enemies/

Ruediger, M. (2018), ‘Electionwatch: Fgv dapp uncovers foreign twitter influence in brazil’.
URL: https://medium.com/dfrlab/electionwatch-fgv-dapp-uncovers-foreign-twitter-influence-in-brazil-7ab24e34223

Sanger, D. E. (2018), ‘Mystery of the midterm elections: Where are the russians?’.
URL: https://www.nytimes.com/2018/11/01/business/midterm-election-russia-cyber.html

Sanger, D. E. & Frenkel, S. (2018), ‘New russian hacking targeted republican groups, microsoft says’.
URL: https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html

Satter, R., Donn, J. & Vasilyeva, N. (2017), ‘Russian hackers hunted journalists in years-long campaign’.
URL: https://apnews.com/c3b26c647e794073b7626befa146caad

Savytskyi, Y. (2016), 'Kremlin trolls are engaged in massive anti-ukrainian propaganda in poland'.
URL: `http://euromaidanpress.com/2016/06/21/kremlin-trolls-are-engaged-in-massive-anti-ukrainian-propaganda-in-poland/`

Sazonov, V., Müür, K. & Mölder, H. (2016), 'Russian information campaign against the ukrainian state and defence forces', *NATO Strategic Communications Centre of Excellence. https://bit. ly/2uwuleY* .

Schafer, B. (2017), 'Dashboards hamilton 68 and artikel 38'.
URL: `https://securingdemocracy.gmfus.org/securing-democracy-dispatch-10/`

Sear, T. & Jensen, M. (2018), 'Russian trolls targeted australian voters on twitter via auspol and mh17'.
URL: `https://theconversation.com/russian-trolls-targeted-australian-voters-on-twitter-via-auspol-and-mh17-101386`

Shane, S. (2018), 'Five takeaways from new reports on russia's social media operations'.
URL: `https://www.nytimes.com/2018/12/17/us/politics/takeaways-russia-social-media-operations.html`

Shane, S. & Blinder, A. (2018), 'Secret experiment in alabama senate race imitated russian tactics'.
URL: `https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html`

Silverman, C. (2016), 'Pro-trump twitter trolls are turning their attention to angela merkel'.
URL: `https://www.buzzfeednews.com/article/craigsilverman/pro-trump-twitter-trolls-and-merkel/`

Silverman, C. & Lawrence, A. (2016), 'How teens in the balkans are duping trump supporters with fake news'.
URL: `https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo#.fu2okXaeKo`

Silverman, C., Lester, F. J., Cvetkovska, S. & Belford, A. (2018), 'Macedonia's pro-trump fake news industry had american links, and is under investigation for possible russia ties'.
URL: `https://www.buzzfeednews.com/article/craigsilverman/american-conservatives-fake-news-macedonia-paris-wade-libert`

Snegovaya, M. (2017), 'Russian propaganda in germany: More effective than you think'.
URL: `https://www.the-american-interest.com/2017/10/17/russian-propaganda-germany-effective-think/`

Sobolev, A. (2019), 'How pro-government "trolls" influence online conversations in russia'.

Solon, O. (2017), 'How syria's white helmets became victims of an online propaganda machine'.
URL: `https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories`

Soshnikov, A. (2017), 'Inside a pro-russia propaganda machine in ukraine'.
URL: https://www.bbc.com/news/blogs-trending-41915295

Staff, M. (2018), 'Russia driving huge online 'disinformation' campaign on syria gas attack, says uk'.
URL: https://www.middleeasteye.net/news/russia-driving-huge-online-disinformation-campaign-syria-gas-attack-says-uk

Stein, J. (2018), 'Tammy baldwin seeks hearing after russians pushed image of obama in noose at badgers game'.
URL: https://www.jsonline.com/story/news/politics/2018/03/21/tammy-baldwin-calls-twitter-troll-hearing-russians-pushed-wisconsin-image-obama-noose/446618002/

Stewart, L. G., Arif, A. & Starbird, K. (2018), Examining trolls and polarization with a retweet network, *in* 'Proc. ACM WSDM, Workshop on Misinformation and Misbehavior Mining on the Web'.

Stojanovski, F. (2017), 'Fake news tries to link austria's chancellor-to-be and philanthropist george soros'.
URL: https://www.stopfake.org/en/fake-news-tries-to-link-austria-s-chancellor-to-be-and-philanthropist-george-soros/

Stubbs, J. & Bing, C. (2018), 'Special report: How iran spreads disinformation around the world'.
URL: https://www.reuters.com/article/us-cyber-iran-specialreport/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FT

Stukal, D., Sanovich, S., Tucker, J. A. & Bonneau, R. (2019), 'For whom the bot tolls: A neural networks approach to measuring political orientation of twitter bots in russia', *SAGE Open* **9**(2).

Subramanian, S. (2017), 'The macedonian teens who mastered fake news'.
URL: https://www.wired.com/2017/02/veles-macedonia-fake-news/

Summers, J. (2017), 'Countering disinformation: Russia's infowar in ukraine'.
URL: https://jsis.washington.edu/news/russia-disinformation-ukraine/

Superlinear (2018), 'Social media disinformation: parallels between the us and south african experiences'.
URL: http://www.superlinear.co.za/social-media-disinformation-parallels-between-the-us-and-south-african-experiences/

Szal, A. (2015), 'Report: Russian 'internet trolls' behind louisiana chemical explosion hoax'.
URL: https://www.manufacturing.net/news/2015/06/report-russian-internet-trolls-behind-louisiana-chemical-explosion-hoax

Szymański, P. (2018), 'Finland: the fight against disinformation'.
URL: https://www.osw.waw.pl/en/publikacje/analyses/2018-10-24/finland-fight-against-disinformation

Tait, M. (2017), 'The macron leaks: Are they real, and is it russia?'.
URL: https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia

Timberg, C. & Romm, T. (2018), 'These provocative images show russian trolls sought to inflame debate over climate change, fracking and dakota pipeline'.
URL: https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/congress-russians-trolls-sought-to-inflame-u-s-debate-on-climate-change-fracking-and-dakota-pipeline/

Troianovski, A. (2018), 'A former russian troll speaks: It was like being in orwell's world'.
URL: https://www.youtube.com/watch?v=9CKYAzPhFAo

van der Noordaa, R. & van de Ven, C. (2019), 'The mh17 plot'.
URL: https://www.groene.nl/artikel/het-mh17-complot

Vilmer, J.-B. J., Escorcia, A., Guillaume, M. & Herrera, J. (2018), Information manipulation: A challenge for our democracies, Technical report, Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces.

Volz, D. (2017*a*), 'U.s. far-right activists, wikileaks and bots help amplify macron leaks: researchers'.
URL: https://www.reuters.com/article/us-france-election-cyber/u-s-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks-researchers-idUSKBN1820QO

Volz, D. (2017*b*), 'U.s. far-right activists, wikileaks and bots help amplify macron leaks: researchers'.
URL: https://www.reuters.com/article/us-france-election-cyber/u-s-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks-researchers-idUSKBN1820QO

Watts, C. (2017), 'Clint watts' testimony: Russia's info war on the u.s. started in 2014'.
URL: https://www.thedailybeast.com/clint-watts-testimony-russias-info-war-on-the-us-started-in-2014

Watts, C. & Weisburd, A. (2016), 'How russia wins an election'.
URL: https://www.politico.com/magazine/story/2016/12/how-russia-wins-an-election-214524

Weixel, N. (2018), 'Nearly 600 russian troll accounts tweeted about obamacare: report'.
URL: https://thehill.com/policy/healthcare/406309-nearly-600-russian-troll-accounts-tweeted-about-obamacare-report

Wendling, M. (2017), 'Russian trolls promoted california independence'.
URL: https://www.bbc.com/news/blogs-trending-41853131

Withnall, A. (2018), 'Finland: Russian propaganda questioning our validity risks destabilising country'.
URL: https://www.independent.co.uk/news/world/europe/russia-finland-putin-propaganda-destabilising-effect-a7371126.html

Wong, Q. & Hautala, L. (2018), ‘Facebook removes iranian influence campaign as midterms near’.
URL: `https://www.cnet.com/news/facebook-announces-removal-of-iranian-influence-campaign-as-midterms-near/`

Woolley, S. C. & Howard, P. N. (2017), ‘Computational propaganda worldwide: Executive summary’, *Working* (11. Oxford, UK), 14pp.

Yaron, O. (2018), ‘Tel-aviv times? iran created fake hebrew news sites in major ’influence campaign”.
URL: `https://www.haaretz.com/israel-news/.premium-israeli-cyber-security-company-iran-created-fake-hebrew-news-sites-1.6463020`

Yong, C. (2018), ‘Select committee on fake news: Russian trolls divided societies and turned countries against one another’.
URL: `https://www.straitstimes.com/politics/select-committee-on-fake-news-russian-trolls-divided-societies-and-turned-countries-against`

Yourish, K., Buchanan, L. & Watkins, D. (2018), ‘A timeline showing the full scale of russia’s unprecedented interference in the 2016 election, and its aftermath’.
URL: `https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-trump-election-timeline.html`

Zaveri, M. & Fortin, J. (2019), ‘Russian efforts exploited racial divisions, state of black america report says’.
URL: `https://www.nytimes.com/2019/05/06/us/russia-disinformation-black-activists.html`

Zhegulev, I. (2016), ‘Evgeny prigozhin’s right to be forgotten what does vladimir putin’s favorite chef want to hide from the internet?’.
URL: `https://meduza.io/en/feature/2016/06/13/evgeny-prigozhin-s-right-to-be-forgotten`

Zhuang, M. (2018), ‘Intergovernmental conflict and censorship: Evidence from china’s anti-corruption campaign’, *SSRN* .