Trends in Online Influence Efforts*

Diego A. Martin[†] Jacob N. Shapiro[‡] Julia G. Ilhardt[§]

Version 2.0
August 5, 2020

Abstract

Information and Communications Technologies (ICTs) create novel opportunities for a wide range of political actors. 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 updates previous work with data on 76 such foreign influence efforts (FIE) targeting 30 different countries from 2013 through 2019, as well as 20 domestic influence efforts (DIE) in which governments targeted their own citizens. Influence efforts (IEs) are defined as: (i) coordinated campaigns by a state or the ruling party in an autocracy to impact one or more specific aspects of politics at home or 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 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 920 media reports and 380 research articles/reports to identify IEs, track their progress, and classify their features.

*We are grateful to a range of colleagues including Laura Courchesne, Nick Feamster, Andy Guess, Hans Klein, Brendan Stewart, and Alicia Wanless for helpful comments and feedback. Will Lowe provided invaluable advice on data structure and data entry. Jordan Allen, Nicola Bariletto, Arya Goel, Danielle Hull, Janette Lu, Imane Mabrouk, Matthew Merrigan, Justinas Mickus, Brendan O'Hara, Jan Oledan, Kamila Radjabova, Nina Sheridan, Joe Shipley, Jack Tait, Kamya Yadav, and Luca Zanotti provided excellent research assistance. This work was possible thanks to generous funding from the Bertelsmann Foundation and Microsoft. All errors are our own.

[†]Purdue University, Economics Department, West Lafayette, IN 47907. E-mail: dmartinl@purdue.edu.

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

[§]Princeton University, School of Public and International Affairs, Princeton, NJ 08544. Email: jilhardt@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). They have also 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 voters 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, state actors have used social media to influence politics at home and abroad by promoting propaganda, advocating controversial viewpoints, and spreading disinformation (Bail et al. 2020, Golovchenko et al. 2020).

This report describes a database of foreign influence efforts (FIEs) and domestic influence efforts (DIEs) which builds on and extend the previously-released data in Martin et al. (2019). 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. Similarly, DIEs are defined as: (i) coordinated campaigns by a state to impact one or more specific aspects of domestic politics, (ii) through media channels, including social media; by (iii) producing content designed to appear as though it is produced by normal users. To be included in the data an IE 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 in which state-supported media outlets promote specific narratives, IEs disguise the origin of the content (though many IEs appear to be coordinated with such traditional propaganda efforts).

Our data draw on more than 920 media reports to identify IEs, track their progress, and classify their features.[1] We identified 76 FIE and 20 DIE, in 49 targeted countries, from 2011 through 2020.[2]

Fully 64% of FIEs were conducted by Russia. China, Iran, Saudi Arabia, and United Arab Emirates account for most of the remainder. The 20 DIEs were conducted by 18 different countries, including democratic states such as Mexico. In seven cases press reports did not provide sufficient evidence to determine the origin of the campaign. We also examined

[1] For a full listing of news articles consulted in developing the data see this link. For research articles and reports see here.

[2] The closest work to ours is the excellent review by the Australian Strategic Policy Institute which focuses 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."

60 other information operations which met some, but not all of our inclusion criteria.[3]

Russia's frequent use of FIEs is not surprising. 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 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).

FIEs 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. More recent evidence has revealed growing disinformation capacity in Egypt, Saudi Arabia, and the United Arab Emirates (DiResta et al. 2019, Grossman, H., DiResta, Kheradpir & Miller 2020). Though in all three cases there is more reliance on for-profit marketing firms than has been observed for Russia, China, or Iran.

By contrast there is significant geographical diversity in the use of DIEs. Russia and China seem to maintain particularly robust apparatuses for suppressing and drowning out online political opposition (Nimmo, Francois, Eib & Ronzaud 2020, Nimmo 2019). But the other countries using DIEs span a wide range of locations and levels of democracy.

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 reports the new trends observed over the course of 2019 and early 2020. Section 5 discusses implications and 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). For a summary of Russian operation between 2014 and 2020 in Europe and the US see Nimmo, Francois, Eib, Ronzaud, Ferreira, Hernon & Kostelancik (2020) and Grossman et al. (2019) for Russian FIEs targeting multiple countries in Africa. For a deep dive on Iranian influence operation see Revelli & Foster (2019) analyzed.

2 Influence Effort Database

The primary objective of this project is to compile a list of distinct IEs. An IE 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)). We track IEs to summarize trends in these operations, provide baseline information about who is doing what to whom, 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

[3]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.

do not seek to mask its origin).[4]

IEs may involve promoting true content as well as false or misleading information. Note that in our definition the deception refers to the origin of the content as opposed to its veracity. Campaigns often involve false information, but sometimes they simply involve fake personas promoting specific true information. Not all IEs involve misinformation, and not all campaigns to promote misinformation meet this criteria.

We divided IEs into foreign influence efforts (FIEs) and domestic influence efforts. (DIEs). In FIEs the content is designed to look as though it is from the targeted country. For example, Russia targeted Libya beginning in 2018 to support the country's foreign policy goals. Fake Facebook accounts originating in Russia sought to artificially amplify local support for the Libyan National Army (Grossman et al. 2019). Russian social media pages masqueraded as Libyan outlets, and the network established a physical Libyan newspaper to promote content consistent with the foreign policy initiatives of the Kremlin (Grossman, H. & DiResta 2020).

DIE's go beyond normal government propaganda and press work by trying to pass off content as the activity of normal citizens (the analogue of producing content intended to appear indigenous to the target state). Of course, many political parties engage in such work. We consider such efforts to be a DIE when the influence effort is attributable to the ruling party/coalition (holding executive power) which can effectively leverage state resources for its own purposes. We operationalize that consideration as one of the following conditions holding for the majority of years in which the DIE was active, or for the most recent available year if scores for those years have not been published yet: (i) the country is an anocracy or an autocracy;[5] or (ii) constraints on the ruling party's ability to leverage state power for electoral purposes are weak or non-existent.[6] For instance, the case CUB0001 describes the Communist Party of Cuba's network of "ciberclarias" or cyber catfishes, thought to be Cubans paid to maintain fake social media accounts sympathetic to the government (González 2019). Cuba is classified as an anocracy, and thus a campaign to attack political opposition on behalf of the ruling party constitutes a DIE.

The database was built in three steps following standard practices for constructing such data:[7]

[4]IEs are distinct from the broader category of disinformation campaigns which often have a profit motive and can include content clearly labeled as being produced in the influencing state.

[5]Operationalized as overall Polity score of +5 or lower in the Polity IV database (Marshall & Jaggers 2020)

[6]Operationalized as (a) an executive constraints (XCONST) equal to 1, 2 or 3 and (b) a competitiveness of participation score (PARCOMP) equal to 1, 2 or 3, both in the Polity IV database (Marshall & Jaggers 2020).

[7]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.

1. *Develop a coding schema.* Our data 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).[8] 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 923 news stories about influence efforts from dozens of 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.[9] 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 IEs.* In the first version of this report, 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.For the current version we reviewed 104 potential IEs. 23 FIEs met our inclusion criteria, 3 of which started in 2019 and 20 of which were missed in the prior report or were newly discovered. 20 DIEs met our inclusion criteria. Each candidate IE was reviewed and evaluated by all three of the authors.[10] The total of 96 cases from 2011 through the end of 2019 represent a lower bound on the number of IEs to date as it is possible there are IEs we did not capture.[11] Readers who know of such efforts should contact the authors. The database and report will be periodically updated.

[8]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 content.

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

[10]In the previous report all cases were reviewed by one of the authors as well as two student research assistants – one who did the original coding and a second student who had not previously worked on the case.

[11]In compiling this report we found FIEs active before 2019 which were missed in our previous report. 60% of these cases were substantiated by account removals on Facebook, and others garnered new evidence and research which qualified them as FIEs.

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

- Each IE 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, Latvia, 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 IE (e.g. Facebook, Twitter, etc.). We make no judgment about the extent to which different platforms are used.[12]

- The source table records a short description of the event and provides URLs for the main articles, news, reports, working papers, and journal articles 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.

- 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.

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

We also provide a complementary lightly annotated bibliography of 380 references containing research about online propaganda, influence operations and media consumption of voters.[13]

3 Trends in Influence Efforts

The 96 IEs since 2011 targeted 49 different countries. Of the 76 FIEs in the the database, 26% targeted the US; 16% multiple countries;[14] 9% Great Britain; Spain and Germany 4% each; Australia, France, Netherlands, South Africa, and Ukraine 3% each; with Armenia, Austria, Belarus, Brazil, Canada, Central African Republic, Finland, Israel, Italy, Libya, Lithuania, Madagascar, Macedonia, Mozambique, Poland, Saudi Arabia, Sudan, Spain, South Africa, South Saudi, Sweden, Taiwan, Thailand, and Yemen each being targeted once.[15] Of the 20 DIEs, two targeted Russia and two China; with citizens in Cuba, Ecuador, Honduras, Indonesia, Mexico, Malta, Myanmar, Pakistan, Puerto Rico, Saudi Arabia, Tajikistan, Turkey, Venezuela, Vietnam, and Zimbabwe each being targeted by one DIE

Of the 23 additional FIEs that met our inclusion criteria in this report, we found that only 3 started in 2019. Russia was behind these three operations, focused on inflaming Brexit tensions, supporting President Filipe Nyusi in Mozambique's 2019 elections, and supporting the African National Congress in South Africa's 2019 elections.

The last version of this report, published on July 8, 2019, did not include 20 FIEs which began prior to 2019 for several reasons. Twelve of these cases were created using information released after late-June. For example, on August 1st, 2019, Facebook removed multiple accounts originating in Egypt, Saudi Arabia, and the UAE for targeting countries in the Middle East, North and East Africa (Gleicher 2019*e*). Based on this information as well as additional reporting (e.g. Grossman, H., DiResta, Kheradpir & Miller (2020)), we could definitively identify seven FIEs.[16] Similarly, on October 30, 2019, Facebook removed inauthentic accounts originating in Russia which revealed cases in Central African Republic, Libya, Mozambique, Madagascar, and Sudan (Gleicher 2019*h*).

In addition, a number of cases identified as potential FIEs during our initial research acquired supplemental evidence over the past year and thus qualified as influence campaigns. At the time of our first report, for example, we did not find sufficient supporting material for a multinational Chinese FIE targeting the diaspora. However, Nimmo, Francois, Eib & Ronzaud (2020) and Cook (2020) revealed the scope and structure of this campaign targeting multiple countries between 2017 and 2020.

Despite the fact that five cases – two targeting Spain, one in Armenia, one in Macedonia,

[13]The following link provides the annotated bibliography updated on August 3, 2020.

[14]We describe multiple countries as targeted country in sub-section 4.2.

[15]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 were 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.

[16]The political goal of these cases are: influence Libyan politics within Libya and the region (three cases), isolate Qatar diplomatically and economically (two cases), promote pro-Saudi narratives, and promote pro-UAE narratives.

and one in Thailand – did not meet the FIE criteria in the previous version of the report, they are included in the updated database. Upon further review, we found new and missed sources which supported these cases.

Finally, based on two previously coded Iranian campaigns (one targeting Great Britain and one the U.S.), we identified two additional political goals that were missed during initial coding. These were undermining the British monarchy and promoting Iranian foreign policy initiatives in the U.S.

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. Figure 2 provides maps showing the distribution of countries targeted by foreign and domestic influence efforts. FIE targets are shaded according to the number of attacks, and DIEs are shaded according to the year of origin.

The first DIE in our data began in 2011, when protests in Russia catalyzed the creation of a pro-Kremlin trolling force. The Russian government sought to "rein in the Internet" through the tracking and manipulation of social media, and have continued to use this tactic in the years since (Chen 2015, Nimmo & Toler 2018). 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). An additional three FIEs began in 2013 when Egypt, Saudi Arabia, and the United Arab Emirates launched separate campaigns to influence Libyan politics within Libya and the region. There is no reliable evidence that these three FIEs were directly coordinated, although they promoted similar political agendas.

Fully 79% of the FIEs started between 2015 and 2018. The DIEs are more spread out, though 60% started between 2015 and 2018 . FIE attacks last for an average of 2.7 years with standard deviation of 1.8 years, while DIEs last 4.5 years on average with standard deviation 2.3 years.[17] At least one FIE was clearly ongoing in 2020: China's effort to promote pro-government narratives amongst the Chinese diaspora in multiple countries. At least six DIEs remained active in 2020: the Chinese government's attempt to undermine and delegitimize the Hong Kong protests; and efforts to suppress political opposition in Cuba, Honduras, Sudan, Tajikistan, and Venezuela.[18]

The most common actors involved in IEs are private companies (45% in FIEs and 40% in DIEs), media organizations (42% in FIEs and 40% in DIEs), governments (22% in FIEs and 80% in DIEs), and intelligence or military agencies (20% in FIEs and 60% in DIEs). Media reporting was insufficiently detailed to clearly identify the responsible actors in one-fourth of FIEs, but we could find at least one actor in all DIEs.[19]

Panel A in figure 5 presents the number of attacks involving each type of actor from

[17] The median duration is 2 years for FIEs and 4 for DIEs.

[18] Based on the sources, we code end year as the latest year in which the influence effort was active. Cases are not coded beyond 2019 in this iteration of the report.

[19] 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.

2011 through 2019, divided into FIEs and DIEs. Whereas the number of FIEs involving unknown actors increased to a peak of about 14 cases in 2018, no DIEs have included unknown actors. This may reflect FIE actors' increasing proficiency in masking their responsibility. As shown in Panel B, the relative share of FIEs involving each attacker remained fairly stable after 2015, though 2019 saw a mild uptick in the involvement of companies and governments. Conversely, the share of DIEs involving companies has declined significantly, while the share of DIEs involving government actors increased to approximately 75% by 2017.

3.2 Strategies and Tactics

IEs have employed a wide range of strategies and we do not see clear trends over time.[20] The most commonly-used strategy is persuasion, which we define as trying to move the average citizen to one side of an issue, used in 74% of FIEs and 100% of DIEs. Defamation, defined as attempts to harm the reputation of people or institutions, is used in 72% of FIEs and 96% of DIEs.

Only 11% of FIEs use polarization – defined as trying to move opinion to the extremes on one or more issues – and no DIEs use this strategy. These findings contradict the idea that IEs most often work to polarize public opinion (Stewart et al. 2018, see e.g.).[21]

Figure 6, panel A, presents the total number of attacks employing each strategy during the study period. Defame and persuade were used in a majority of IEs throughout the period. Although the number of cases involving polarization is modest – only 9 cases by 2019 – they were an increasing share of active efforts until 2018, as Panel B shows. Efforts to shift the political agenda and undermine institutions have been rare across all IEs.

There is much less heterogeneity in which approaches have been used over time. Three in five FIEs include all three approaches – amplify, create, and distort – in the same operation, as do four in five DIEs. 93% (90%) of the FIEs (DIEs) use creation of original content, 86% (95%) amplification of pre-existing content, and 74% (90%) distortion of objectively verifiable facts.[22] Creation of new content has been the most common approach in every year, as figure 3, panel A shows. Since 2016 amplification has been more commonly used than distortion in FIEs. In DIEs, creation of original content was the most common approach until 2015, when amplification became the most common, as figure 3, panel B presents.

When it comes to tactics, there is a great deal of variance, but few distinct trends over time. Fully 9 out of 10 FIEs and 8 out of 10 DIEs use trolls. Half of the FIEs use automation to spread their message, and 65% of DIEs use bots. The share of IEs doing so has been fairly stable since 2014, as we see in figure 7, panel B. Similarly, just over half of the FIEs use fake accounts, a number which has remained stable since 2014. However,

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

[21] 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.

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

95% of the DIEs use fake accounts. 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 credibly makes that claim. 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 32% of FIEs and half of DIEs.

3.3 Platforms

Twitter, Facebook, and news outlets are the most common platforms used in FIEs, as figure 8 shows. In DIEs, the most common platforms are Facebook, Twitter, Instagram, and other platforms. Twitter is used in 86% of FIEs and 75% of DIEs, followed by Facebook (70% of FIEs and 79% of DIEs), news outlets for FIEs (55%), and Instagram for DIEs (45%).[23] This pattern likely reflects Facebook and Twitter's market shares, as well as the fact that both platforms offer free access and historically had low capacity to screen content, though that is changing. All three characteristics make them good 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 nation-state operations on their platforms.[24] These reports, and Twitter's regular data releases, make it easier to report on how IEs have used them, which in turn leads them to be highly represented in our data.

Other platforms are used in 54% of FIEs and 45% of DIEs.[25] As figure 8, Panel B shows, Instagram has been used in an increasing share of all IEs since 2014, and YouTube has been used in an increasing share of FIEs. Despite these apparent trends, it is important to note that the use of platforms in furtherance of IEs is distinct from an assessment of interaction of IE content on those platforms. Assessing the latter requires approaches akin 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 continued to increase on Twitter in the following two years but fell on Facebook.

3.4 Combinations Across Fields

Table 2.1 shows the percentage of cases that combine two strategies. Defame and persuade (70% of FIEs and 100% of DIEs) is the most commonly-used combination, followed by undermine institutions and shift the political agenda (37% of FIEs and 50% of DIEs). Table 2.2, analogously, shows that trolling, bots (88% of FIEs and 85% of DIEs), fake

[23]Both Facebook and Twitter are commonly used by political activists 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.

[24]E.g. Facebook reporting on Russia's operation targeting the 2016 US presidential election (NewsWhip 2018).

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

accounts (88% of FIEs and 79% of DIEs), and hashtag hijacking (86% of FIEs and 80% of DIEs) are typically used together. Finally, table 2.3 demonstrates that Twitter, Facebook, Instagram, and e-mail are used together most of the time.

3.5 Attacking countries

Russia has been the main country using FIEs to date, as figure 4, Panel A, shows. In 2019, Russia was the only country initiating new FIEs, though at a lower rate than in previous years (others did continue previously-started campaigns). China and Tajikistan initiated new DIEs in 2019. At its peak in 2017, we estimate that Russia was engaged in 34 distinct campaigns around the world. As figure 4, Panel B shows, the initiation of new campaigns also peaked globally in 2017 with 18 new FIEs and 6 new DIEs. 11 of these campaigns came from Russia, followed by two each from China, Iran, Saudi Arabia, and an unknown attacker. Iran was involved in 2 cases between 2014 and 2015, but steadily increased their activity through 2018 when they were operating against 10 other nations.[26] China, Egypt, Iran, Saudi Arabia, United Arab Emirates, and Venezuela each initiated FIEs during our study period. As for DIEs, Russia and China each carried out 2 campaigns, while all other countries carried out 1 case each.[27]

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 country's 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.[28]

Based on media reporting prior to 2019, those managing Russian IEs organize their workers in a hierarchical manner. Employees at the Internet Research Agency, for example, reportedly received subjects to write about each day and were divided into groups, where those with the 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 occurrences,

[26]There is some evidence suggesting that Iran also carried out a FIE in Nigeria in 2018 and 2019. A network of Iranian Facebook accounts removed in March 2019 included eight pages attempted to appear indigenous to Nigeria (Nimmo et al. 2019). One focused on Nigeria's 2019 presidential election, but most sought to promote Iranian leadership in the Islamic world. ClearSky (2018) found additional evidence of Iranian websites impersonating Nigerian outlets and emphasizing the persecution of Nigeria's Shia minority.

[27]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.

[28]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. Watts argues that Russia's Active Measures today work far better than that of their Soviet predecessors. During the Cold War, Soviet operatives 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.

such as new policies, diplomatic events between governments, and various kinds of accidents. Pro-Kremlin trolls have also been involved in domestic efforts, such as attacks on the opponents of President Putin (Khachatryan 2015). In 2019, Russian FIEs increasingly depended on private companies and military contractors compared to earlier periods.

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.[29] However, as with Russia, China has conducted two DIEs, and a growing body of literature examines China's efforts to influence the Chinese diaspora abroad (Wallis et al. 2020). We added one Chinese FIE targeting multiple countries because the messaging was focused on discrediting opposition figures within China across contexts.

When it comes to partisanship, Russian efforts are most-often associated with driving right-wing or Russia-friendly parties. Leading up to Madagascar's 2018 presidential elections, for example, Russia used social media manipulation and bribery to support a number of different candidates as they became the frontrunner (Schwirtz & Borgia 2019). In the Central African Republic, Russia distorted support for President Faustin-Archange Touadéra, who has maintained close ties with Kremlin actors (Thomas 2019*a*). Particularly in Europe, however, there are cases of Russia supporting left-wing parties and movements, such as leaking and amplifying documents to advance the agenda of the UK's Labour Party in 2019 (Wendling 2019). Rather than following a fixed political ideology, Russian FIEs sometimes focus on stoking social tensions or pragmatically adjusting support according to different geopolitical goals.

In particular, Russia has operated a number of well-documented interference efforts in the United States which amplify both sides of political issues. In the 2016 US presidential elections, 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 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.

Overall, Russia has conducted 13 distinct FIEs in the US; 4 in Great Britain;[30] 3 against multiple countries simultaneously with a common political goal; two each against Australia, Germany, Netherlands, South Africa, and the Ukraine (one of which has been ongoing since 2015); and one FIE in each of the following countries: Armenia, Austria, Belarus, Brazil, Canada, Central African Republic, Finland, France, Italy, Libya, Lithuania, Macedonia, Madagascar, Mozambique, Poland, Sweden, Spain, Sudan, Thailand, and Syria (the latter involving efforts to obscure responsibility for chemical weapons attacks by the Syrian government). Russia has launched two DIEs, focused almost exclusively on suppressing political opposition.

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

[30]According to a British parliamentary report released on July 21, 2020, British authorities have largely ignored sustained Russian efforts to interfere in British politics dating back to at least 2014 (Landler & Castle 2020). The report concludes that the government has done little to investigate Russian involvement in the Brexit referendum and other significant events.

Russian IE 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), Emmanuel Macron in the 2017 French elections, Hillary Clinton in the 2016 US Presidential election, the White Helmets, Theresa May, US military operations in various locations around the world, anti-government protests in Sudan, and domestic political opposition.[31]

- 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), the Brexit referendum, Catalonia's 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,[32] the Annexation of Crimea by the Russian Federation, the Libyan National Army and General Khalifa Haftar, the National Congress (ANC) party in South Africa's 2019 Presidential election, Russian foreign policy across Central Asia and Thailand, President Faustin-Archange Touadéra in the Central African Republic, pro-Russia candidates in Madagascar's 2018 Presidential elections, Filipe Nyusi in Mozambique's 2019 Presidential election, and Moscow's housing demolition plan.

- Undermine and reduce support for: Angela Merkel and her political decisions, the Belarusian government, Sebastian Kurz after the 2017 Presidential elections in Austria, the Australian government, Barack Obama, the relationship between Poland and Ukraine, and Armenia's 2017 Presidential elections.

- Other political goals include: criticizing the UK's participation in the Syrian conflict, discrediting people identifying Russian propaganda, distorting perceptions of the relationship between Lithuania and Belarus, influencing Brazilian elections,[33] promoting Russian propaganda, reducing 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, preventing Macedonia from acceding to NATO, and inflaming Brexit tensions in the UK.

Russia uses political interference for a broad array of foreign policy initiatives, and other countries appear to be learning from Russian activities. Iranian trolls followed a similar mix of strategies to the Russians, though no evidence has come to light of an Iranian

[31]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).

[32]There are examples of Russian-origin tweets supporting the YesCalifornia group and Russian-created Facebook pages supporting Texas Independence.

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

company running operations as the Internet Research Agency did for Russia.[34] Unlike Russian FIEs, Iranian trolls have attacked President Trump, the Republican party, Secretary of State Mike Pompeo, and the British monarchy, 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, while simultaneously pushing their own agendas (Barojan 2018*c*, Nimmo & Brookie 2018*b*). Iranian trolls have also attacked both the Israeli and Saudi Arabian governments (Kanishk et al. 2019).[35] 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 What is new?

Over the course of 2019 and early-2020, we observed a number of notable new trends in both the tactics and objectives employed by FIEs. First, recent IEs originating in Russia, the Middle East, and elsewhere frequently involved the use of commercial bot networks and marketing firms. This obscured the involvement of state actors and, in some cases, made it impossible to attribute campaigns to particular countries. Relatedly, more campaigns employed local nationals to manage and promote social media pages than was previously observed. Second, we observed several cases where states targeted multiple countries. For example, campaigns from Saudi Arabia, the United Arab Emirates (UAE), and Egypt sought to influence Libyan politics both within Libya and the region more broadly. Other cases involved common content with country-specific distribution. Third, a series of seemingly related efforts originated in Russia which interfered in the elections and domestic politics of several African countries, particularly where Russian firms have significant mining interests.

The number of countries which engaged in DIEs was substantially greater than those which conducted FIEs, and several DIEs extended over at least five years. DIEs were often used to support the rule of authoritarian regimes by complementing traditional censorship tactics and quelling political opposition.

4.1 Outsourcing IEs to Marketing Firms

In May of 2019, Facebook removed a network of accounts associated with the Israeli political marketing firm Archimedes Group. The campaign interfered in political events and

[34] Nimmo (2018*e*) 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.

[35] 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.

local media landscapes, targeting countries across Central and Northern Africa, Latin America, and Southeast Asia (Gleicher 2019*b*). While Archimedes Group's tactics reflected those of the Kremlin and other state-backed social media campaigns, researchers could not identify evidence of the PR firm's clients. Despite pursuing a number of distinct political goals such as disrupting Nigeria's 2019 election, Archimedes Group effectively concealed the involvement of government actors (Bandeira et al. 2019). The group's social media advertising was paid for in everything from Brazilian reals to Israeli shekels to U.S. dollars, according to Facebook.

Archimedes Group is one of a growing number of marketing firms found to be involved in influence efforts in recent years (Bandeira et al. 2019). In December of 2019, for example, Twitter removed 88,000 accounts operated by the Saudi Arabian marketing firm Smaat (Twitter 2019). Smaat's known clients included companies like Coca Cola and Toyota as well as the Saudi General Directorate of Civil Defense and other government departments (DiResta et al. 2019). Smaat used fake and automated accounts to promote the brands of corporate clients, interspersed with political content disavowing Saudi Arabia role in the murder of journalist Jamal Khashhogi and attacking the governments of Qatar and Iran. In 2019, account takedowns by Facebook and Twitter also implicated marketing firms based in the United Arab Emirates, Egypt, and Nigeria. China's campaign to undermine pro-democracy protests in Hong Kong made use of bot networks that also promoted spam and commercial content (Stewart 2019), while attacks on Spain's elections involved bots which formerly targeted Venezuelan politics (Applebaum 2019).

The use of such contractors make it challenging to identify the actors behind social media manipulation. Outsourcing these operations also allows states to engage in political interference without developing the necessary expertise.

In 2019 there was also more evidence of states using local content creators, which also helped to obscure the identification of influence efforts (Schwirtz & Borgia 2019). In a 2019 takedown of Russian accounts, Facebook said the campaign used "authentic accounts of local nationals in Madagascar and Mozambique to manage Pages and Groups, and post their content" (Gleicher 2019*h*). This was a different approach than that followed by Russia's Internet Research Agency (IRA) in earlier years, providing the pages with a degree of authenticity (Grossman et al. 2019). In networks targeting the United States in 2016, the IRA reportedly employed trolling operations in Macedonia (Silverman et al. 2018), but we did not previously observe efforts to employ people within targeted countries. Going forward, the involvement of local networks, accounts, and outlets could increase the challenges of distinguishing FIEs from genuine discourse.

4.2 Campaigns Across Borders

In the previous version of this report, only 2 out of 54 FIEs involved multiple targeted countries. In the 2019 update, however, 9 out of 23 newly identified FIEs sought to simultaneously influence several countries. A number of these cases involved common content with country-specific distribution networks pushing the same policy agenda across targets. For example, a broad campaign associated with government actors and marketing firms in Saudi Arabia amplified pro-Saudi narratives in countries including Qatar, Saudi Arabia, UAE, Bahrain, Egypt, Morocco, Palestine, Lebanon and Jordan (Gleicher 2019*e*). Twitter accounts involved in the FIE posted primarily in Arabic and English, but also

Japanese, Russian, Spanish, and other languages (DiResta et al. 2019). Similar to traditional propaganda campaigns, officials used social media manipulation to distort local support for topics such as the Saudi Crown Prince or the Saudi Armed Forces.

The United Arab Emirates, China, and Russia engaged in similarly self-promotional behavior targeting broad multinational audiences. An FIE linked to the Russian government designed Facebook networks which amplified state-backed Russian media outlets masquerading as local content in numerous Central Asian countries. This significantly enhanced engagement with stories sympathetic to the foreign policy initiatives of the Kremlin. In Thailand, social media manipulation was used to amplify articles in New Eastern Outlook (NEO), a news website managed by the Russian Academy of Science's Institute for Oriental Studies. NEO maintains a page of Thailand-focused 'news' with some writers purporting to be based in Thailand, but also includes pages for tens of other countries around the world. NEO published content attributed to multiple fake journalistic personas, all of whom write along the "Kremlin party line" (EUvsDisinfo 2019*a*).

In addition, a number of FIEs sought to interfere in a country's domestic politics while also influencing regional or international sentiment surrounding that country. Notable examples are the cases which sought to support the Libyan National Army (LNA) and General Khalifa Haftar in the Libyan Civil War. Saudi Arabia, the United Arab Emirates, and Egypt were all linked with inauthentic Twitter networks which posed as Libyan citizens and pushed content designed to give the impression that other Libyans supported the LNA. At the same time, state-backed media outlets and local accounts in the Middle East amplified pro-Haftar stories and hashtags throughout the region. Inauthentic Twitter accounts thought to originate in the UAE spread similar messaging abroad in French and English (Carvin & Kassab 2019). This form of coordinated multinational influence effort was uncommon prior to 2019.

FIEs focusing on Libya also raised important questions about the extent to which attacks were interrelated. In a number of recent events, researchers found campaigns based in multiple countries pursuing tightly aligned political goals, but found no direct evidence of coordination. For example, in August of 2019, Facebook took down a network of accounts associated with the digital marketing firms "New Waves" in Egypt and "Newave" in the United Arab Emirates, both of which targeted countries in the Middle East and North Africa with content supported of Egyptian and UAE foreign policy. While the New York Times and others reported that these companies were "working in concert" on several narratives, including efforts to undermine pro-democracy protests in Sudan in 2019, they did not provide specific examples of coordination (Walsh & Rashwan 2019). Two months later, Facebook removed accounts from additional firms and told BuzzFeed News that the networks were "highly synced" (Lytvynenko & McDonald 2019), but again there was not unambiguous evidence of coordinated activity.

This trend made it somewhat more challenging to identify distinct FIEs within broader campaigns. We separated campaigns without evidence of explicit coordination into multiple events.

4.3 FIEs Targeting Africa

Nearly half of the new FIEs recorded in 2019 targeted African countries or regional groups including North Africa, compared to only one African case in the previous report. Though not explicitly connected, most of these 2019 events originated in Russia and were linked with Russian oligarch Yevgeny Prigozhin. Prigozhin is well-known for his association with the Internet Research Agency (IRA) and was indicted by special counsel Robert Mueller for interfering in the 2016 U.S. presidential election (Harding & Burke 2019, Golovchenko et al. 2020). The campaigns identified in 2019 targeted Libya, Sudan, South Africa, the Central African Republic, Madagascar, and Mozambique. In four of these countries, the Russian military contractor Wagner Group was also actively providing security, training, or working alongside local militias.

A clear economic incentive underlay some of these efforts, as Prigozhin-linked mining companies have obtained numerous contracts and deals in Africa (Searcey 2019). The Russian social media campaigns across Africa shared structural similarities, producing fake news pages designed to appear indigenous and promoting Russia-friendly candidates (Grossman et al. 2019). Unlike the IRA's efforts to sow political polarization in the United States, the content of campaigns in Africa was almost exclusively aligned with the political agenda of the Kremlin (Grossman 2019).

4.4 Widespread Use of DIEs

We observe 18 countries engaged in DIEs, compared to only 6 which interfered in foreign politics by creating false social media content. DIEs were used in several small countries including Malta and Honduras. The most common type of DIE aimed to increase support for a particular ruler or administration and to discredit the political opposition. For example, a number of social media campaigns were conducted on behalf of Mexican Institutional Revolutionary Party (PRI) candidates during Enrique Peña Nieto's presidency from 2012 to 2018 (Martinez 2018). Pro-PRI accounts came to be dubbed "Peñabots," artificially amplifying the president's agenda or accomplishments (Daniels 2016). As in a number of other campaigns, Mexico's "King of Fake News," entrepreneur Carlos Merlo, was explicit about the use of bots and other tactics to benefit various politicians or parties (Nimmo, Barojan, Peñarredonda & Karan 2018).

In other cases, DIE networks were openly incorporated into the government. In Vietnam, the military created a cyber unit called Task Force 47 — a 'troll army' charged with promoting the Vietnam Communist Party (VCP) and attacking opposition figures on social media. According to an official from the People's Army of Vietnam, he saw no reason to keep Task Force 47 a secret (TuoiTreNews 2017). Sudan created a similar "cyber jihadist unit" under the country's intelligence service, aimed at monitoring and regulating political thought via social media manipulation (FreedomHouse 2019). This form of sustained domestic interference inhibits the use of social media for personal expression or political discourse and has been employed to influence elections in both democratic and authoritarian regimes.

In addition to long-term efforts to embed political rule, some DIEs focused on influencing activism aroun specific events. For example, a state-backed Chinese network aimed to sow polarization and discord during the 2019 pro-democracy protests in Hong Kong. A

similar campaign targeted the Western Papuan independence movement in Indonesia. More than half of observed DIEs began in 2017 or later. Our research therefore suggests states are increasingly using social media manipulation to shape domestic politics.

4.5 Cases Involving No Influence Effort

Over the course of our review, we discuss a number of cases which aimed to interfere in the politics of domestic or foreign states but which did not meet our definitional criteria. We found numerous propaganda campaigns which lacked social media manipulation or any effort to make the content appear organic to the target. For example, Russian targeting of central Asian states met our criteria because the campaigns included fake personas, but Russia targeting of Serbia did not.[36]

In both events, Russia amplified the stories of state-backed media outlets such as Sputnik and Russia Today (RT) in an effort to popularize pro-Russian, anti-US and anti-EU sentiment. In Serbia, Russian news outlets have proliferated over the past several years, including a local Sputnik branch and television channels sponsored by Moscow (Šajkaš 2016). While stories originating in Russia sometimes fail to disclose their origins or quote any sources (EUvsDisinfo 2018), we found no evidence that Russian-backed outlets falsely claimed to be authentically Serbian. On the other hand, in Central Asian countries such as Romania and Tajikistan, a state-backed Russian campaign designed organic-looking social media networks which amplified Sputnik and other sources as local news (Aleksejeva et al. 2019*b*).

We also excluded a number of cases which involved certain state or party actors but did not have the clear support or financial backing of government entities. For instance, in Colombia, two officials participated in a WhatsApp group which coordinated social media campaigns designed to amplify support for the ruling party. Citizens participating in the group were instructed to troll various political dissidents or use particular hashtags (LaLiga 2020). Although this campaign included social media manipulation and was designed to appear indigenous, it is not clear that government officials acted on behalf of the state and thus carried out a DIE. Rather, it appeared to be the actions of enthusiastic government supporters.

Similarly, political parties in India have long made use of influence operations. Prime Minister Narendra Modi's Bharatiya Janata Party (BJP) developed an IT cell in 2007, and during Modi's 2014 campaign, the cell transitioned to focusing on social media (Dasgupta 2018). A former volunteer for Modi's troll network claimed that BJP coordinated online attacks directed at opposition politicians and journalists (Safi 2016). Prior to India's 2019 election, Facebook removed accounts linked to BJP and the major opposition party, the Indian National Congress (INC) (Karan & Nimmo 2019). While influence operations play a significant role in Indian politics, they do not constitute DIEs because these social media networks are associated with political parties in a democratic country where the parties face significant barriers to leveraging the government for political gain. We identified several other examples of parties using influence effort tactics in democracies.

[36]For full details on 37 borderline cases which met some but not all of our inclusion criteria see data here.

5 Conclusion

Foreign Influence Efforts (FIEs) have targeted countries around the world since 2013, and Domestic Influence Efforts (DIEs) have operated since 2011. While Russia has been the most active user of this new form of statecraft, other countries are following suit, with Egypt, Saudi Arabia, UAE, and Venezuela adopting the approach. 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.

6 Figures and tables

Table 1: Summary statistics

	Freq.			Freq.	
Variable	FIE	DIE	Variable	FIE	DIE
First sighting			Last sighting		
2011	0	1	2011	0	0
2012	0	3	2012	0	0
2013	4	1	2013	0	0
2014	9	1	2014	1	0
2015	13	3	2015	1	1
2016	16	0	2016	7	0
2017	18	6	2017	14	1
2018	13	3	2018	29	1
2019	3	2	2019	24	17

	Mean			Mean	
Variable	FIE	DIE	Variable	FIE	DIE
Actor			Platform		
Astroturf	0.09	0.10	Email	0.07	0.00
Company	0.45	0.35	Facebook	0.70	0.95
Cyber espionage group	0.05	0.10	Fake websites	0.12	0.15
Government	0.22	0.75	Google	0.13	0.05
Intelligence/Military Agency	0.20	0.55	Instagram	0.34	0.45
Media organization	0.42	0.35	Line	0.01	0.00
Real NGO	0.03	0.00	News outlets	0.55	0.25
Wealthy individual	0.05	0.05	Other media	0.20	0.05
Unknown	0.26	0.00	Reddit	0.09	0.00
Strategy			Twitter	0.86	0.75
Defame	0.70	0.95	Whatsapp	0.05	0.35
Persuade	0.72	1.00	Wikipedia	0.01	0.00
Polarize	0.12	0.00	Youtube	0.26	0.20
Shift agenda	0.11	0.10			
Undermine institutions	0.17	0.05	Tactic		
			Bot	0.54	0.65
Approach			Fake account	0.67	0.95
Amplify	0.86	0.95	Hashtag hijacking	0.29	0.50
Create	0.93	0.90	Other tactics	0.25	0.00
Distort	0.74	0.90	Steal information	0.12	0.25
			Troll	0.86	0.80

Influence efforts (IEs) are defined as coordinated campaigns by one state to impact politics in another state (or same state for DIE) through media channels, including social, in a manner which involves producing content that appears indigenous to the target state. The number of FIEs is is 76 and DIEs is 20, for a total number of 96 IEs. Each category is not mutually exclusive.

Table 2.1: Strategy combination

Panel A: Foreign influence efforts

	Defame	Persuade	Polarize	Shift agenda	Undermine
Defame	100				
Persuade	70	100			
Polarize	8	4	100		
Shift agenda	9	13	11	100	
Undermine	23	20	33	38	100

Panel B: Domestic influence efforts

	Defame	Persuade	Polarize	Shift agenda	Undermine
Defame	100				
Persuade	100	100			
Polarize	0	0	.		
Shift agenda	11	10	.	100	
Undermine	5	5	.	50	100

Notes: Given the total number of foreign or domestic influence efforts (FIEs or DIEs), panel A and panel B, respectively, using the strategy listed in the column, the table shows the percentage of cases also using the strategy listed in the row. For example, out of 9 FIEs that include polarization, 3 also include efforts to undermine institutions (33%). Numbers are the percentage rounded to the closest integer. The number of FIEs is 76 and DIEs is 20, for a total of 96 influence efforts (IEs).

Table 2.2: Tactic combination

Panel A: Foreign influence efforts

	Bots	Fake account	#Hijacking	Other tactics	Steal info.	Trolls
Bots	100					
Fake account	76	100				
#Hijacking	41	31	100			
Other tactics	20	24	9	100		
Steal info.	12	14	14	11	100	
Trolls	88	88	86	68	89	100

Panel B: Domestic influence efforts

Bots	100					
Fake account	100	100				
#Hijacking	69	53	100			
Other tactics	0	0	0	.		
Steal info.	31	21	30	.	100	
Trolls	85	79	80	.	80	100

Notes: Given the total number of foreign or domestic influence efforts (FIEs or DIEs), panel A and panel B, respectively, using the tactic listed in the column, the table shows the percentage of cases also using the tactic listed in the row. For example, out of 22 FIEs that include hashtag hijacking, 19 also include trolling (86%). Numbers are the percentage rounded to the closest integer. The number of FIEs is 76 and DIEs is 20, for a total of 96 influence efforts (IEs).

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	60	100											
Fake websites	40	14	100										
Google	20	15	25	100									
Instagram	0	46	33	45	100								
Line	0	0	0	0	0	100							
News outlets	40	44	50	73	46	100	100						
Other media	0	17	8	9	17	0	21	100					
Reddit	0	7	0	27	6	0	9	6	100				
Twitter	100	83	100	91	83	0	83	88	100	100			
Whatsapp	0	15	17	0	9	0	9	6	0	12	100		
Wikipedia	0	0	0	0	0	0	2	0	14	1	0	100	
Youtube	0	26	17	55	31	0	28	38	71	29	36	0	100

Given the total number of influence efforts (IEs) using the platform listed in the column, the table shows the percentage of cases also using the platform listed in the row. For example, out of 7 IEs that include the use of Reddit, 5 also include the use of YouTube (71%). The table combines foreign influence efforts (FIEs) and domestic influence efforts (DIEs), and numbers are the percentage rounded to the closest integer. The number of FIEs is 76 and DIEs is 20, for a total of 96 influence efforts (IEs).

Figure 1: Relational database structure

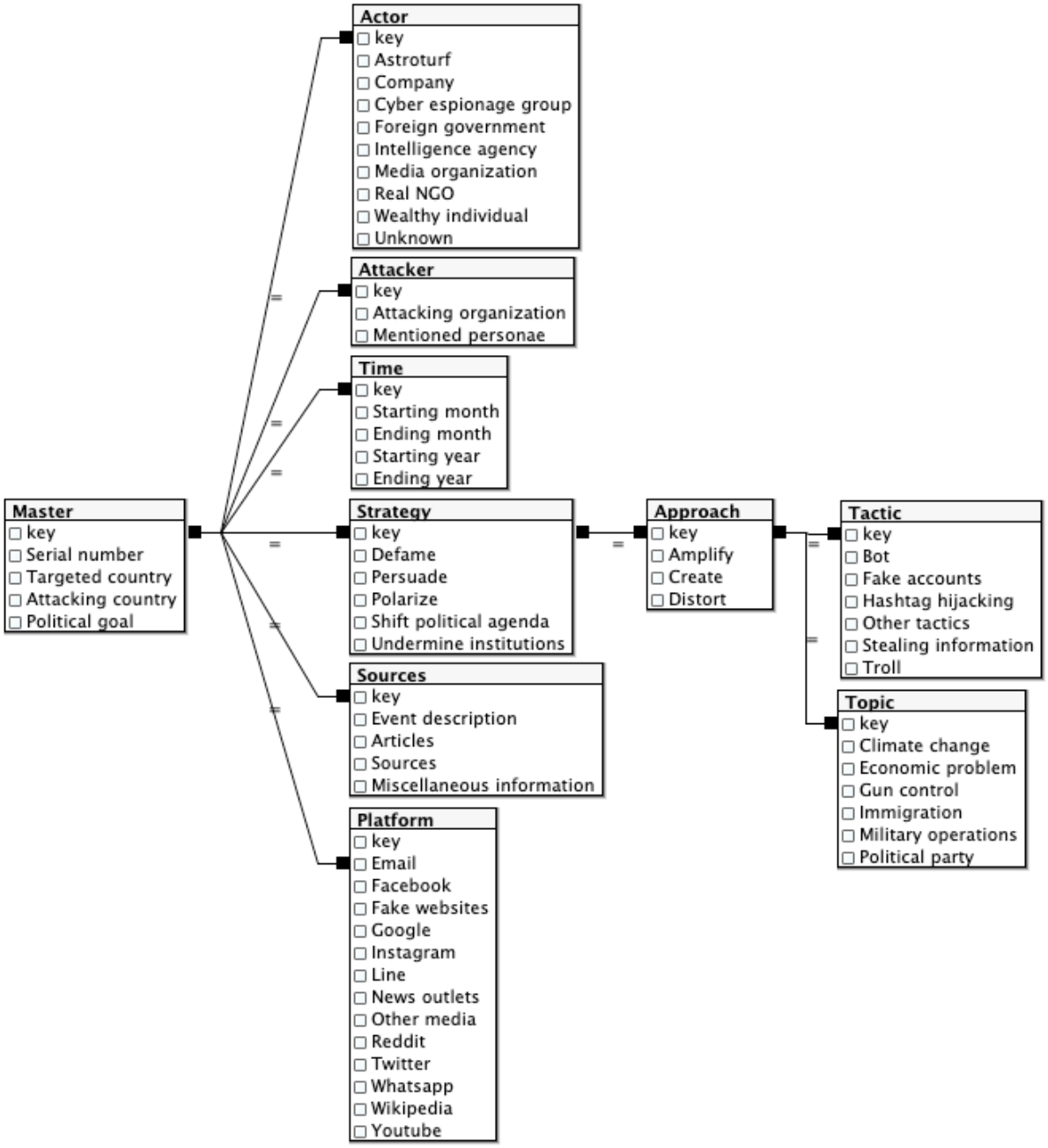
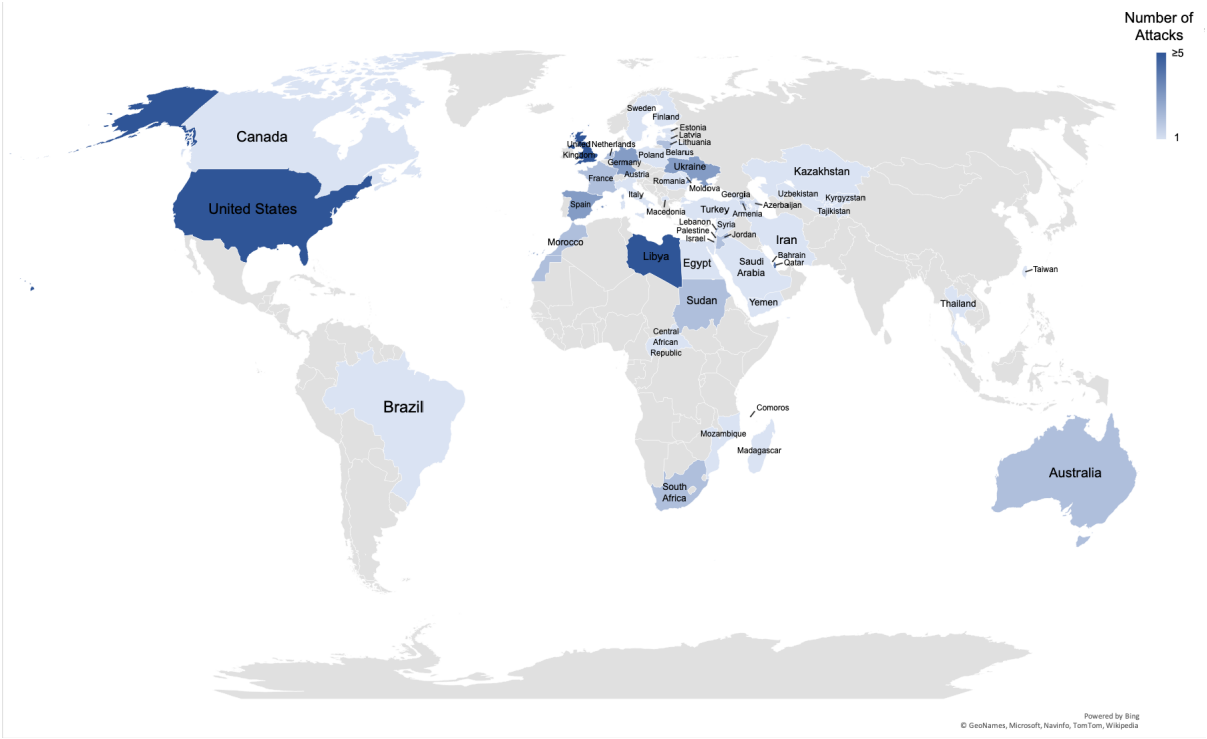
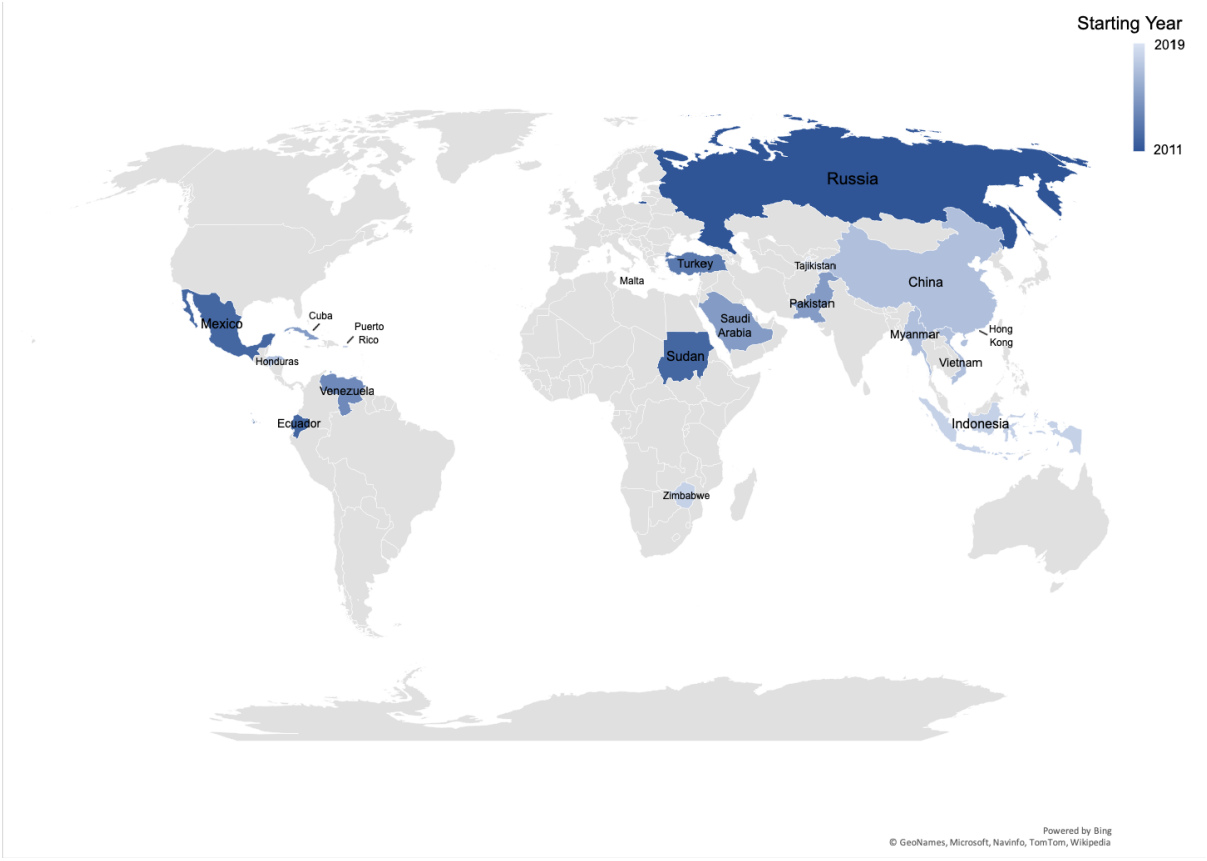


Figure 2: Distribution of influence efforts

Panel A: Countries targeted by foreign influence efforts



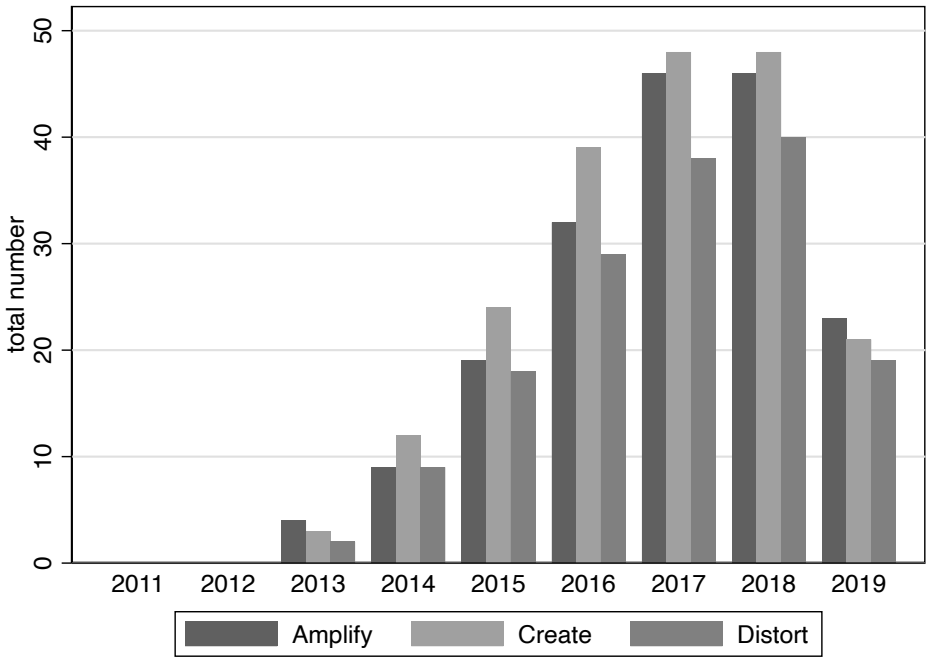
Panel B: Domestic influence efforts by year of origin



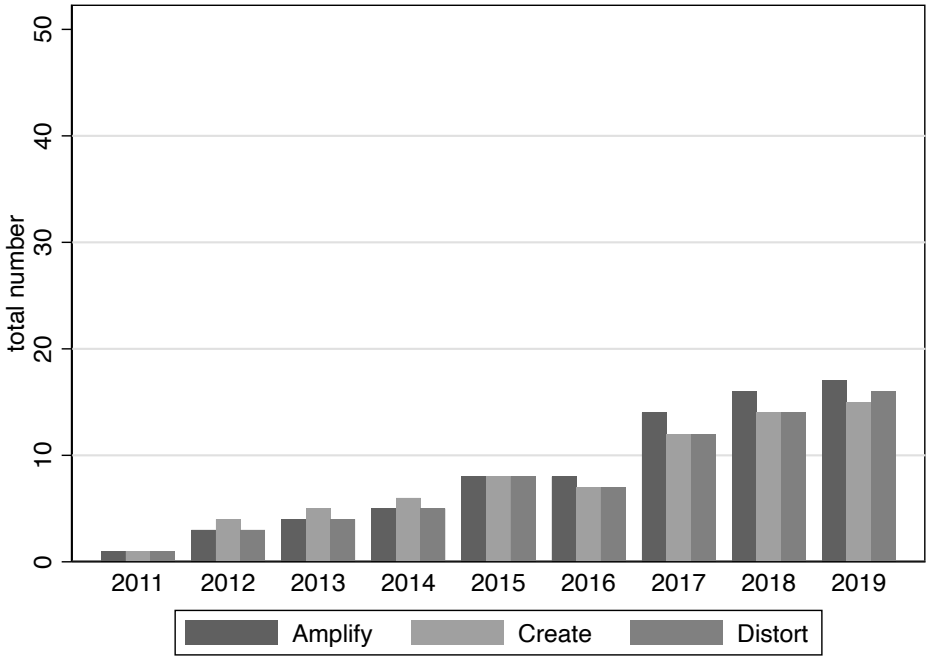
Panel A: This map includes all countries which have been targeted by FIEs, colored according to the number of attacks. For cases attacking multiple countries simultaneously, we have included all known targets, generally derived from Facebook investigations. Countries falling into the ≥ 5 category are the United States (21 FIEs), the United Kingdom (7 FIEs), and Libya (5 FIEs). *Panel B*: Countries in this map are colored according to the earliest known year in which domestic influence efforts (DIEs) were active. For countries with multiple DIEs, coloring reflects the start year of the earliest DIE.

Figure 3: Approach

Panel A: Foreign influence efforts



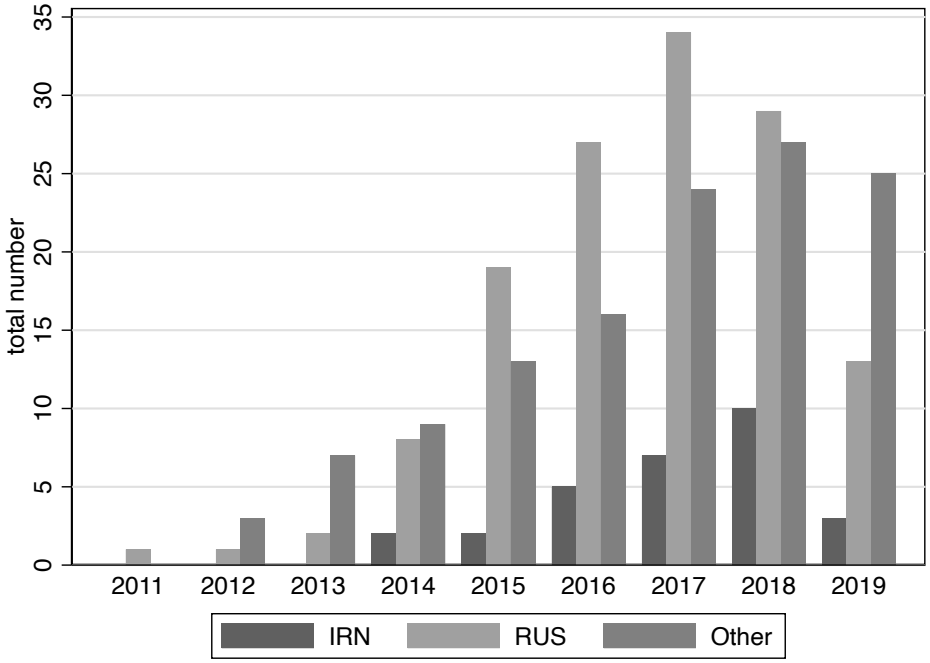
Panel B: Domestic influence efforts



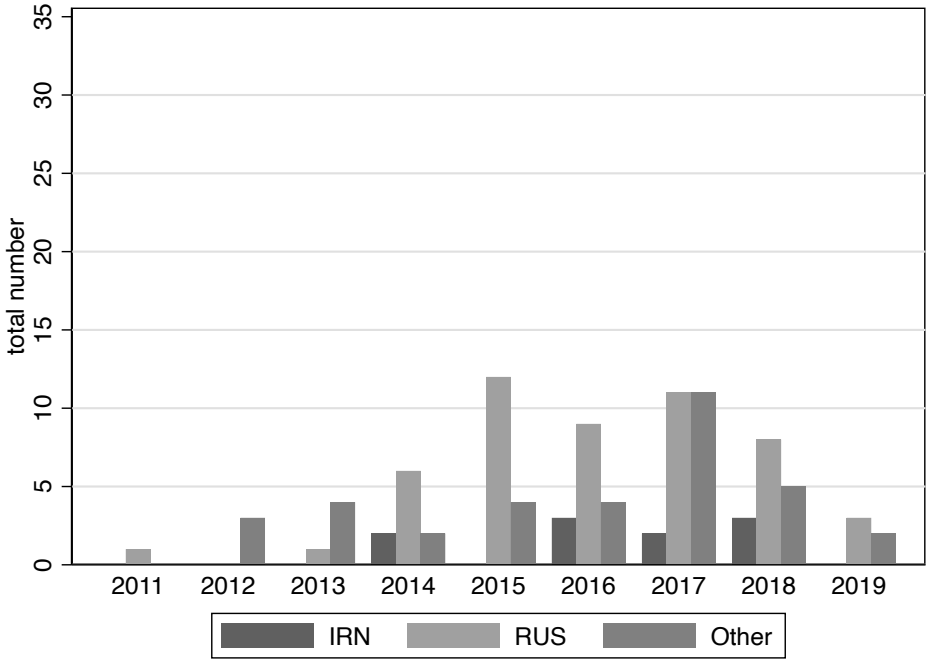
Panel A (B) shows the total number of foreign (domestic) influence efforts (FIEs) (DIEs) per approach and year. Number of FIE is 76 and DIE is 20, for a total number of 96 IEs

Figure 4: Origin of Influence Efforts

Panel A: Ongoing year



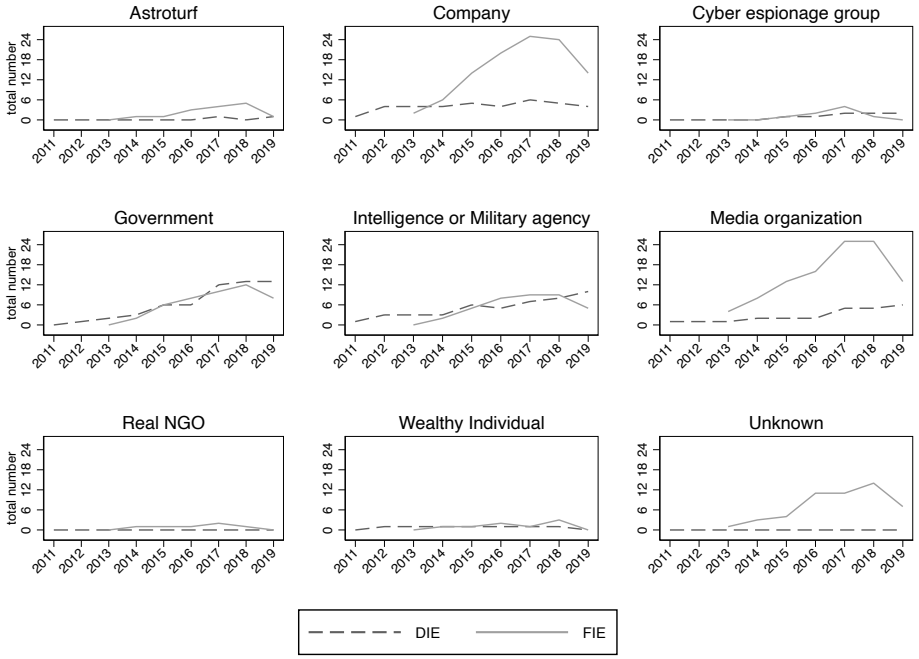
Panel B: Starting year



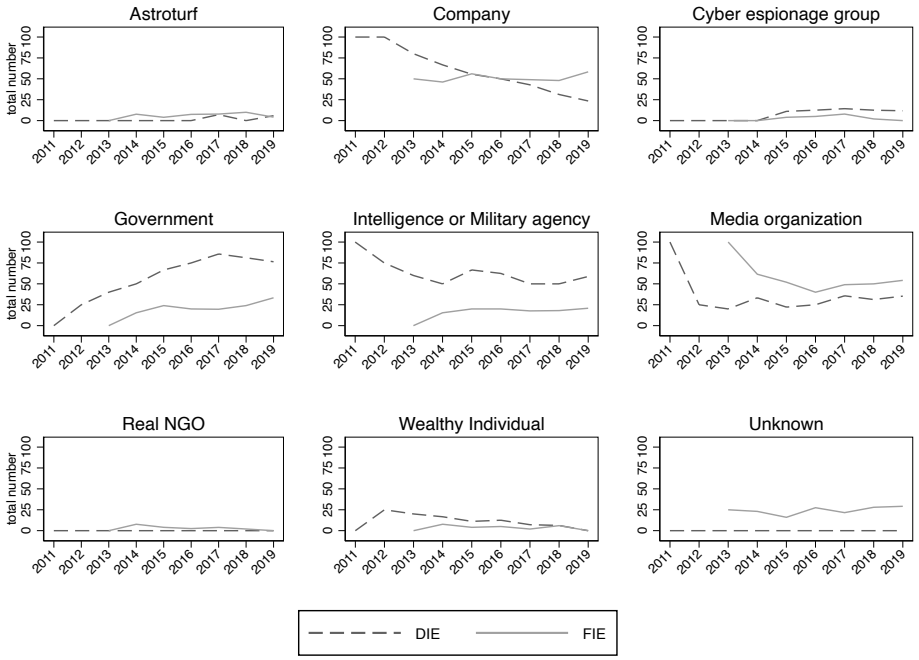
Panel A shows the total number of ongoing influence efforts (IEs) by year depending on the origin of the attack. Panel B shows the number of IEs initiated each year by country. The total number of FIEs is 76 and DIEs is 20, for a total number 96 IEs. The category *other* includes: China, Cuba, Ecuador, Egypt, Honduras, Indonesia, Mexico, Malta, Myanmar, Pakistan, Puerto Rico, Saudi Arabia, Sudan, Tajikistan, Turkey, United Arab Emirates, Venezuela, Zimbabwe, and Unknown.

Figure 5: Actors

Panel A: Total number of attacks per actor



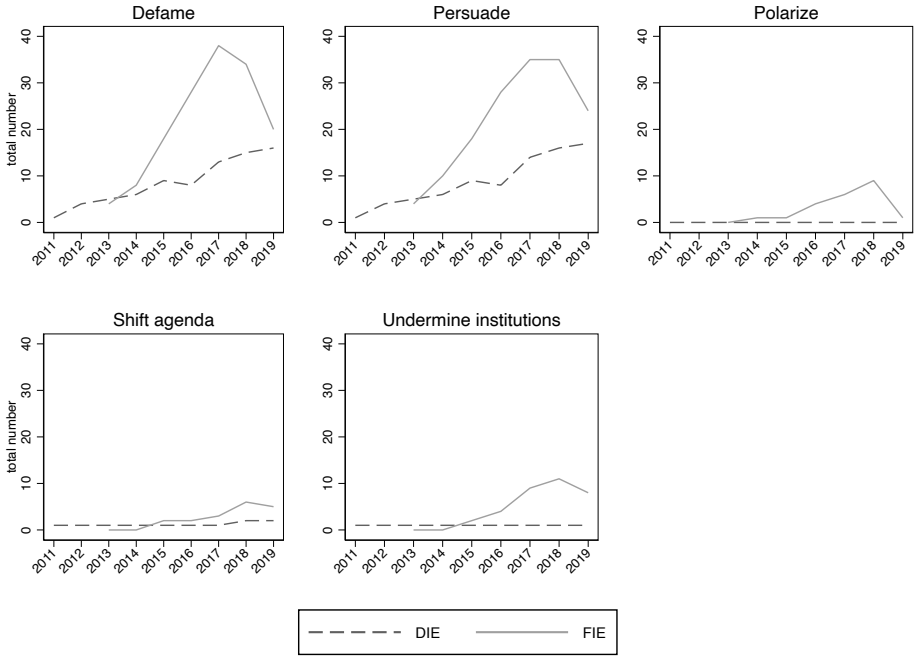
Panel B: Share of attacks involving actors



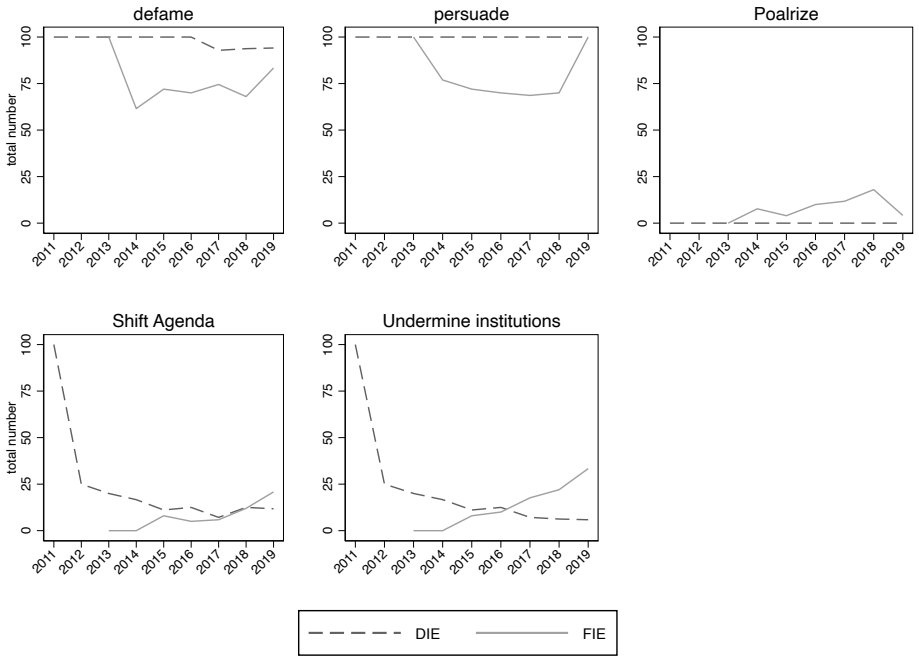
Panel A shows the total number of influence efforts (IEs) divided into foreign influence efforts (FIEs) per actor and domestic influence efforts (DIEs) per actor. Panel B presents the share of total efforts made by a particular actor per year. For example, the total number of FIEs using a Company in 2014 divided by the total number of cases in the same year. Each category is not mutually exclusive.

Figure 6: Strategy

Panel A: Total number of attacks per strategy



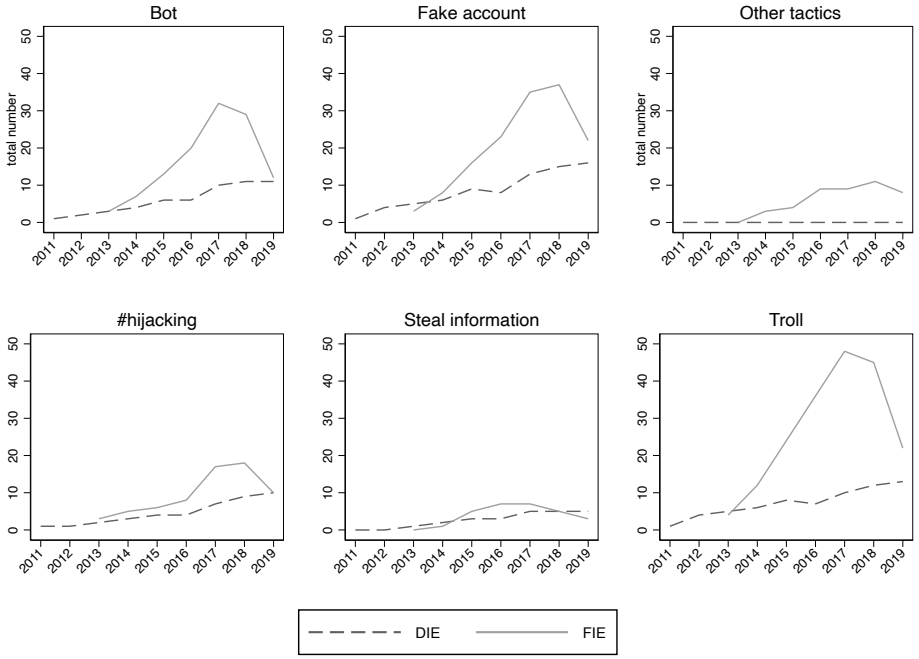
Panel B: Share of attacks involving strategies



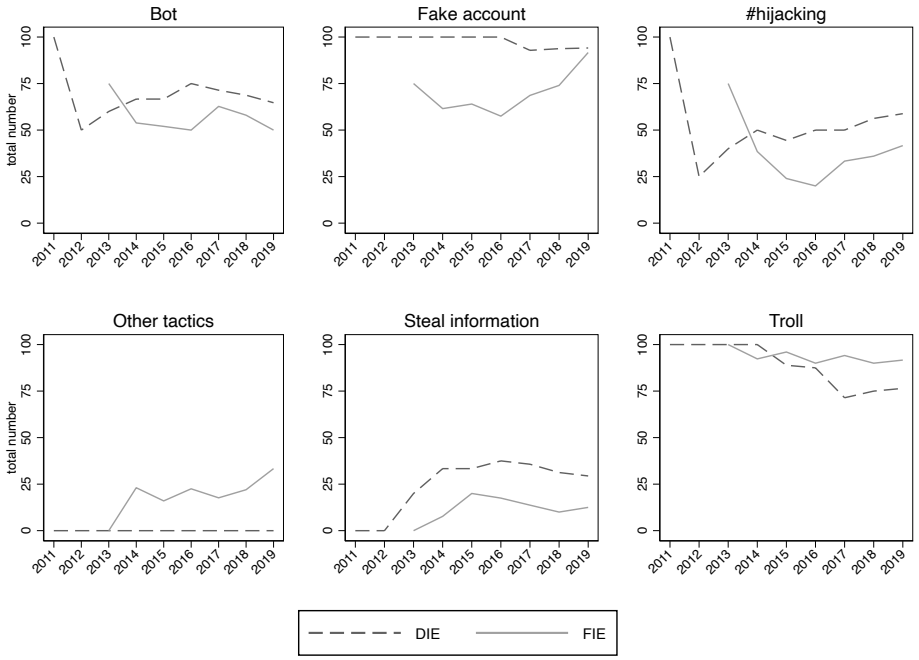
Panel A shows the total number of influence efforts (IEs) divided into foreign influence efforts (FIEs) per strategy and domestic influence efforts (DIEs) per strategy. Panel B presents the share of total efforts made by a particular strategy per year. For example, the total number of FIEs using a polarization in 2014 divided by the total number of cases in the same year. Each category is not mutually exclusive.

Figure 7: Tactic

Panel A: Total number of attacks



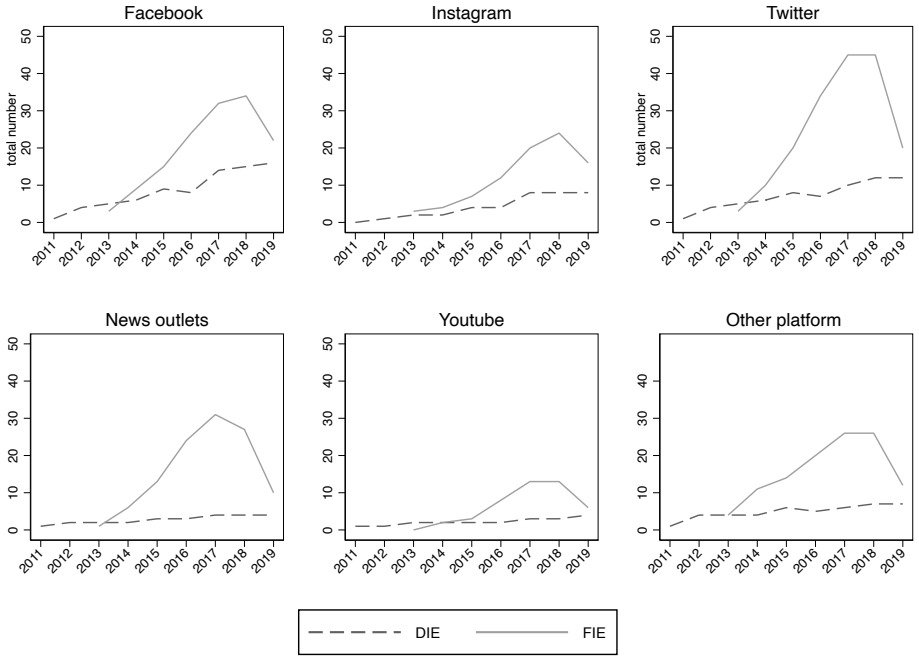
Panel B: Share of attacks involving tactics



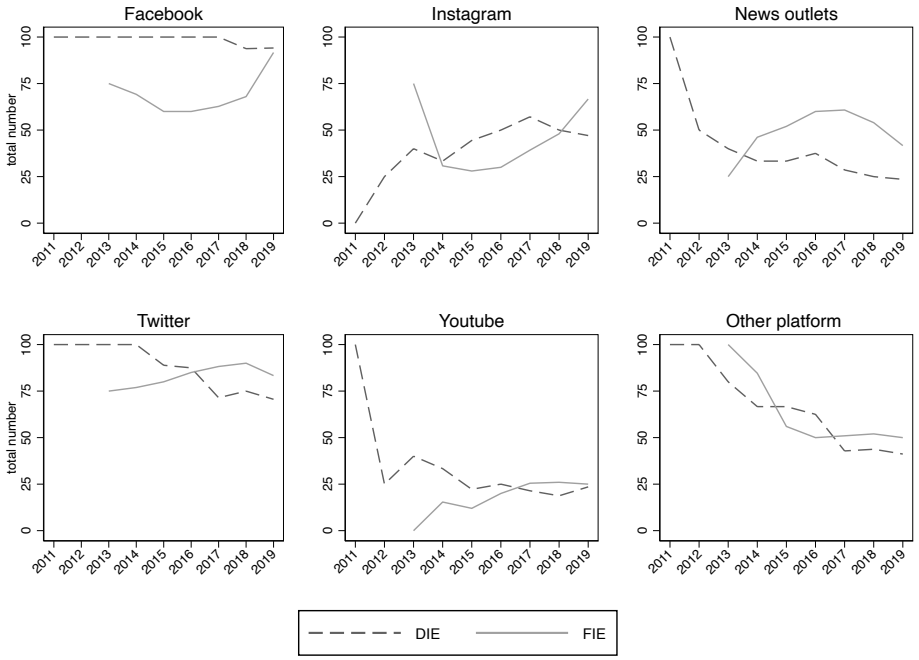
Panel A shows the total number of influence efforts (IEs) divided into foreign influence efforts (FIEs) per tactic and domestic influence efforts (DIEs) per tactic. Panel B presents the share of total efforts made by a particular tactic per year. For example, the total number of FIEs using a trolls in 2014 divided by the total number of cases in the same year. Each category is not mutually exclusive.

Figure 8: Platform

Panel A: Total number of attacks per plarform



Panel B: Share of attacks involving platforms



Notes: Panel A shows the total number of influence efforts (IEs) divided into foreign influence efforts (FIEs) per platform and domestic influence efforts (DIEs) per platform. Panel B presents the share of total efforts made by a particular platform per year. For example, the total number of FIEs using a Facebook accounts in 2014 divided by the total number of cases in the same year. Each category is not mutually exclusive. Each category is not mutually exclusive. *Other platforms* category includes email, Google, fake websites, Line, other media which includes radio, TV, and newspapers, Reddit, Whatsapp, and Wikipedia.

A Codebook

Table A-1: Codebook

Variable	Definition	Example
		Master
Serial number	Four-digit code showing the order in which we found the observations.	0001 is the first identified effort against a country. The serial number starts again from 0001 for a new targeted country.
Targeted country	Country being attacked (use the International Standards Organization (ISO) 3-digit alphabetic codes). Select MUL (multiple targeted countries) when the political goal targets more than one country. Select UNK when the targeted country is unknown.	i) Russia operated an influence effort during the Crimea referendum (Ukraine) in 2014, the U.S. elections in 2016, the Brexit referendum in 2016, and France's elections in 2017. ii) Facebook removed pages aiming to amplify content from the Kremlin's media agency. The Facebook accounts represented a systematic campaign to spread Russian content across 13 countries in Central Asia (i.e. MUL).
Attacking country	Country planned and/or ordered the attack. Select MUL when there is evidence of a coordinated attack (e.g. using the same firm) with the same political goal from two or more countries. Select UNK when the attacking country is unknown.	i) Russia hired people in Macedonia to produce fake news targeting the U.S. The attack is coded as RUS (for Russia), not MKD (for Macedonia). ii) After Sudanese soldiers massacred protesters in June 2019, a social media campaign was launched by Egypt together with the United Arab Emirates (UAE). An Egyptian digital marketing company called New Waves as well as a UAE company called Newave were paid to spread organic-looking pro-military messages on Facebook, Twitter, Instagram and Telegram (i.e. MUL).
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, e.g. Brexit, Elect Donald Trump, etc. Include citations for each article or source of information, e.g. (Karan, Kaul and Nimmo, 2019).	i) Supporting a specific individual or party in an election in a foreign country. Changing U.S. policy in Syria/Ukraine/Balkans/etc. ii) Undermine trust in the political system. iii) With Brexit, the political objective was to get the UK to vote to leave the EU. iv) With many 2016 election efforts in the U.S., the goal was to get President Trump elected or to foster support for Roy Moore's re-election campaign in the Sep. '17 special election in Alabama.

	Time	
Starting month	The earliest month where the attack started (code using numbers e.g. write 1 for January).	The earliest attack was in January.
Ending month	The latest month where the attack was made (code using numbers e.g. write 3 for March).	The latest attack seen was in March.
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.
	Actor	
Astroturf	Equal to 1 when a false organization or social movement is being created as part of the attack.	Philando Castile was shot by a police officer. In response, the Black Lives Matter movement organized a protest in front of the governor's mansion in Minnesota, according to Mica Grimm, an activist in this group. At the same time, a mysterious group used the death of Castile to create a movement called Don't Shoot and organized protests outside the police department where the officer who shot Castile 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 or company (e.g. Yevgeny Prigozhin) orders or directs operations to influence political decisions in a foreign country in pursuit of corporate goals (e.g. Internet Research Agency (IRA) is a Russian company based in Saint Petersburg).	The IRA is a company working for the Russian state. Yevgeny Prigozhin is a Russian businessman with ties to Russian president Vladimir Putin. Prigozhin controls "a network of companies," including three accused of interference in the 2016 United States elections. Prigozhin, his companies and associates face economic sanctions and criminal charges in the United States and are considered to have carried out various influence efforts.

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 included in the Fireye list and publicly linked to a Russian intelligence agency, creates websites to steal information from conservative groups which criticized U.S. President Donald Trump.
Media organization	Equal to 1 when one of the actors in the effort is an established media organization, with an installed capacity in terms of employment and buildings. It is not a news web page working for a short period of time or closed after the influence effort concludes.	i) RT (formerly Russia Today) is a Russian International television network funded by the Russian government. RT is directed at audiences outside of Russia, with content produced in languages including English. ii) Macedonian media attorney Trajche Arsov created the media organization called usapoliticstoday.com to spread fake news about the elections in the U.S.
Intelligence/Military agency	Equal to 1 when attack conducted by an intelligence or military agency of a country or a directly controlled subsidiary (e.g. Main Intelligence Directorate of the General Staff (GRU)).	i) Bots from the Internet Research Agency "troll army" amplified the hashtag #Brexit over two months to encourage voting in favor of Brexit. Press reports suggest this activity was directed by the Main Intelligence Directorate of the General Staff GRU. ii) Fake accounts associated with the Russian oligarch Yevgeny Prigozhin as well as the Wagner Group — a private Russian military contractor — began to promote pro-Haftar and pro-Libyan National Army (LNA) narratives in Libya in late 2018.
Government	Equal to 1 when politicians order the influence effort or when they are part of the strategy. Coded 1 for DIE if there is reliable evidence that government agencies were involved.	The Grand Jury for the District of Columbia said the Russian Federation operated a military intelligence agency called the Main Intelligence Directorate of the General Staff. This is evidence that a foreign government was the actor of this influence effort.
Real NGO	Equal to 1 when the attack is executed by an activist group that is neither government nor a for-profit corporation. This category includes Wikileaks, Openleaks, AJTransparency, Globalleaks.com, Balkanleaks.eu, etc.	Maria Katasonova launched what she referred to as a Twitter "flash mob" under the hashtag #dislikeMacron. She is a Russian nationalist who works for a high-ranking politician and is part of a Russian patriotic artists' collective, heading up the "Women for Marine" movement.

Wealthy individual	Equal to 1 when a wealthy individual orders a campaign to influence political decisions in a foreign country. Equal to 0 when the wealthy individual mentioned is the CEO of a company conducting the campaign.	Russian businessmen created media propaganda to reduce the price of land in South Africa, where they were interested in buying and building a nuclear plant.
Unknown	Equal to 1 when there are hints about other actors involved, but there is not enough supporting material to classify actors into one of the categories.	A Facebook spokesman said the company had not found sufficient evidence to link an operation to the governments of Egypt or the United Arab Emirates, but there were suggestions of such a link.
	Attacker	
Attacking organization	Name of the primary organization responsible for the attacks. Code Actor 1 (name of the attacker), Actor 2 (name of the attacker), and so on. Write Actor 1 (Unknown) when there is insufficient information about the attacker identity.	Intelligence agency (GRU), Intelligence agency (Project Lakhta), Company (IRA). IRA is widely considered to be the main Russian organization which produced propaganda in favor of Donald Trump during the 2016 Presidential Election.
Mentioned personae	Name of websites, Facebook profiles, Twitter accounts or people which are mentioned in sources as possible creators and amplifiers of misinformation and fake news. Write name (brief description about people mentioned) and Unknown when there is insufficient information about the attacker identity.	Yevgeny Prigozhin (Russian oligarch). U.S. investigations found that Prigozhin was a key actor in Russian efforts to interfere in the 2016 U.S. elections.

Strategy		
Defame	Equal to 1 when there is a direct attack against a person, intended to discredit him or her.	Trolls from the Internet Research Agency (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 in which the goal appears to be to directly shift political views about an issue or actor in an identifiable direction (the goal is to shift 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 effort aims to change the agenda (putting something new on the political agenda).	As an exporter of energy, Russia desires to eliminate or mitigate the American energy threat, and to do so by influencing social media users, American voters, and public officials. For this goal, they exploited media platforms such as Facebook and Instagram by sharing images related to Native American social and political issues. In the case of building the Dakota Access Pipeline, for example, Russia started an influence effort to stop this project saying that Native Americans would be in danger because the Pipeline would cross their territory.
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 the attack involves emails with misinformation or emails attempting to steal 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. 0 otherwise.	Facebook, Twitter and Google have all identified the Internet Research Agency as a prime source of provocative posts on divisive American issues, including race, religion, gun laws and gay rights, particularly during the 2016 presidential election.
Google	Equal to 1 when an attack involves Google platforms. 0 otherwise.	Facebook, Twitter and Google have all identified the Internet Research Agency as a prime source of provocative posts on divisive American issues, including race, religion, gun laws and gay rights, particularly during the 2016 presidential election.
Fake websites	Equal to 1 when the 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 on Facebook or Reddit.	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 attack involves activity on Instagram. 0 otherwise.	The official Instagram account of Angela Merkel, Chancellor of Germany, was the target of a coordinated attack from Russian trolls, who posted negative comments on every picture in the account except for those ones including Vladimir Putin.
Line	Equal to 1 when an attack involves activity on Line. 0 otherwise.	Line was used to falsely claim that the central government of China was planning to impose draconian restrictions on pensioners.
News outlets	Equal to 1 when the attack involves the creation of news websites. This category does not include news pages on Facebook or Reddit.	Trolls in Macedonia created news websites against the Hillary Clinton campaign during the U.S election.

Other media	Equal to 1 when an attack involves other media such as TV, newspapers and radio.	News providers in Ukraine that had a Russian shareholder or partner tended to be more restrained in their criticism of Russia than comparable news providers without such support from Moscow.
Reddit	Equal to 1 when the attack involves Reddit. 0 otherwise.	Reddit accounts were involved in spreading messages against Hillary Clinton and in favor of Donald Trump during the 2016 elections.
Twitter	Equal to 1 when the attack involves Twitter. 0 otherwise.	Twitter released data from more than 10 million tweets that had been circulated by propaganda farms and their associated puppet accounts.
WhatsApp	Equal to 1 when the attack involves WhatsApp. 0 otherwise.	Using WhatsApp, Russia spread rumors saying that Hillary Clinton was in favor of White Americans.
Wikipedia	Equal to 1 when an attack involves manipulating results on Wikipedia.	Russian Trolls created 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. 0 otherwise.	Iranian Trolls created 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 created fake social media accounts and wrote blog posts meant to sow divisions in the U.S. and turn Russians against Americans.
Miscellaneous information	Relevant information about classification of any variables.	Melvin Redick is one of the accounts Russia used to spread the emails stolen from Hillary Clinton campaign. It is not clear if he is a real person or not.

Source	Provide link to where news and media sources related to the influence effort can be found. Include at least three sources per influence effort	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 the individual (Trolls or Bots) work to promote specific content, whether real or fake.	A suspected network of 13,000 Twitter Bots retweeted and shared 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, a 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 on social media, though the woman targeted in the attack denied the claim.

Tactic		
Bot	Equal to 1 when an automated account is used, e.g. to 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 employs fake accounts of fictitious personas. Equal to 2 if there is misuse of a real person's identity (e.g. creation of an account in someone's name that is not controlled by them). Equal to 3 if the effort includes both fictitious personae and the misuse of real identities. 0 otherwise. Record in notes if ambiguous.	@SouthLoneStar was a fake account used for amplifying racist messages in the Brexit election. FB reported they took down more than 1B fake accounts in 2018. As an example of fake accounts 3, in the Iranian efforts to influence U.S. policy, Iran both created fake social media personas and replicated accounts for actual U.S. House of Representative candidates.
Hashtag hijacking	Equal to 1 when attackers use hashtags 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 tactics are neither using trolls, bots, micro-profiling, Hashtag hijacking, stealing information, nor fake accounts.	Russia uses TV programing to encourage people in Crimea to vote in favor of becoming part of Russia.
Stealing information	Equal to 1 when a person tries to steal information from emails, personal websites or group pages. 0 otherwise.	Phishing emails sought to access conversations between Hillary Clinton and her team during the 2016 U.S. 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 across Russia.
		Topic (selected list)
Economic issues	Equal to 1 when an attack exploits an economic issue.	Russian trolls used the Keystone XL pipeline in Canada to generate division in the country.
Gun control	Equal to 1 when an attack exploits debates over gun control.	Russian media organization created posts claiming that Sweden sells weapons to the Islamic state.
Immigration	Equal to 1 when an attack exploits propaganda against immigration.	In the Brexit Referendum, trolls posted several tweets claiming that 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 used the NATO's military exercises in Estonia to claim that the country was preparing an attack against Russia.
Political party	Equal to 1 when an attack exploits politicians and political parties.	Russian trolls attacked Hillary Clinton while simultaneously supporting 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 Influence Efforts

This section summarizes key details of all 96 influence efforts included in the database. The references and details are not exhaustive. For full details please consult data at this link. Each IE has a unique identifier which concatenates 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 IE. AUSRUS0001, for example, is the first FIE we identified in which Australia was targeted by Russian actors. For DIE, the code is simplified since the targeted country is equal to the attacking country. CHN0001, for example, is the case in which the Chinese government sought to discredit prominent dissidents in its territory. 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.

The following annotated lists are organized by this code. Sub-section B.1 (B.2) presents the event description for 76 (20) foreign (domestic) influence efforts.

B.1 Annotated List of Foreign Influence Efforts

ARMRUS0001. Targeted country **Armenia**. Attacking country **Russia**. Political goal **Discredit Armenia's 2017 parliamentary elections**:

In 2017, a Russian-led Twitter bot campaign sought to undermine faith in Armenia's parliamentary elections by promoting a narrative of interference by the United States. The 2017 election was the first vote under a new law which marked the transition towards a parliamentary system of rule (Nimmo & Barojan 2017). Initially, the circulation of a fake letter from the United States Agency for International Development (USAID) by tens of Twitter users posting in Russian was debunked due to several grammatical and spelling errors as well as the association with a gmail account (Nimmo & Barojan 2017). The letter supposedly provided instructions on how to meddle in Armenia's election. A corrected fake letter was then shared on pastebin.com on March 29, 2017 and amplified by Twitter bots. An investigation of the Russian bot network showed that all accounts were created around the same time, had very few followers, and tweeted similarly worded messages linked to the USAID letter (Nimmo & Barojan 2017). The Russian-language profiles frequently made use of the hashtag #armvote17 to promote the narrative (Mackinnon 2017). Twitter attempted to remove these Russian accounts a day before the election, but inadvertently took down the accounts of several prominent Armenian journalists (Khana 2017).

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 Defense Forces (ADF) were also confronted by Russian military 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).

CAFRUS0001. Targeted country **Central African Republic**. Attacking country **Russia**. Political goal **Support President Faustin-Archange Touadéra and criticize France's involvement in the Central African Republic**:

In 2019, Facebook identified a network of 13 pages linked to Russian oligarch Yevgeny Prigozhin which sought to appear indigenous to the Central African Republic (CAR) and influence the CAR's domestic politics (Grossman et al. 2019). The majority of these pages purported to provide local news and often focused on Russia's positive role in the CAR or amplified pro-President Touadéra stories. Further, these pages frequently denigrated France and the UN, accusing France of hindering the CAR's development and trying to "recolonize" (Grossman et al. 2019). This effort is consistent with the Kremlin's foreign policy initiatives, as Russia has aimed to compete with France's influence and provisioning of resources in the CAR since at least 2017 (Ross 2019). The Facebook network occasionally published pro-opposition content, but the vast majority of material supported Russia's actions in the CAR and tried to shape local political discourse in favor of the government.

In addition to social media interference, Wagner Group, a Russian private military contractor, has been active in the CAR since 2017, acting as a security detail for President Touadéra or guarding Russian mining sites (Reynolds 2019). A Prigozhin-linked mining company also established the radio station Radio Lengo Songo in the CAR (Searcey 2019), and the account behind one of the inauthentic Facebook pages claimed to be a journalist from this station (Grossman et al. 2019).

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

Russian-based groups used social media to promote Catalonia's independence referendum 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).

ESPUNK0001. Targeted country **Spain**. Attacking country **Unknown**. Political goal **Support Catalonia independence in 2017**:

Venezuelan Twitter accounts sympathetic to the Chavista regimes of Nicolás Maduro and Hugo Chávez helped to amplify a Russian disinformation campaign supporting the 2017 Catalan independence movement (Lesaca 2017). The vast majority of social media activity related to Catalonia came from automated networks, and approximately one-third of analyzed messages originated in Venezuela (Díaz 2017).

The Venezuelan social media effort sought to undermine confidence in Spanish law enforcement and promote pro-independence narratives, primarily by amplifying articles from state-linked Russian media outlets RT and Sputnik (Lesaca 2017). This suggests that the campaign originated in Russia and employed a Venezuelan bot network, however, there is no evidence that the Venezuelan bots worked on behalf of a particular government or entity. A small amount of polarizing content content also criticized the movement, highlighting how Catalonia's independence would hurt the Spanish economy. Some content was unrelated to Russian sources, with accounts frequently pushing the hashtag #VenezuelaSalutesCatalonia (Alandete 2017).

ESPUNK0002. Targeted country **Spain**. Attacking country **Unknown**. Political goal **Promote the far-right Vox party in Spain preceding the 2019 election**:

Leading up to Spain's parliamentary elections in April of 2019, researchers identified a network of Twitter bots and inauthentic accounts promoting Islamophobic content and messages in favor of the far-right Vox political party (Peinado 2019). The accounts had produced 4.4 million pro-Vox tweets since 2018 and Islamophobic tweets dating back to 2017. Though the origins and funding of this network are unclear, the accounts were originally established to attack the Maduro government in Venezuela but began focusing on Spain following a 2017 terrorist attack (Applebaum 2019). The network has also consistently promoted Venezuelan opposition youtuber Alberto Franceschi, a vocal supporter of Vox. In addition to Twitter, disinformation supporting Vox or Vox's political agenda frequently spread via WhatsApp and Facebook preceding the 2019 election (Smith 2019).

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 incident included a cache of documents 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, 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 was extensively promoted on Twitter by bots (Volz 2017). While there are sources saying that Russia is behind the attack, there is no concrete evidence to prove the claim. 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).

GBRIRN0003. Targeted country **Great Britain**. Attacking country **Iran**. Political goal **Undermine British monarchy**:

On May 28, 2019, Facebook took down 92 accounts, pages, and groups linked with Iran, some of which curated organic-looking content for the U.K. (Gleicher 2019*g*). These personas criticized the supposed corruption of the royal family, contrasted with poverty and health issues (Karan, Kaul & Nimmo 2019). Some accounts photoshopped images of the royals or overlayed pictures with comments about unreasonable costs on pages made to look as if they originated in the U.K. Personas sometimes posed as journalists to conduct interviews with made up UK-based individuals. The Facebook takedown closely followed and was related to Twitter's May 2019 removal of 4,800 Iranian-linked accounts (BBC 2019*b*).

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.

GBRRUS0004. Targeted country **Great Britain**. Attacking country **Russia**. Political goal **Inflame Brexit tensions in 2019**:

Six weeks prior to the UK's general election in December 2019, the Reddit account Gregoratior leaked unredacted documents from UK-US trade discussions which benefited the political agenda of the Labour Party and stoked Brexit tensions (Nimmo 2019). This campaign is thought to be associated with the "Secondary Infektion" Russian information operation which has been active since 2014. According to Reddit, additional accounts manipulated the votes on this original post to amplify the leak. Suspected Russian "burner accounts" also reposted the documents on German and English websites, while the Twitter user @gregoratior began amplifying the post in an effort to catch the attention of UK politicians and media figures. The documents spread to fringe platforms such as 4chan, and accompanying posts contained English errors characteristic of non-native speakers (Wendling 2019). Eventually, the leak was picked up by mainstream media in the UK, and Labour leader Jeremy Corbyn presented the documents at a press conference (Furlong 2019).

To date, researchers have been unable to identify any central entity behind the Second Infektion operation. Similar social media campaigns have focused on topics including Ukraine, the US, European disunity, Russian dissidence, and anti-Islamic sentiment (Nimmo, Francois, Eib, Ronzaud, Ferreira, Hernon & Kostelancik 2020).

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 September 2017 German Federal Election began in May of that year. Material from German-language news outlets connected to the Russian government—such as RT Deutsch, Sputnik Deutsch, and News-Front 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**:

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).

LBYRUS0001. Targeted country **Libya**. Attacking country **Russia**. Political goal **Influence domestic Libyan politics**:

A network of Russian accounts sought to interfere in Libya's domestic politics in favor of Russian foreign policy priorities. In late-2018 fake accounts associated with the Russian oligarch Yevgeny Prigozhin as well as the Wagner Group — a private Russian military contractor — began to promote pro-Haftar and pro-Libyan National Army (LNA) narratives in Libya (Grossman et al. 2019). In addition to creating pro-Haftar, anti-Qatar, and anti-Turkey pages, Russian actors also produced unique content nostalgic for Muammar Gaddafi and promoting the political prospects of his son and Haftar competitor, Saif al-Islam Gaddafi. It is not clear whether Russian accounts promoted both Haftar and Gaddafi in an effort to maintain options or to identify persuadable Gaddafi supporters. All of these Facebook pages were at least partially managed by people in Egypt to obscure Russian involvement. Prigozhin's group further established a physical Libyan newspaper called Voice of the People to create pro-LNA stories and gained significant control of various Libyan TV networks (Grossman, H. & DiResta 2020). Beyond interfering in Libyan news and social media, Russian mercenaries fought alongside the LNA.

LTURUS0001. 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.[37]

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

[37]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).

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.

MDGRUS0001. Targeted country **Madagascar**. Attacking country **Russia**. Political goal **Promote pro-Russia political candidates and spread pro-Russia content**:

Leading up to the 2018 presidential election in Madagascar, Russian operatives associated with oligarch Yevgeny Prigozhin and the military contractor Wagner Group sought to promote various candidates through the use of social media manipulation and bribery (Grossman et al. 2019). Initially, the network backed a pro-Russian candidate, but pivoted to support Andry Rajoelina as he became the frontrunner (Schwirtz & Borgia 2019). Several Facebook pages associated with the campaign purported to be local news outlets, posting in support of President Rajoelina following his inauguration. The news page and associated website Afrique Panorama also posted partisan African content consistent with Russia's foreign policy aims (Grossman et al. 2019). One page claimed to be the official account for a parliamentary candidate until he lost an election in March 2019.

MKDRUS0001. Targeted country **Macedonia**. Attacking country **Russia**. Political goal **Hinder Macedonia's accession to NATO**:

In 2018, Twitter accounts linked to Russia attempted to interfere in a Macedonian referendum on changing the country's name and thus inhibit Macedonia's accession to NATO (SBSNews 2018). Macedonia's name has fueled a long dispute with Greece, preventing Macedonia from joining the NATO alliance. Destabilizing NATO and maintaining influence over the Balkans are significant foreign policy initiatives for Russia (Santora & Barnes 2018). The social media campaign cannot be definitively attributed to the Russian state, but is consistent with the Kremlin's political agenda.

Leading up to the day of the vote, thousands of fake Twitter and Facebook accounts with the hashtag #Bojkotiram, meaning "boycott," flooded social media platforms in Macedonia. This campaign aimed to reduce voter turnout below 50 percent – the minimum required to make the referendum binding. Some of the accounts tried to stoke tensions between Macedonia's Slav majority and the Albanian minority (Squires 2018). In addition, an anonymous Twitter account associated the referendum with fascism, posting memes that made use of Nazi symbols (Petreski 2018).

Macedonia formally changed its name and signed the Prespa Agreement with Greece in June 2018. Macedonia became a formal NATO member in March 2020.

MOZRUS0001. Targeted country **Mozambique**. Attacking country **Russia**. Political goal **Support Filipe Nyusi in 2019 Mozambique presidential election**:

A network associated with Russian oligarch Yevgeny Prigozhin interfered in Mozambique's 2019 presidential elections on behalf of incumbent candidate Filipe Nyusi from the Frelimo party (Grossman et al. 2019). Prigozhin has close ties with Russian President Putin. The group created fake Facebook pages to amplify Nyusi support, praise the government's efforts to fight an Islamist insurgency, and defame the opposition Renamo party. Another entity associated with Prigozhin — the International Anticrisis Center —

conducted an illegal poll and amplified results supposedly predicting a victory for Nyusi (Lister & Shukla 2019).

MULCHN0001. Targeted country **Multiple**. Attacking country **China**. Political goal **Promote pro-China narratives amongst the Chinese diaspora**:

In 2019, Twitter released data on a series of removed accounts linked to state actors from the People's Republic of China. The network consisted of fake accounts and suspected bots which promoted content consistent with the interests of the Chinese government. Accounts in the network were created as early as 2007 and acted as spam or marketing bots, but linguistic and behavioral data suggest the accounts were purchased and repurposed by actors in China around mid-2017 (Uren et al. 2019). From 2017 onward, tweets were primarily in Chinese and English, as well as Indonesian, Arabic, and several other languages. The self-reported locations of the accounts ranged around the world but concentrated in the United States and Europe. Prior to 2019, campaigns focused on defaming prominent Chinese dissidents such as Guo Wengui, a Chinese businessman who fled to the United States and frequently speaks about corruption in the Chinese government. An Australian Strategic Policy Institute (ASPI) report argues the network sought to "influence the opinions of overseas Chinese diasporas, perhaps in an attempt to undermine critical coverage in Western media of issues of interest to the Chinese government" (Uren et al. 2019). In 2019, the Twitter campaign turned its attention to disrupting the pro-democracy protests in Hong Kong, likely primarily targeting Hong Kong residents but also the international diaspora (Karan & Zhang 2019). Based on a dataset from April 2020, researchers found inauthentic Chinese social media accounts promoting pro-China narratives related to Taiwan, responses to COVID-19, and George Floyd protests in the United States (Wallis et al. 2020).

Consistent with the aim of influencing the overseas diaspora in favor of the Chinese government, state-owned news outlet China News Service contracted the Beijing-based marketing firm OneSight Technology Ltd. to bolster the outlet's Twitter following (Kao & Li 2020). Chinese state media outlets also spend significant amounts of money to enhance overseas viewership or purchase local media enterprises in other countries (Cook 2020).

MULEGY0001. Targeted country **Multiple**. Attacking country **Egypt**. Political goal **Influence Libyan politics within Libya and the region**:

In April of 2019, Libyan General Khalifa Haftar announced that the Libyan National Army (LNA) would pursue an offensive on the capital city of Tripoli. In the weeks preceding and following this announcement, disinformation campaigns originating in a variety of countries began promoting political narratives related to Libya, though it is not clear that these efforts were coordinated. Commercial bot networks from Egypt posted and amplified hashtags in support of Haftar, including accounts linked to a technology company called DotDev which has offices in Egypt and the UAE (FSI 2019). Elements of this campaign sought to influence public opinion within Libya. One suspected DotDev account impersonated a real LNA spokesperson, while another claimed to be "The Official page of General Khalifa Haftar."

In addition, Arabic-language Egyptian accounts targeted a regional audience with content in support of Haftar. For instance, the Egyptian Twitter account @MasterLocalZone, which previously participated in online campaigns supporting the Egyptian government,

congratulated followers on making a pro-Haftar hashtag the top hashtag in Egypt. Egyptian news outlets such as ElBalad amplified similar narratives (Kassab & Carvin 2019). Consistent with the political agenda of Egypt's government, this campaign also attacked Qatar for supporting terrorism in Libya, targeted the Muslim Brotherhood, and criticized Turkey. Pro-Haftar messaging dated as far back as 2013 and has continued with Haftar's subsequent efforts to seize power, with added emphasis on defaming Libyan Prime Minister Fayez al-Sarraj (Grossman, H., DiResta, Kheradpir & Miller 2020).

MULRUS0001. Targeted country **Multiple**. Attacking country **Russia**. Political 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 **Multiple**. Attacking country **Russia**. 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*d*).

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).[38]

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).

MULRUS0003. Targeted country **Multiple**. Attacking country **Russia**. Political goal **Spreading misinformation in Central Asia and amplifying Sputnik and TOK content**:

In January 2019, Facebook removed 289 Facebook pages, 75 Facebook accounts, and several Instagram accounts which originated in Russia (Satariano 2019). The pages' main objective was to amplify the content from two of Russia's state-backed media outlets, Sputnik and the video service TOK. Both outlets are associated with Rossiya Segodnya, the Kremlin's media agency (Aleksejeva et al. 2019*a*). The social media effort represented a systematic campaign to spread the content of the agency across 13 countries in Central Asia, namely Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, Armenia, Azerbaijan, Georgia, Moldova, Romania, Belarus, Estonia, Latvia, and Lithuania (Gleicher 2019*c*). Pages and accounts were linked to employees of Sputnik and frequently posted about topics like anti-NATO and anti-corruption sentiment. The social media content and personas were adapted for local audiences and obscured any connection to Rossiya Segodnya. In some cases, the accounts claimed to be people indigenous to the target country.

All of these pages shared content from Sputnik and TOK, and in total the network amassed 853,413 followers. This represented a significant increase in audience compared to Sputnik's official following across the Central Asian countries. Over one-quarter of the

[38]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).

pages were created in October 2017, with 32 produced in a single day. Moreover, some pages in the network cross-posted videos from Sputnik and TOK, indicating coordination (Aleksejeva et al. 2019*a*).

MULSAU0001. Targeted country **Multiple**. Attacking country **Saudi Arabia**. Political goal **Deny Saudi government responsibility for the murder of journalist Jamal Khashoggi**:

Twitter banned a network of accounts attempting to sow doubt regardin 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*c*). This FIE has "multiple" as the targeted country because the campaign targeted populations around the world that speak English and/or Arabic.

MULSAU0002. Targeted country **Multiple**. Attacking country **Saudi Arabia**. Political goal **Promote pro-Saudi narratives across Middle East and North Africa and defame Iran, Qatar, and Turkey, among others**:

In 2019, Facebook took down a network of accounts associated with the Saudi Arabian government which targeted countries across the Middle East and North Africa. The network created fictitious accounts and news pages purporting to be indigenous to countries including Iran, Qatar, and Turkey (Karan 2019). Content frequently focused on praising Crown Prince Mohammad Bin Salman and his "Vision 2030" reform plan as well as supporting the activities of the Saudi Armed Forces, particularly in Yemen. Other accounts sought to denigrate Turkish President Erdoğan following the killing of journalist Jamal Khashoggi in Turkey, to attack the Qatari royal family, and to undermine the Al-Jazeera news network and Amnesty International (Gleicher 2019*e*).

Facebook and Bellingcat (on whom Facebook relied for its investigation) found links to individuals working in the Saudi government, namely bin Salman's communications chief Saud al-Qahtani (NPR 2019). Research done by the DFRLab could not confirm this link, though the content of the takedown reflected the interests of the Saudi royal family (Karan 2019).

In addition, a 2019 Twitter takedown of accounts created by the state-backed Saudi Arabian digital marketing company Smaat promoted similar political narratives aligned with the Saudi Arabian government, though most Smaat content was commercial in nature (DiResta et al. 2019). Political accounts frequently focused on Khashoggi and criticizing the governments of rival countries Qatar, Turkey, and Iran. These accounts usually posted in Arabic and English but also Japanese, Russian, Spanish, and other languages (Gleicher 2019*e*, DiResta et al. 2019).

MULSAU0003. Targeted country **Multiple**. Attacking country **Saudi Arabia**. Political goal **Isolate Qatar diplomatically and economically**:

As early as April of 2017, a network of Twitter bots primarily originating in Saudi Arabia was established to criticize Qatar and Iran and praise President Trump prior to his visiting Riyadh (Chappelle 2018). In May of 2017, the Qatar News Agency (QNA) and its associated social media pages were hacked. A fake speech was attributed to Qatar's Emir in which he praised Iran as well as Islamist groups Hamas, Hezbollah and

the Muslim Brotherhood (Pinnell 2018). An Al Jazeera investigation linked the hack to Saudi Arabia, though US intelligence found evidence of senior UAE officials discussing the attack a day before it occurred (DeYoung & Nakashima 2017). Various countries including Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain used this fake story as a justification to break ties with Qatar and isolate the country diplomatically.

Twitter bots from Saudi Arabia used the hack as an opportunity to amplify anti-Qatar messaging and push hashtags critical of the Tamim regime (Nimmo 2018*c*). Saudi Arabian social media accounts claiming to be based in Qatar also promoted negative content to give the impression that Qataris wanted a change in leadership, and this trend was reported by Saudi Arabian media outlets such as Al Arabiya (Chappelle 2018). According to Facebook, disinformation efforts targeting Qatar extended beyond the 2017 hack and have been linked with government-associated officials in Saudi Arabia. Although a number of states participated in the attack on Qatar, there is no clear evidence that Saudi Arabia coordinated with other countries.

MULSAU0004. Targeted country **Multiple**. Attacking country **Saudi Arabia**. Political goal **Influence Libyan politics within Libya and the region**:

In April of 2019, Libyan General Khalifa Haftar announced that the Libyan National Army (LNA) would pursue an offensive on the capital city of Tripoli. In the weeks preceding and following this announcement, disinformation campaigns originating in a variety of countries began promoting political narratives related to Libya, though it is not clear that these efforts were coordinated. Twitter accounts from Saudi Arabia were amongst the first to amplify certain pro-Haftar hashtags, and this campaign is suspected to have involved the use of Twitter bots (DemocracyReporting 2019). Saudi news oulets such as Al Arabiya also promoted stories in support of Haftar's campaign.

In addition, campaigns linked with Saudi Arabia have aimed to influence domestic public opinion in Libya. In 2019 Twitter took down a number of accounts attributed to Saudi Arabia, the UAE, and Egypt which falsely claimed to be based in Libya. This network frequently used the hashtag "Sarraj the traitor of Libya," targeting Libyan Prime Minister Fayez al-Sarraj (Grossman, H., DiResta, Kheradpir & Miller 2020). These accounts also amplified the tweets of Libyans who were supportive of the LNA. The Saudi Arabian disinformation network could not be definitively linked to government actors, though the narratives it promoted reflect Saudi Arabia's political interests and were closely aligned with disinformation campaigns originating in the UAE and Egypt.

MULUAE0001. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Promote pro-United Arab Emirates (UAE) narratives in Iran, Qatar, and Turkey, among others**:

Over the course of 2019, a number of social media takedowns involved marketing firms and fake accounts originating in the United Arab Emirates (UAE). In addition to attacking regional rivals such as Iran, Qatar, and Turkey, and seeking to influence domestic politics in Libya, these networks consistently promoted the government and role of the UAE abroad. In a network of Twitter accounts studied by the DFRLab in July of 2019, fake accounts frequently amplified positive messaging about the UAE and attacked the Human Rights Watch Executive Director after he criticized the UAE's stifling of free speech (Carvin & Kassab 2019).

In a Facebook takedown from August of 2019, accounts originating from Egypt and the UAE pursued a goal of promoting the UAE while also engaging in regional political discourse. For example, fake accounts impersonated public figures or posed as local news agencies across the Middle East and North Africa, then amplified content supportive of the UAE (Gleicher 2019*e*). BuzzFeed News also identified Twitter accounts posing as journalists which "heavily promoted the Emirates" (Lytvynenko & McDonald 2019). Accounts often used pro-UAE narratives in tandem with other political content, for instance pushing the hashtag #Libya_UAE with messages about the UAE's humanitarian support. Networks also reposted stories from UAE-based media outlets (FSI 2019). These campaigns have not been directly linked to a particular entity, but closely reflect the political interests of the UAE.

MULUAE0002. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Isolate Qatar diplomatically and economically**:

In May of 2017, the Qatar News Agency (QNA) and its associated social media pages were hacked. A fake speech was attributed to Qatar's Emir in which he praised Iran as well as Islamist groups Hamas, Hezbollah and the Muslim Brotherhood (Pinnell 2018). An Al Jazeera investigation linked the hack to Saudi Arabia, though US intelligence found evidence of senior UAE officials discussing the attack a day before it occurred (DeYoung & Nakashima 2017). Various countries including Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain used this fake story as a justification to break ties with Qatar and isolate the country diplomatically. The fake story was reported as fact by media outlets in the UAE and Saudi Arabia, and Twitter bots amplified anti-Qatar narratives both within Qatar and across the region (Jones 2019).

Disinformation relating to Qatar has continued to circulate in the years following the QNA hacking. In 2019, Facebook removed a commercial bot network associated with the companies "Newave" in the UAE and "New Waves" in Egypt which frequently aimed to denigrate Qatar. Another Facebook takedown linked to the UAE included fake accounts targeting Qatar's Emir and news websites accusing Qatar of sponsoring terrorism (Karan, Rizzuto & Kann 2019). Although a number of states participated in the attacks on Qatar, there is no clear evidence that the UAE coordinated with other countries.

MULUAE0003. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Influence Libyan politics within Libya and internationally**:

In April of 2019, Libyan General Khalifa Haftar announced that the Libyan National Army (LNA) would pursue an offensive on the capital city of Tripoli. In the weeks preceding and following this announcement, disinformation campaigns originating in a variety of countries began promoting political narratives related to Libya, though it is not clear that these efforts were coordinated. Commercial bot networks from the United Arab Emirates (UAE) posted and amplified hashtags in support of Haftar and included the use of fake personas (FSI 2019). One aim of this campaign appeared to be influencing people within Libya. For example, some accounts tried to promote a hashtag saying "People of Libya want the Libyan Army to secure the capital" (Kassab & Carvin 2019). Others amplified the tweets of Libyans who were supportive of the LNA.

In addition, UAE-based networks sought to influence international opinion towards Libya and to distort public debate on the conflict there. A network of Twitter accounts which could not be definitively linked to the UAE amplified similar pro-Haftar and pro-UAE

messaging in French and English. Consistent with the political agenda of the UAE's government, this campaign also attacked Qatar for supporting terrorism in Libya, targeted the Muslim Brotherhood, and criticized Turkey (Kassab & Carvin 2019). Along with accounts from Saudi Arabia and Egypt, bots and influencers from the UAE used Arabic-language hashtags and local media outlets to promote Haftar. Pro-Haftar messaging dated as far back as 2013 and has continued with Haftar's subsequent efforts to seize power, with added emphasis on defaming Libyan Prime Minister Fayez al-Sarraj (Grossman, H., DiResta, Kheradpir & Miller 2020).

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). 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).

SAUIRN0001. 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 is-

sues (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 inauthentic. It was often written in non-native English, and focused on issues from the Iranian state point of view. Three out of the top 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, Brookie & Karan 2018*b*).

SDNRUS0001. Targeted country **Sudan**. Attacking country **Russia**. Political goal **Discredit anti-government protests and support Russian foreign relations**:

From at least 2017 onward, former Sudanese President Omar al-Bashir maintained a close relationship with Russia. Also during this period, the Kremlin-linked paramilitary organization Wagner Group trained local Sudanese forces (Grossman et al. 2019). With the outbreak of anti-government protests in late 2018, a network associated with Russian oligarch Yevgeny Prigozhin created a strategy to maintain Bashir's power. The Russian mining company M-Invest, which has an office in the Sudanese capital of Khartoum, was the source of the proposal (Lister et al. 2019). Leaked documents reveal that the Russian network sought to discredit Sudanese protests through a disinformation campaign on social media, linking demonstrations to Israel and anti-Islamic sentiment. The proposal suggested building social media teams to attack protesters in parallel and support the government. In addition, the Russian network designed news websites such as Sudan Daily which frequently reposted content from the Russian outlet Sputnik (Alba & Frenkel 2019).

President al-Bashir was deposed in a coup in April of 2019. As part of an account takedown in October of 2019, researchers found that Russian Facebook pages designed to appear indigenous to Sudan have tended to support whatever regime is in power, frequently posing as Sudanese news sources (Grossman et al. 2019). These pages also repost stories from Russian news outlets Sputnik and RT.

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).

THARUS0001. Targeted country **Thailand**. Attacking country **Russia**. Political goal **Promote Russian foreign policy initiatives**:

Facebook took down a number of pages accused of "coordinated inauthentic behavior," based in Thailand but with substantial connections to Russia (Poulsen, 2019). The pages' main goal was to disseminate Russian foreign policy preferences while masquerading as organic Thai content. This network of 22 fake profiles drove people to off-platform blogs pretending to be local news outlets and claiming to have Thailand-based writers. Stories often countered the narratives of American media outlets or criticized Western influence in Southeast Asia. One page, for example, shared a story claiming that "the US and its allies are also busy locking up journalists like Julian Assage for exposing their own extensive right violations," a form of "human rights hypocrisy" (Gleicher 2019*d*). Another article was titled "Why is the Financial Times Smearing Thailand?"

Similar or cross-posted stories were shared by the outlet New Eastern Outlook (NEO), an English-language website managed by the Russian Academy of Science's Institute for Oriental Studies (EUvsDisinfo 2019*a*). NEO was first created in May 2010 and had three managers based in Thailand, Greece, and Russia at the time of the Facebook takedown. While pretending to be a neutral news outlet, NEO's Facebook page posted pro-Russia stories targeting a variety of countries including the US and promoting content consistent with Russian foreign policy initiatives (Robertson et al. 2019). NEO's website maintains pages adapted for a number of regional audiences including Thailand. Some pages in the Thai Facebook network were associated with the persona "Anthony Cartalucci," a writer for New Eastern Outlook who claimed to be an "American geopolitical analyst based in Thailand" (BangkokPost 2019).

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 by Russia:

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*b*)–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).[39]

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).

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, Brookie & Karan 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*).

[39]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).

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 Elections Nimmo & Brookie (2018*b*). However, the Iranian network of fake websites and accounts reported by Lim et al. (2019) also aimed at amplifying geopolitical tensions between the United States and countries in the Middle East.

USAIRN0004. Targeted country **United States**. Attacking country **Iran**. Political goal **Promote Iranian foreign policy initiatives in U.S.**:

A network thought to be of Iranian origin created social media personas posing as Americans, including journalists and Republican candidates for the U.S. House of Representatives in 2018 (Revelli & Foster 2019). These accounts posted general pro-Iranian messages, including anti-Saudi, anti-Israeli, and pro-Palestinian themes (Revelli & Foster 2019). They also posted in opposition to President Trump, and in some later cases posted anti-Iranian messaging, perhaps to build a broader audience or foster polarization. The accounts impersonating American political candidates directly plagiarized tweets and pictures from the real candidates and created original content about the Kavanaugh hearings as well as typical pro-Iranian messages (Timberg & Romm 2019).

In some instances, personas from the network conducted remote interviews with American or UK-based individuals while posing as journalists. Personas in the network published letters in a variety of local and larger newspapers, including the Los Angeles Times and the Seattle times, pretending to be based in the U.S. (Revelli & Foster 2019).

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

Russian trolls 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.

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, including the email account of the Clinton Campaign's chairman. A member of the 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" on or around March 2016 (Muller 2018).

The Internet Research Agency (IRA) created fictitious social-media personas, spreading falsehoods and promoted messages criticizing Hillary Clinton (Muller 2018). IRA tactics included applauding Donald Trump's candidacy while trying to undermine Hillary Clinton's (MacFarquhar 2018). Workers for the organization allegedly placed Facebook and Twitter ads carrying fake or harshly critical news about Hillary Clinton. The content of some of those ads was amplified via automated systems, i.e. "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 (actblue.com) 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 included fake accounts on social media trying to persuade voters not to choose the Democratic Party.[40] 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

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

assault by migrants (Nimmo, Brookie & Karan 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 sought to discredit the US Federal Bureau of Investigations (FBI) from 2017 onwards, especially its research on Russian influence operations. This was part of a larger campaign to discredit American institutions (Linvill & Warren 2018, Nimmo, Brookie & Karan 2018*a*). For example, Russian trolls promoted the effort to force the release of classified documents which allegedly show bias against President 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). Trolls linked to the Internet Research Agency (IRA) also 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, 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 by Obama's ties to the Muslim Brotherhood as they are by Trump's fake ties to Russia" (Poulsen & Ackerman 2018). 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 and 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 President 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(de Haldevang 2018). The state-funded news outlet RT coordinated with that activity by highlighting 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). 20,000 to 25,000 tweets were sent out daily using the hashtag #alabamasenaterace from approximately 600 twitter accounts. These accounts were being monitored by 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 came 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 suspended accounts used by five people involved in the project (Romm & Timberg 2018). Although the tactics were 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). 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 the 2018 midterm election**:

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).

ZAFRUS0002. Targeted country **South Africa**. Attacking country **Russia**. Political goal **Support African National Congress (ANC) party in 2019 South African presidential election**:

Leading up to South Africa's presidential election in May of 2019, a Russian network sought to promote disinformation and influence voters. A campaign associated with Russian oligarch Yevgeny Prigozhin, a Russian NGO called the Association for Free Research and International Cooperation (AFRIC), and the International Anticrisis Center worked to support South Africa's ruling African National Congress (ANC) party (Haffajee

2019). Leaked documents reveal a proposal to disseminate pro-ANC videos and use social media to defame opposition leaders. Some fake Twitter accounts were established for the ANC, but ultimately the Russian campaign seemed to have little effect on the election (BusinessTech 2019). The ANC has maintained a positive relationship with Moscow since the era of fighting against the apartheid regime (Burke & Harding 2019).

B.2 Annotated List of Domestic Influence Efforts

CHN0001. Targeted country **China**. Political goal **Discredit prominent dissidents of the Chinese government**:

In August of 2019, Twitter and other social media platforms removed over 1,000 fake accounts associated with the Chinese government. Much of the early activity of these accounts focused on attacking Chinese entrepreneur Guo Wengui, who fled to New York City in 2017 following the arrest of an associate. Wengui has publicly accused Chinese government officials of corruption (Wood et al. 2019). Twitter accounts in this network amplified messages criticizing Wengui's character, connections to the West, and accusing him of criminality. Narratives focusing on Wengui continued into 2019, with claims that Wengui helped organize the Hong Kong protests.

A smaller campaign targeted Gui Minhai, who wrote negative content about Chinese officials and has been detained multiple times by the Chinese government after disappearing from Thailand in 2015 (Li 2019). Other targets included human rights lawyer Yu Wensheng and Chinese veterans who protested against the government in 2018.

CUB0001. Targeted country **Cuba**. Political goal **Promote the political agenda of the Communist Party of Cuba**:

Since as early as 2015, Cuba's ruling Communist Party is thought to have coordinated the creation of Twitter bots and fake accounts to campaign for the party and promote political narratives (Torres & Vela 2018). According to reporting from 2019, so-called "ciberclarias" or cyber catfishes are Cubans who maintain fake social media accounts on behalf of Cuba's intelligence agency in return for cell phone data or other "privileges" (González 2019). Some ciberclarias are students recruited from Cuba's University of Informatics Sciences (UCI). These accounts often post in support of Cuba's political elite, attack opposition journalists, and downplay human rights abuses for an international audience (ADNCuba 2020). In May of 2020, multiple sources reported on apparent instructions distributed to Cubans maintaining fake accounts on how to respond to the broadcast of an "anti-Cuban" interview with American officials (RadioTelevisionMartí 2020). This effort appears to be ongoing.

ECU0001. Targeted country **Ecuador**. Political goal **Attack Rafael Correa's political opposition**:

In 2015, an investigation by Fundación Mil Hojas found that the Ecuadorian company Ribeney SA was operating a troll center to monitor and attack former President Rafael Correa's political opposition on Facebook and Twitter. Ribeney had multiple contracts with the Ecuadorian Ministry of Strategic Sectors, including one to design a strategic communication plan aimed at promoting Ecuador's management of oil exploitation (Mil-Hojas 2015).

Ximah Digital, another company awarded contracts by the Ecuadorian government, admitted to having created the Facebook page for the popular Twitter account El Patriota. The account frequently attacked opponents of Correa's government and highlighted positive aspects of the government's agenda (ElUniverso 2014).

Allegations associating Correa with social media manipulation date back to 2012, when a former congressman received a list of accounts used to defend Correa from critics and journalists online (Morla 2015). During his tenure, President Correa also publicly encouraged trolling. Correa used his weekly presidential TV program to ask supporters to spam various Twitter accounts which had been critical of Correa's administration (BBC 2015).

HKGCHN0002. Targeted country **Hong Kong**. Attacking country **China**. Political goal **Undermine and delegitimize the Hong Kong protests**:

In August of 2019, Facebook, Twitter, and Google collectively removed over 1,000 accounts linked to the Chinese government, all of which were engaging in a coordinated effort to undermine pro-democracy protests in Hong Kong (Stewart 2019). The Twitter network of 936 accounts included automated bots which posted in a variety of languages such as Cantonese, Indonesian, Arabic, and English (Karan & Zhang 2019). Many of these accounts were previously used to promote spam and commercial content, but pivoted to promoting political narratives related to Hong Kong in late 2018. Tweets included messages accusing protesters of "ulterior motives," asking that viewers "support the police squad," and suggesting the manipulation of information by "Western media" (Wood et al. 2019).

As part of this takedown, Google removed 210 YouTube accounts engaging in similarly misleading behavior, and Facebook removed 15 accounts, pages, or groups. The Facebook pages attracted more than 15,000 followers. State-run Chinese media outlets such as Xinhua News Agency and China Daily also financed social media advertisements criticizing the protests (Mac & Adams 2019). These promoted stories sought to counter the coverage of Hong Kong by foreign news outlets.

HON0001. Targeted country **Honduras**. Political goal **Support Honduran President Juan Orlando Hernández**:

From July of 2019 through April of 2020, Facebook and Twitter collectively removed thousands of accounts and pages "when it became clear a staffer created the fake accounts on the government's behalf," according to Twitter (Ljubas 2020). The Facebook takedown included fake accounts designed to amplify positive messages about President Hernandez. On both Twitter and Facebook, one of the suspended accounts was that of the state-run media organization Televisión Nacional de Honduras (TNH) which had amassed over 40,000 followers (Cryst & García-Camargo 2020). TNH promoted stories praising actions of the Hernandez administration, retweeted the president's own posts, and shared links for TNH news stories. Other suspended accounts had "explicit connections to the presidency," though the majority of the takedown consisted of automated accounts created in 2019 to retweet President Hernandez and amplify hashtags (Cryst & García-Camargo 2020).

There is also evidence that the private Israeli firm Archimedes Group financed advertisements and created fake accounts supporting President Hernandez and attacking the

opposition in 2019. However, this effort has not been linked to Hernandez or any government officials (Bandeira 2019).

IDN0001. Targeted country **Indonesia**. Political goal **Reduce support for the Western Papuan Independence movement**:

A pro-Indonesian government campaign was launched on Facebook in order to spread content critical of the Western Papuan independence movement. On October 3rd, 2019, Facebook announced the removal of 69 Facebook accounts, 42 Pages and 34 Instagram accounts involved in coordinated inauthentic behavior in Indonesia (Gleicher 2019*f*). About 410,000 accounts followed one or more of these Facebook pages and around 120,000 accounts followed at least one of the Instagram pages. The campaign spent $300,000 on Facebook advertising. The content was linked to a Jakarta-based media company, InsightID, which shared content directly from the government's news agency website, Ankara (Kann & Buziashvili 2019). These pages were created with names which appeared to be sympathetic toward the independentist movement in Western Papua, but they actually posted pro-Indonesian government content. The overarching Facebook strategy was to paint a picture of the independentist movement as radical and dangerous.

This network also spread positive messages about the Indonesian government's economic development projects in Western Papua, defended the government's respect for human rights, and disseminated messages advocating for Indonesian interests at the United Nations (Kann & Buziashvili 2019). Automated accounts (bots) and trolls spammed pro-independence hashtags such as "freewestpapua" with positive stories about the government, thus engaging in a form of hashtag hijacking to distort public debate (Strick & Syavira 2019).

MEX0001. Targeted country **Mexico**. Political goal **Support the Mexican Institutional Revolutionary Party (PRI)**:

Leading up to the 2017 Mexican gubernatorial elections, the Governor of the State of Mexico's office of social communications paid various fake media outlets to promote content in favor of politicians from the ruling Institutional Revolutionary Party (PRI) (Barragán 2017). Earlier in 2017, researchers also discovered a network of Twitter bots attempting to discredit protests and share content from the pro-government newspaper Excélsior (Gallagher 2017).

In addition, ahead of Mexico's presidential election in July 2018, a network of Twitter bots and Facebook pages sought to defame candidate Andrés Manuel López Obrador from the National Regeneration Movement party. This network was associated with Mexican entrepreneur Carlos Merlo who reportedly controls "millions of automated social media bots, and dozens of 'fake news' pages and websites" (Nimmo, Barojan, Peñarredonda & Karan 2018). Merlo claims to have been hired for work on behalf of candidates and parties including PRI in the past (Gallagher 2019). Similar social media and hashtag campaigns were conducted on behalf of PRI Senate candidates in 2018 (Barojan 2018*b*).

PRI is known to rely on social media manipulation ahead of elections, with pro-PRI bots being dubbed "Peñabots." Peñabots originated with the election of PRI candidate Enrique Peña Nieto as President of Mexico in 2012, and actively amplified pro-Peña Nieto narratives over the course of his tenure (Daniels 2016).

MLT0001. Targeted country **Malta**. Political goal **Discredit prominent opponents**

of the Maltese government:

At least eight senior staff members of the Maltese government as well as President Marie-Louise Coleiro Preca and Prime Minister Joseph Muscat were part of Facebook groups which coordinated attacks on opposition politicians and anti-corruption activists (TheShift 2018*b*). Some of the groups had up to 60,000 members, producing abusive and violent posts to influence and distort public political debate. The groups also promoted the policies of the Prime Minister and denied negative news related to Muscat.

One example of the network's defamation tactics occurred in 2017, when Facebook accounts launched a hate campaign against anti-corruption activist and journalist Daphne Caruana Galizia following her assassination. A Facebook account associated with the campaign said "Let's celebrate" after Caruana Galizia was found murdered, and group members were instructed to "unite behind the Prime Minister and follow his instructions" (TheShift 2018*a*).

MMR0001. Targeted country **Myanmar**. Political goal **Promote anti-Rohingya sentiment**:

Operatives associated with the military of Myanmar produced news websites, Facebook pages, and Instagram accounts which appeared to be organic to Myanmar. After attracting followers with non-political content, these platforms were used to promote propaganda and disinformation targeting the Muslim Rohingya minority group (Roose 2017, Beech & Nang 2018, Gleicher 2019*i*). In this case, social media was used as "a tool for ethnic cleansing," inciting murder and violence which forced more than 700,000 Rohingya to flee the country (Mozur 2018). Myanmarese officers used trolls, fake accounts, and celebrity Facebook pages to attack posts critical of the military and stoke arguments amongst social media users (Roose 2017, Beech & Nang 2018).

In one effort to consolidate military power, social media operatives created Muslim Facebook pages to warn of imminent anti-Muslim protests organized by Buddhist monks. At the same time, operatives created Buddhist Facebook pages claiming that "jihad attacks" were being planned by Rohingya Muslims. By distorting reality through the use of social media, this campaign stoked fear and distrust along ethnic lines (Mozur 2018).

PAK0001. Targeted country **Pakistan**. Political goal **Support Pakistan's military and foreign policy initiatives**:

On April 1st, 2019, Facebook took down a network of approximately 100 Pakistani pages which spread fake news and inflammatory messages about India as well as Pakistan's claims over Kashmir (Gleicher 2019*a*). The posted content extolled Pakistan's military operations and sought to discredit India, often through the production of fake stories (Nimmo & Karan 2019). One goal of this campaign was to bolster support for the military within Pakistan. Facebook claimed that the pages involved were associated with employees of the Inter-Service Public Relations, the media wing of the Pakistani army. In addition, the content shared on these pages was consistent with the interests of the Pakistani government (Nimmo & Karan 2019).

PRI0001. Targeted country **Puerto Rico**. Political goal **Support Ricardo Rosselló**:

A number of government officials including former Puerto Rican Governor Ricardo Rosselló participated in a Telegram chat which is thought to have coordinated the behavior of a

group of pro-government Twitter trolls (Sepúlveda 2019). The Twitter accounts supported Rosselló and his administration, promoted a hashtag in support of Puerto Rico's police, and targeted political opponents. For example, the network attempted to associate the mayor of San Juan and a Puerto Rican senator with the Nicolas Maduro regime in Venezuela after similar instructions appeared in the Telegram chat (Bandeira & Ponce de León 2019).

RUS0001. Targeted country **Russia**. Political goal **Suppress domestic political opposition**:

On multiple occasions, fake accounts and bots associated with a troll factory in St. Petersburg were used to attack President Vladimir Putin's political opponents, suppress opposition, and promote government propaganda within Russia. Content is spread across social media platforms such as Facebook, Twitter, YouTube, and Livejournal.com as well as the Russian networks VK.com and Odnoklassniki (Nimmo & Toler 2018). Pro-Kremlin trolling became widespread in the wake of 2011 protests, when the Russian government sought to "rein in the Internet" through the tracking and manipulation of social media (Chen 2015).

For example, after the murder of vocal Putin critic and politician Boris Nemtsov on February 27, 2015, an extensive network of bots shared and promoted narratives questioning the circumstances surrounding Nemtsov's death. This effort was coordinated by the Internet Research Agency (IRA) and persisted throughout 2015, peaking from the time of the assassination through early March 2015. Trolls attempted to discredit both Nemtsov and political opposition by claiming that Nemtsov was murdered to attract more people to an antigovernment rally planned for March 1, 2015 (Khachatryan 2015).

A similar campaign sought to distort Russian protests in 2019. State-backed media outlets first attempted to suppress information about the protests, and then used social media and broadcasting to claim that foreign countries were inciting unrest and interfering in Russian politics (Assenova 2019). Kremlin outlet RT also reported that 12,000 protesters appeared in Moscow, while the actual number was approximately 20,000 (Andriukaitis 2019).

RUS0002. Targeted country **Russia**. Political goal **Support Moscow's housing demolition plan**:

In March of 2017, Russian Mayor Sergey Sobyanin announced a plan to demolish Soviet-era apartment buildings known as "Khrushchyovki" and replace them with high-rises (Kovalev 2017). In the months following, social media users from Moscow's "Youth Chamber" amplified pro-Sobyanin content and falsely claimed to live in the targeted housing units. This campaign was connected to the company Moscow Information Technologies (MIT) which is owned by the Moscow City Government (Chizhova 2017). In addition, the city of Moscow was involved in the creation of local news websites and newspapers which distort the media landscape in favor of governmental campaigns. For example, the Vechernyaya Moskva newspaper claimed that a photo showed a rally of Muscovites in favor of demolition when the photo actually came from an anti-demolition protest.

SAU0001. Targeted country **Saudi Arabia**. Political goal **Promote Saudi government narratives**:

Since at least 2015, Saudi Arabia operated a Twitter troll farm to undermine political dissidence and try to infiltrate accounts (Benner et al. 2018). Social media "trolls" were instructed to attack particular users, promote pro-government messages, meet Tweet quotas, and make use of various memes. In 2015, western intelligence officials also informed Twitter that an employee, Ali Alzabarah, could be a Saudi spy. By 2018, Saudi Arabia made use of Twitter bots to amplify hashtags supporting government initiatives and Crown Prince Mohammed bin Salman as well as obfuscate information on the death of journalist Jamal Khashoggi (Collins & Wodinsky 2018). In 2019, Facebook suspended accounts linked to the Saudi Arabian government which, in addition to promoting domestic interests, also criticized Iran, Qatar, and Turkey, and sought to undermine Al Jazeera and Amnesty International. Around the same time, Twitter suspended the official account of Saudi royal court adviser Saud al-Qahtani (Chee & Paul 2019).

In addition, a 2019 Twitter takedown of accounts created by the Saudi Arabian digital marketing company Smaat promoted similar political narratives aligned with the Saudi Arabian government, though most Smaat content was commercial in nature (DiResta et al. 2019). Accounts frequently focused on defaming Khashoggi and criticizing the governments of rival countries.

SDN0001. Targeted country **Sudan**. Political goal **Support the Sudanese government and attack political opposition**:

In the wake of the Arab Spring in 2011, the Sudanese government established a "cyber jihadist unit" as part of the National Intelligence and Security Service (NISS). It is not clear when the unit began to make use of coordinated disinformation campaigns, but based on a 2012 interview, Freedom House reported that the NISS branch promoted misinformation and planted online contributors to defame government critics (FreedomHouse 2014).

In recent years, the cyber jihadist unit has monitored online content for political dissidence, infiltrated online groups to quell opposition and amplify disinformation, and orchestrated cyber attacks (FreedomHouse 2019). Reporters Without Borders (RSF 2020) described the unit as a "troll army" which has actively sought to discredit the transitional government following the 2019 Sudanese Revolution. As an example, the unit promoted a story about police killings in January 2019 which was found to be fake, then attacked the characters of activists and journalists who shared the story.

In addition, prior to the deposition of President Omar al-Bashir in April 2019, Bashir received strategic advice on quelling protests from the Russian company M-Invest. This strategy involved attacking the protesters on social media and spreading fake stories blaming Israel for the unrest (Lister et al. 2019).

TJK0001. Targeted country **Tajikistan**. Political goal **Support the Tajik government and attack opposition**:

The Tajik government is suspected of maintaining a "troll farm" for amplifying political propaganda and suppressing dissidence online (RFE/RL 2019). Some fake pro-government accounts are run by unpaid university students and staff, who say that they are threatened into compliance by school administrations and officials from the Education and Science Ministry. Other social media profiles are thought to be maintained by paid operatives from a state-backed network which promotes government narratives, including

the notion that Tajikistan is free of COVID-19 (Eurasianet 2020). Social media trolls are also used to harass political critics such as journalist Humayra Bakhtiyar, who reported on corruption in Tajikistan (CPJ 2019).

According to reporting by the Tajik outlet Akhbor, up to 70 employees work in a troll farm at offices for Tajiktelecom, the national telecommunications operator (BBC 2019*a*). The unit has established a number of websites and Facebook pages for disseminating pro-government news and disinformation.

TUR0001. Targeted country **Turkey**. Political goal **Discredit government opponents and support the ruling AKP party**:

Following the Gezi Park protests in 2013, the ruling AKP (Justice and Development Party) increased its online presence by creating a troll army known as the AK Trolls (6,000 units), employing automated bots and stealing profiles in order to boost online consensus for the party and discredit opponents (Albayrak & Parkinson 2013). Instances of these efforts are the online aggressions perpetrated against journalists such as Ceyda Karan, Selin Girit, and Nevşin Mengü (Monaco & Nyst 2018), as well as the spread of nationalist and anti-Kurd content (Yesil et al. 2017). Despite AKP officials repeatedly denying the building of online influence capacity, several studies have ascertained the existence of such domestic influence effort (Monaco & Nyst 2018, Yesil et al. 2017, Bulut & Yörük 2017, Saka 2018), also confirmed by a tape recording of President Recep Tayyip Erdoğan's daughter speaking of trolls ready to help in AKP's campaigns.

VEN0001. Targeted country **Venezuela**. Political goal **Support the Nicolás Maduro regime**:

For several years, Venezuelan President Nicolás Maduro has used social media to promote political content supportive of the Maduro regime. State-linked Twitter account creation first surged in March 2014 with the outbreak of anti-government protests and has continued to rise particularly during periods of unrest (Karan, Peñarredonda & Bandeira 2019). In addition, Venezuela's Ministry of Communications creates a daily hashtag which is amplified by suspected bot accounts. State-owned media outlets such as Venezolana de Televisión also promote these hashtags, sometimes with the implication that the hashtags appeared organically (Peñarredonda & Karan 2019). Another network with potential links to the Maduro government attacked opposition leader Juan Guaidó following the Venezuelan National Assembly elections in January 2020 (Ponce de León & Pérez 2020).

In addition, a Twitter network originating in Venezuela frequently posted in English about such topics as the 2018 U.S. midterm elections, though this could not be definitively attributed to Venezuelan state actors (Collins 2019). According to Twitter, this campaign seems to have been operated by a "commercial entity originating in Venezuela" (Roth 2019).

VNM0001. Targeted country **Vietnam**. Political goal **Support Vietnam Communist Party**:

In 2017, the Vietnam People's Army (VPA) created a cyber military unit called Task Force 47, a 10,000-strong network used to attack the Vietnam Communist Party's political opponents and promote government content on Facebook and other social media platforms (Phuong 2018). Officially, Task Force 47 is comprised of military personnel

trained to combat the "peaceful revolution" of Western political ideology online. In addition, Force 47 suppresses and attacks political dissidents, who often face penalties and prison time for criticizing the government (Hookway 2017).

In recent years, cyber espionage groups based in Vietnam have also carried out a number of sophisticated attacks, including the hacking of Toyota and the ASEAN Secretariat (Thomas 2019*b*). For example, APT32 is thought to be affiliated with the Vietnamese government and uses strategies that include stealing login information and targeting government opposition.

ZWE0001. Targeted country **Zimbabwe**. Political goal **Promote President Mnangagwa and attack opposition in the 2018 presidential elections**:

Leading up to Zimbabwe's 2018 presidential election, both the ruling Zanu-PF party and the MDC-Alliance made use of "online warriors," including bots and paid or volunteering youth. These networks promoted doctored images and fake stories to "project the false impression of overwhelming support" and undermine the opposition (Moyo 2018). The incumbent President Emerson Mnangagwa, who took power after a military coup in 2017, dubbed his online campaigners the "Varakashi," meaning destroyers, and encouraged them to attack enemies of the party online (Mwareya 2019). Following Mnangawa's election, the Varakashi have used fake accounts to disrupt criticism of the administration. In addition, opposition candidate Nelson Chamisa accused Zanu-PF of employing "foreigners" in a fake news campaign, with the suggestion that he was referring to Russia (Griffin 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

ADNCuba (2020), '¿cómo detectar a una ciberclaria?'.
URL: https://adncuba.com/noticias-de-cuba/como-detectar-una-ciberclaria

Alandete, D. (2017), 'Russian network used venezuelan accounts to deepen catalan crisis'.
URL: https://english.elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

Alba, D. & Frenkel, S. (2019), 'Russia tests new disinformation tactics in africa to expand influence'.
URL: https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html

Albayrak, A. & Parkinson, J. (2013), 'Turkey's government forms 6,000-member social media team'.
URL: https://www.wsj.com/articles/turkeys-government-forms-6000member-social-media-team-1379351399

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

Aleksejeva, N., Karan, K., Barojan, D. & Nimmo, B. (2019*a*), 'Facebook's sputnik takedown — in depth'.
URL: https://medium.com/dfrlab/facebooks-sputnik-takedown-in-depth-f417bed5b2f8

Aleksejeva, N., Karan, K., Barojan, D. & Nimmo, B. (2019*b*), 'Facebook's sputnik takedown — top takeaways'.
URL: https://medium.com/dfrlab/facebooks-sputnik-takedown-top-takeaways-dbc22f7e9540

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

Andriukaitis, L. (2019), 'Kremlin outlets downplay the size of the july 20 protests in moscow'.
URL: https://medium.com/dfrlab/kremlin-outlets-downplay-the-size-of-the-july-20-protests-in-moscow-56a36aa5b9f5

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

Applebaum, A. (2019), 'Want to build a far-right movement? spain's vox party shows how.'.
URL: https://www.washingtonpost.com/graphics/2019/opinions/spains-far-right-vox-party-shot-from-social-media-into-parliament-overnight-how/

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

Assenova, M. (2019), 'Russia: Non-information as disinformation'.
URL: https://www.polygraph.info/a/russia-non-information-as-disinformation/30110010.html

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

Bail, C. A., Guay, B., Maloney, E., Combs, A., Hillygus, D. S., Merhout, F., Freelon, D. & Volfovsky, A. (2020), 'Assessing the russian internet research agency's impact on the political attitudes and behaviors of american twitter users in late 2017', *Proceedings of the national academy of sciences* **117**(1), 243–250.

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

Bandeira, L. (2019), 'Archimedes ran politically charged facebook ads in crisis-torn honduras'.
URL: https://medium.com/dfrlab/archimedes-ran-politically-charged-facebook-ads-in-crisis-torn-honduras-1137f355e159

Bandeira, L., Carvin, A., Karan, K., Kasab, M., Kaul, A., Nimmo, B. & Sheldon, M. (2019), 'Inauthentic israeli facebook assets target the world'.
URL: https://medium.com/dfrlab/inauthentic-israeli-facebook-assets-target-the-world-281ad7254264

Bandeira, L. & Ponce de León, E. (2019), 'From telegram to twitter: Top puerto rican officials plotted possible information operation'.
URL: https://medium.com/dfrlab/from-telegram-to-twitter-top-puerto-rican-officials-plotted-possible-information-operation-a899a00e078e

BangkokPost (2019), 'Facebook shows posts of banned accounts in thailand'.
URL: https://www.bangkokpost.com/thailand/politics/1719415/facebook-shows-posts-of-banned-accounts-in-thailand

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*), 'Electionwatch: Down ballot bots in mexico'.
URL: https://medium.com/dfrlab/electionwatch-down-ballot-bots-in-mexico-e1bee023291d

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

Barragán, D. (2017), 'Eruviel le da millones a "sitios digitales", "agencias", muros de facebook y "revistas" fantasma'.
URL: https://www.sinembargo.mx/28-07-2017/3269866

BBC (2015), 'Ecuador president rafael correa's troll warfare'.
URL: https://www.bbc.com/news/blogs-trending-31057933

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

BBC (2019*a*), 'Highlights from central asian press, websites 16 aug 19'.
URL: https://advance-lexis-com.ezproxy.princeton.edu/api/document?collection=news&id=urn:contentItem:5WTX-5681-DYRV-33VJ-00000-00&context=1516831

BBC (2019*b*), 'Twitter removes iranian-backed accounts'.
URL: https://www.bbc.com/news/technology-48635878

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

Beech, H. & Nang, S. (2018), 'In myanmar, a facebook blackout brings more anger than a genocide charge'.
URL: https://www.nytimes.com/2018/08/31/world/asia/myanmar-genocide-facebook-military.html

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

Benner, K., Mazzetti, M., Hubbard, B. & Isaac, M. (2018), 'Saudis' image makers: A troll army and a twitter insider'.
URL: https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

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

Bulut, E. & Yörük, E. (2017), 'Digital populism: Trolls and political polarization of twitter in turkey', *International Journal of Communication* **11**, 25.

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

Burke, J. & Harding, L. (2019), 'Documents suggest russian plan to sway south africa election'.
URL: https://www.theguardian.com/world/2019/may/08/documents-suggest-russian-plan-to-sway-south-africa-election

BusinessTech (2019), 'Documents show alleged russian plot to interfere in south african elections: report'.
URL: https://businesstech.co.za/news/government/315678/documents-show-alleged-russian-plot-to-interfere-in-south-african-elections-report/

Carvin, A. & Kassab, M. (2019), 'Libyan hashtag campaign has broader designs: Trolling qatar'.
URL: https://medium.com/dfrlab/libyan-hashtag-campaign-has-broader-designs-trolling-qatar-8b2ba69c7334

Chappelle, A. (2018), 'Twitter bots, fake news and propaganda in the qatar crisis'.
URL: https://www.aljazeera.com/news/2018/06/twitter-bots-fake-news-propaganda-qatar-crisis-180604134035342.html

Chee, F. Y. & Paul, K. (2019), 'Twitter suspends saudi royal adviser qahtani, fake gulf accounts'.
URL: https://www.reuters.com/article/us-twitter-saudi/twitter-suspends-saudi-royal-adviser-qahtani-fake-gulf-accounts-idUSKBN1W50O0

Chen, A. (2015), '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.

Chizhova, L. (2017), ''living bots': How moscow's mayor uses stealth to shape public opinion'.
URL: https://www.rferl.org/a/moscow-mayor-sobyanin-mobilizing-influencers-stealth-campaign-bots-khrushchyovki/28504056.html

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

ClearSky (2018), 'Global iranian disinformation operation'.
URL: https://www.clearskysec.com/wp-content/uploads/2018/11/Global-Iranian-Disinformation-Operation-Clearsky-Cyber-Security.pdf

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. (2019), 'Twitter and facebook say they removed thousands of troll accounts in run-up to 2018 midterms'.
URL: https://www.nbcnews.com/tech/security/twitter-says-it-removed-troll-accounts-tied-russia-iran-venezuela-n965491

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

Cook, S. (2020), 'Beijing's global megaphone'.
URL: https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone

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

CPJ (2019), 'Tajik authorities harass journalist humayra bakhtiyar and family'.
URL: https://cpj.org/2019/07/tajik-authorities-harass-journalist-humayra-bakhti/

Cryst, E. & García-Camargo, I. (2020), An analysis of twitter's takedown of honduran accounts, Technical report.
URL: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/04022020-hondurastakedown.pdf

Daniels, L. (2016), 'Rise of the peñabots'.
URL: https://points.datasociety.net/rise-of-the-pe%C3%B1abots-d35f9fe12d67

Dasgupta, P. (2018), ''it's like frankenstein's monster': The founder of bjp's it cell says pm modi's team started the rot'.
URL: https://www.huffingtonpost.in/2018/06/22/its-like-frankensteins-monster-the-father-of-the-bjps-it-cell-says-team-modi-started-the-rot_a_23464587/

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

de Haldevang, M. (2018), 'Russian trolls and bots are flooding twitter with ford-kavanaugh disinformation'.
URL: https://qz.com/1409102/russian-trolls-and-bots-are-flooding-twitter-with-ford-kavanaugh-disinformation/

DemocracyReporting (2019), 'Libya social media monitoring report'.
URL: https://democracy-reporting.org/libya-social-media-report/april-may-june/

DeYoung, K. & Nakashima, E. (2017), 'Uae orchestrated hacking of qatari government sites, sparking regional upheaval, according to u.s. intelligence officials'.
URL: https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html

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., Grossman, S., K.H. & Miller, C. (2019), Analysis of twitter takedown of state-backed operation attributed to saudi arabian digital marketing firm smaat, Technical report.
URL: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20191223_smaat.pdf

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

Díaz, I. (2017), 'Venezuela and russia teamed up to push pro-catalan fake news'.
URL: https://www.thedailybeast.com/why-is-venezuela-waging-cyber-war-in-europe

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

ElUniverso (2014), 'Compañía ximah creó en facebook cuenta crítica a oposición en ecuador'.
URL: https://www.eluniverso.com/noticias/2014/09/08/nota/3774286/ximah-creo-facebook-cuenta-critica-oposicion

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.

Eurasianet (2020), 'Tajikistan's nonchalance on coronavirus shows cracks'.
URL: https://eurasianet.org/tajikistans-nonchalance-on-coronavirus-shows-cracks

EUvsDisinfo (2018), 'Disinformation analysis on the western balkans: Lack of sources indicates potential disinformation'.
URL: https://euvsdisinfo.eu/disinformation-analysis-on-the-western-balkans-lack-of-sources-indicates-potential-disinformation/

EUvsDisinfo (2019*a*), 'The journalists who exist only on paper'.
URL: https://euvsdisinfo.eu/the-journalists-who-exist-only-on-paper/

EUvsDisinfo (2019*b*), '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.

FreedomHouse (2014), 'Freedom on the net 2014'.
URL: https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

FreedomHouse (2019), 'Freedom of the net 2019: Sudan'.
URL: https://freedomhouse.org/country/sudan/freedom-net/2019

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/

FSI (2019), 'Libya: Presidential and parliamentary elections scene setter'.
URL: https://cyber.fsi.stanford.edu/io/news/libya-scene-setter

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

Furlong, A. (2019), 'Labour: Dossier indicates nhs 'up for sale' in us trade deal'.
URL: https://www.politico.eu/article/labour-dossier-indicates-nhs-up-for-sale-in-us-trade-deal/

Gallagher, E. (2017), 'Mexican media botnet study'.
URL: https://medium.com/@erin_gallagher/mexican-media-botnet-study-21c78a1664c3

Gallagher, E. (2019), 'Mexico: Coordinated inauthentic behavior on facebook twitter'.
URL: https://medium.com/@erin_gallagher/mexico-coordinated-inauthentic-behavior-on-facebook-twitter-a670280d02fc

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/

Gleicher, N. (2019*a*), 'Removing coordinated inauthentic behavior and spam from india and pakistan'.
URL: https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/

Gleicher, N. (2019*b*), 'Removing coordinated inauthentic behavior from israel'.
URL: https://about.fb.com/news/2019/05/removing-coordinated-inauthentic-behavior-from-israel/

Gleicher, N. (2019*c*), 'Removing coordinated inauthentic behavior from russia'.
URL: https://about.fb.com/news/2019/01/removing-cib-from-russia/

Gleicher, N. (2019*d*), 'Removing coordinated inauthentic behavior in thailand, russia, ukraine and honduras'.
URL: https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/

Gleicher, N. (2019*e*), 'Removing coordinated inauthentic behavior in uae, egypt and saudi arabia'.
URL: https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/

Gleicher, N. (2019*f*), 'Removing coordinated inauthentic behavior in uae, nigeria, indonesia and egypt'.
URL: https://about.fb.com/news/2019/10/removing-coordinated-inauthentic-behavior-in-uae-nigeria-indonesia-and-egypt/

Gleicher, N. (2019*g*), 'Removing more coordinated inauthentic behavior from iran'.
URL: https://about.fb.com/news/2019/05/removing-more-cib-from-iran/

Gleicher, N. (2019*h*), 'Removing more coordinated inauthentic behavior from russia'.
URL: https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/

Gleicher, N. (2019*i*), 'Taking down more coordinated inauthentic behavior in myanmar'.
URL: https://about.fb.com/news/2019/08/more-cib-myanmar/

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/

Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A. & Tucker, J. A. (2020), 'Cross-platform state propaganda: Russian trolls on twitter and youtube during the 2016 us presidential election', *The International Journal of Press/Politics* p. 1940161220912682.

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

González, O. (2019), '"ciberclarias", un ejército que invade las redes sociales con cuentas falsas'.
URL: https://www.cubanet.org/destacados/ciberclarias-un-ejercito-que-invade-las-redes-sociales-con-cuentas-falsas/

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

Griffin, T. (2018), 'Zimbabwe's opposition leader accused the ruling party of hiring "fake news mercenaries"'.
URL: https://www.buzzfeednews.com/article/tamerragriffin/zimbabwe-fake-news

Grossman, S. (2019), 'Russia wants more influence in africa. it's using disinformation to get there.'.
URL: https://www.washingtonpost.com/politics/2019/12/03/russia-wants-more-influence-africa-its-using-disinformation-get-there/

Grossman, S., Bush, D. & DiResta, R. (2019), Evidence of russia-linked influence operations in africa, Technical report.
URL: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf

Grossman, S., H., K. & DiResta, R. (2020), 'Blurring the lines of media authenticity: Prigozhin-linked group funding libyan broadcast media', *Stanford Internet Observatory* .
URL: https://cyber.fsi.stanford.edu/io/news/libya-prigozhin

Grossman, S., H., K., DiResta, R., Kheradpir, T. & Miller, C. (2020), 'Blame it on iran, qatar, and turkey: An analysis of a twitter and facebook operation linked to egypt, the uae, and saudi arabia'.
URL: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20200402_blame_it_on_iran_qatar_and_turkey_v2_0.pdf

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/

Haffajee, F. (2019), 'Exclusive: Did putin's 'chef' attempt to interfere in south african election?'.
URL: https://www.dailymaverick.co.za/article/2019-05-07-exclusive-did-putins-chef-attempt-to-interfere-in-south-african-election/

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

Harding, L. & Burke, J. (2019), 'Leaked documents reveal russian effort to exert influence in africa'.
URL: https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influence-in-africa

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

Hookway, J. (2017), 'Introducing force 47, vietnam's new weapon against online dissent'.
URL: https://www.wsj.com/articles/introducing-force-47-vietnams-new-weapon-against-online-dissent-1514721606

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.

Jones, M. O. (2019), 'The gulf information war— propaganda, fake news, and fake trends: The weaponization of twitter bots in the gulf crisis', *International journal of communication* **13**, 27.

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

Kann, A. & Buziashvili, E. (2019), 'Facebook takes down pro-indonesian pages targeting west papua'.
URL: https://medium.com/dfrlab/facebook-takes-down-pro-indonesian-pages-targeting-west-papua-3c8b56449bfd

Kao, J. & Li, M. S. (2020), 'How china built a twitter propaganda machine then let it loose on coronavirus'.
URL: https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

Karan, K. (2019), 'Royally removed: Facebook takes down pages promoting saudi interests'.
URL: https://medium.com/dfrlab/royally-removed-facebook-takes-down-pages-promoting-saudi-interests-edc0ce8b972a

Karan, K., Kaul, A. & Nimmo, B. (2019), 'Facebook removes iran-based assets. again.'.
URL: https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f

Karan, K. & Nimmo, B. (2019), 'Electionwatch: Inauthentic activity in india'.
URL: https://medium.com/dfrlab/electionwatch-inauthentic-activity-in-india-8940588e09b5

Karan, K., Peñarredonda, J. L. & Bandeira, L. (2019), 'Trolltracker: Venezuelan government-linked influence campaign on twitter'.
URL: https://medium.com/dfrlab/trolltracker-venezuelan-government-linked-influence-campaign-on-twitter-63a8fe7a62e0

Karan, K., Rizzuto, M. & Kann, A. (2019), 'Uae facebook pages targeted qatar and muslim brotherhood'.
URL: https://medium.com/dfrlab/uae-facebook-pages-targeted-qatar-and-muslim-brotherhood-8aec916fa1f7

Karan, K. & Zhang, P. (2019), 'Twitter's hong kong archives: Chinese commercial bots at work'.
URL: https://medium.com/dfrlab/twitters-hong-kong-archives-chinese-commercial-bots-at-work-f4c7ae8eea64

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

Kassab, M. & Carvin, A. (2019), 'A twitter hashtag campaign in libya: How jingoism went viral'.
URL: https://medium.com/dfrlab/a-twitter-hashtag-campaign-in-libya-part-1-how-jingoism-went-viral-43d3812e8d3f

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

Khachatryan, D. (2015), 'How to become a troll hunter'.
URL: https://novayagazeta.ru/articles/2015/03/10/63342-kak-stat-trollhanterom

Khana, C. (2017), 'Bots, blockades and blackouts: how armenia media copes'.
URL: https://oc-media.org/features/bots-blockades-and-blackouts-how-armenia-media-copes/

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

Kovalev, A. (2017), 'The city of moscow has its own propaganda empire'.
URL: https://www.themoscowtimes.com/2017/05/16/the-city-of-moscow-has-its-own-propaganda-empire-a58005

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

LaLiga (2020), 'En las entrañas de una 'bodeguita' uribista'.
URL: https://ligacontraelsilencio.com/2020/02/06/en-las-entranas-de-una-bodega-uribista/

Landler, M. & Castle, S. (2020), "no one' protected british democracy from russia, u.k. report concludes'.
URL: https://www.nytimes.com/2020/07/21/world/europe/uk-russia-report-brexit-interference.html

Lesaca, J. (2017), 'Why did russian social media swarm the digital conversation about catalan independence?'.
URL: https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/

Li, J. (2019), 'China's twitter operation focused on this exiled tycoon before hong kong protests'.
URL: https://qz.com/1700575/the-people-china-linked-twitter-accounts-aimed-at-before-hong-kong/

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'.

Lister, T. & Shukla, S. (2019), 'Russian mercenaries fight shadowy battle in gas-rich mozambique'.
URL: https://www.cnn.com/2019/11/29/africa/russian-mercenaries-mozambique-intl/index.html

Lister, T., Shukla, S. & Elbagir, N. (2019), 'Fake news and public executions: Documents show a russian company's plan for quelling protests in sudan'.
URL: https://www.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html

Ljubas, Z. (2020), 'Twitter axes 20,000 government-linked accounts, most from serbia'.
URL: https://www.occrp.org/en/daily/12004-twitter-axes-20-000-government-linked-accounts-most-from-serbia

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

Lytvynenko, J. & McDonald, L. (2019), 'Hundreds of propaganda accounts targeting iran and qatar have been removed from facebook'.
URL: https://www.buzzfeednews.com/article/janelytvynenko/uae-propaganda

Mac, R. & Adams, R. (2019), 'Have you seen these ads about hong kong's protests? china certainly hopes you have.'.
URL: https://www.buzzfeednews.com/article/ryanmac/hong-kong-protests-violent-facebook-twitter-ads-china-state

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

Mackinnon, A. (2017), 'Manipulating elections via twitter in armenia'.
URL: https://www.codastory.com/disinformation/in-armenia-a-snapshot-of-digital-manipulation-ahead-of-the-election/

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

Marshall, M. G. & Jaggers, K. (2020), Polity iv project: Political regime characteristics and transitions, Technical report.
URL: http://www.systemicpeace.org/inscr/p5manualv2018.pdf

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

Martin, D. A., Shapiro, J. N. & Nedashkovskaya, M. (2019), 'Recent trends in online foreign influence efforts', *Journal of Information Warfare* **18**(3), 15–48.

Martinez, M. (2018), 'Mexico election: Concerns about election bots, trolls and fakes'.
URL: https://www.bbc.com/news/blogs-trending-44252995

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

MilHojas (2015), 'Troll center: derroche y acoso desde las redes sociales'.
URL: http://milhojas.is/cms-front-noticias.php?id=612261

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

Monaco, N. & Nyst, C. (2018), 'State-sponsored trolling: How governments are deploying disinformation as part of broader digital harassment campaigns'.
URL: https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf

Morla, R. (2015), 'Correa's social-media troll center exposed in quito'.
URL: https://panampost.com/rebeca-morla/2015/03/25/correas-social-media-troll-center-exposed-in-quito/

Moyo, D. (2018), 'A vicious online propaganda war that includes fake news is being waged in zimbabwe'.
URL: https://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402

Mozur, P. (2018), 'A genocide incited on facebook, with posts from myanmar's military'.
URL: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

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

Mwareya, R. (2019), 'Meet the 'varakashi' - zimbabwe's online army'.
URL: https://www.iafrikan.com/2019/09/12/introducing-the-varakashi-zimbabwes-state-sponsored-online-army/

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*), 'Robot wars: How bots joined battle in the gulf', *Journal of International Affairs* **71**(1.5), 87–96.

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

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

Nimmo, B. (2019), Operators keen to hide their identities disseminated leaked uk/us trade documents in a similar fashion to russian operation "secondary infektion," exposed in june 2019, Technical report.
URL: https://public-assets.graphika.com/reports/graphika_report_uk_trade_leaks_updated_12.12.pdf

Nimmo, B., Aleksejeva, N., Karan, K. & Weimert, D. (2019), 'In depth: Iranian propaganda network goes down'.
URL: https://medium.com/dfrlab/takedown-details-of-the-iranian-propaganda-network-d1fad32fdf30

Nimmo, B. & Barojan, D. (2017), 'Fakes, bots, and blockings in armenia'.
URL: https://medium.com/dfrlab/fakes-bots-and-blockings-in-armenia-44a4c87ebc46

Nimmo, B., Barojan, D., Peñarredonda, J. L. & Karan, K. (2018), 'Electionwatch: Trending beyond borders in mexico'.
URL: https://medium.com/dfrlab/electionwatch-trending-beyond-borders-in-mexico-2a195ecc78f4

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., Francois, C., Eib, C. S. & Ronzaud, L. (2020), Return of the (spamouflage) dragon, Technical report.
URL: https://public-assets.graphika.com/reports/Graphika_Report_Spamouflage_Returns.pdf

Nimmo, B., Francois, C., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C. & Kostelancik, T. (2020), Secondary infektion, Technical report.
URL: https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

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

Nimmo, B. & Karan, K. (2019), 'Pakistan army's covert social network'.
URL: https://medium.com/dfrlab/pakistan-armys-covert-social-network-23ce90feb0d0

Nimmo, B. & Toler, A. (2018), 'The russians who exposed russia's trolls'.
URL: https://medium.com/dfrlab/the-russians-who-exposed-russias-trolls-72db132e3cd1

NPR (2019), 'Inside saudi arabia's disinformation campaign'.
URL: https://www.npr.org/2019/08/10/750086287/inside-saudi-arabias-disinformation-campaign

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

Peinado, F. (2019), 'Una red de cuentas falsas de twitter promueve a vox en campaña'.
URL: https://elpais.com/politica/2019/04/25/actualidad/1556203502_359349.html

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

Petreski, V. (2018), 'Electionwatch: Fascist falsification ahead of macedonian referendum'.
URL: https://medium.com/dfrlab/electionwatch-fascist-falsification-ahead-of-macedonian-referendum-77e9c15acdb7

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

Peñarredonda, J. L. & Karan, K. (2019), 'influenceforsale: Venezuela's twitter propaganda mill'.
URL: https://medium.com/dfrlab/influenceforsale-venezuelas-twitter-propaganda-mill-cd20ee4b33d8

Phuong, N. T. (2018), 'The truth about vietnam's new military cyber unit'.
URL: https://thediplomat.com/2018/01/the-truth-about-vietnams-new-military-cyber-unit/

Pinnell, O. (2018), 'The online war between qatar and saudi arabia'.
URL: https://www.bbc.com/news/blogs-trending-44294826

Ponce de León, E. & Pérez, D. S. (2020), 'Network of pro-maduro twitter accounts pushed anti-guaidó hashtags'.
URL: https://medium.com/dfrlab/network-of-pro-maduro-twitter-accounts-pushed-anti-guaid%C3%B3-hashtags-530f034f3628

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), '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

RadioTelevisionMartí (2020), '"me enfurece" y "contenidos emocionales": las presuntas instrucciones a las "ciberclarias"'.
URL: https://www.radiotelevisionmarti.com/a/me-enfurece-y-contenidos-emocionales-las-presuntas-instrucciones-a-las-ciberclarias-/264779.html

Revelli, A. & Foster, L. (2019), 'Network of social media accounts impersonates u.s. political candidates, leverages u.s. and israeli media in support of iranian interests'.
URL: https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html

Reynolds, N. (2019), 'Putin's not-so-secret mercenaries: Patronage, geopolitics, and the wagner group'.
URL: https://carnegieendowment.org/2019/07/08/putin-s-not-so-secret-mercenaries-patronage-geopolitics-and-wagner-group-pub-79442

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

RFE/RL (2019), 'Tajik students, educators claim they're pressured to 'troll' government critics'.
URL: https://www.rferl.org/a/tajik-students-educators-claim-they-re-pressured-to-troll-government-critics/29936072.html

Robertson, I., Karan, K. & Kaul, A. (2019), 'Facebook takes down inauthentic pages with connections to thailand'.
URL: https://medium.com/dfrlab/facebook-takes-down-inauthentic-pages-with-connections-to-thailand-7dbf331f5ba5

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/

Roose, K. (2017), 'Forget washington. facebook's problems abroad are far more disturbing.'.
URL: https://www.nytimes.com/2017/10/29/business/facebook-misinformation-abroad.html

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

Ross, A. (2019), 'How russia moved into central africa'.
URL: https://www.reuters.com/article/us-africa-russia-insight/how-russia-moved-into-central-africa-idUSKCN1MR0KA

Roth, Y. (2019), 'Information operations on twitter: principles, process, and disclosure'.
URL: https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

RSF (2020), 'Rsf unveils 20/2020 list of press freedom's digital predators'.
URL: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

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

Safi, M. (2016), 'India's ruling party ordered online abuse of opponents, claims book'.
URL: https://www.theguardian.com/world/2016/dec/27/india-bjp-party-ordering-online-abuse-opponents-actors-modi-claims-book

Saka, E. (2018), 'Social media in turkey as a space for political battles: Aktrolls and other politically motivated trolling', *Middle East Critique* **27**(2), 161–177.

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

Santora, M. & Barnes, J. (2018), 'In the balkans, russia and the west fight a disinformation-age battle'.
URL: https://www.nytimes.com/2018/09/16/world/europe/macedonia-referendum-russia-nato.html

Satariano, A. (2019), 'Facebook identifies russia-linked misinformation campaign'.
URL: https://www.nytimes.com/2019/01/17/business/facebook-misinformation-russia.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* .

SBSNews (2018), 'Macedonia to hold name-change referendum on september 30'.
URL: https://www.sbs.com.au/news/macedonia-to-hold-name-change-referendum-on-september-30

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

Schwirtz, M. & Borgia, G. (2019), 'How russia meddles abroad for profit: Cash, trolls and a cult leader'.
URL: https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html

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

Searcey, D. (2019), 'Gems, warlords and mercenaries: Russia's playbook in central african republic'.
URL: https://www.nytimes.com/2019/09/30/world/russia-diamonds-africa-prigozhin.html

Sepúlveda, A. (2019), 'Detallan movilización de 'trolls tuiteros' por los 'brothers' de fortaleza'.
URL: https://www.noticel.com/article/20190730/detallan-movilizacion-de-trolls-tuiteros-por-los-brothers-de-fortaleza/

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

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

Smith, R. (2019), 'Venezuelan bots, whatsapp and disinformation in spain'.
URL: https://firstdraftnews.org/latest/venezuelan-bots-whatsapp-and-disinformation-in-spain/

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

Squires, N. (2018), 'Russia 'orchestrating covert campaign to wreck macedonia name change vote".
URL: https://www.telegraph.co.uk/news/2018/09/27/russia-orchestrating-covert-campaign-wreck-macedonia-name-change/

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, E. (2019), 'How china used facebook, twitter, and youtube to spread disinformation about the hong kong protests'.
URL: https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media

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/

Strick, B. & Syavira, F. (2019), 'Papua unrest: Social media bots 'skewing the narrative".
URL: https://www.bbc.com/news/world-asia-49983667

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

TheShift (2018*a*), 'Behind the scenes: How labour online groups reacted to daphne caruana galizia's assassination'.
URL: https://theshiftnews.com/2018/05/24/behind-the-scenes-how-labour-online-groups-reacted-to-the-assassination-of-daphne-caruana-galizia/

TheShift (2018*b*), 'Investigating joseph muscat's online hate machine'.
URL: https://theshiftnews.com/2018/05/14/investigating-joseph-muscats-online-hate-machine/

Thomas, E. (2019*a*), 'Russian trolls are staging a takeover in africa—with help from mercenaries'.
URL: https://www.thedailybeast.com/yevgheny-prigozhins-russian-trolls-are-staging-a-takeover-in-the-central-african-republicwith-help-from-his-wagner-mercenaries

Thomas, J. (2019*b*), 'Cyber warfare in vietnam'.
URL: https://theaseanpost.com/article/cyber-warfare-vietnam

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/

Timberg, C. & Romm, T. (2019), 'It's not just the russians anymore as iranians and others turn up disinformation efforts ahead of 2020 vote'.
URL: https://www.washingtonpost.com/technology/2019/07/25/its-not-just-russians-anymore-iranians-others-turn-up-disinformation-efforts-ahead-vote/

Torres, A. & Vela, H. (2018), 'Twitter accounts masquerading as cubans spread socialist propaganda'.
URL: https://www.local10.com/news/2018/03/08/twitter-accounts-masquerading-as-cubans-spread-socialist-propaganda/

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

TuoiTreNews (2017), 'Vietnam has 10,000-strong 'cyber troop': general'.
URL: https://tuoitrenews.vn/news/politics/20171226/vietnam-has-10000strong-cyber-troop-general/43326.html

Twitter (2019), 'New disclosures to our archive of state-backed information operations'.
URL: https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html

Uren, T., Thomas, E. & Wallis, J. (2019), 'Tweeting through the great firewall'.
URL: https://www.aspi.org.au/report/tweeting-through-great-firewall

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), '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

Wallis, J., Uren, T., Thomas, E., Zhang, A., Hoffman, S., Li, L., Pascoe, A. & Cave, D. (2020), Evidence of russia-linked influence operations in africa, Technical report.
URL: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_0.pdf

Walsh, D. & Rashwan, N. (2019), "we're at war': A covert social media campaign boosts military rulers'.
URL: https://www.nytimes.com/2019/09/06/world/middleeast/sudan-social-media.html

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

Wendling, M. (2019), 'General election 2019: Reddit says uk-us trade talks document leak 'linked to russia"'.
URL: https://www.bbc.com/news/blogs-trending-50695558

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/

Wood, D., McMinn, S. & Feng, E. (2019), 'China used twitter to disrupt hong kong protests, but efforts began years earlier'.
URL: https://www.npr.org/2019/09/17/758146019/china-used-twitter-to-disrupt-hong-kong-protests-but-efforts-began-years-earlier

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

Yesil, B., Sözeri, E. K. & Khazraee, E. (2017), 'Turkey's internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance'.
URL: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1021&context=internetpolicyobservatory

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* .

Šajkaš, M. (2016), 'How influence of russian media risks making serbia a moscow bureau'.
URL: https://cpj.org/2016/10/how-influence-of-russian-media-risks-making-serbia/