Recent Trends in Online Foreign Influence Efforts

Diego A. Martin, Jacob N. Shapiro, Michelle Nedashkovskaya

Woodrow Wilson School of Public and International Affairs
Princeton University
Princeton, New Jersey, United States

E-mail: diegoam@princeton.edu
Email: jns@princeton.edu
E-mail: mpn@princeton.edu

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

Introduction
Information and Communications Technologies (ICTs) have changed the way people communicate about politics and access information on a wide range of topics (Foley 2004, Chigona et al. 2009). Social media in particular has transformed communication between leaders and voters by enabling direct politician-to-voter engagement outside traditional avenues, such as speeches and press conferences (Ott 2017). In the 2016 U.S. presidential election, for example, 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 technological developments, however, have also resulted in new challenges for democratic systems; foreign actors have sought to exploit ICTs to influence politics in a range of countries by promoting propaganda, advocating controversial viewpoints, and spreading disinformation. High-profile episodes of such foreign influence efforts (FIEs), such as Russian efforts to influence the outcomes of the 2016 U.S. presidential election, have prompted numerous studies on this subject (Boyd et al. 2018, Risch et al. 2018, Howard et al. 2018). Many of these studies, however, extrapolate from isolated examples of Russian efforts to polarize public opinion abroad (see Hegelich & Janetzko 2016, Connell & Vogler 2017, Hellman & Wagnsson 2017, among others).
We advance the literature by applying a consistent definition and set of coding criteria to the full set of identified FIEs since 2013. (The results described in this article were first discussed in our report Trends in Online Foreign Influence Efforts, released here in late-June 2019.) Drawing on a wide range of media reports, our data identified 53 FIEs in 24 targeted countries from 2013 through 2018. In total, 72% of the campaigns were conducted by Russia, with China, Iran, and Saudi Arabia accounting for most of the remainder. Our findings highlight the breadth of FIEs to date, suggest a small number of actors are launching these campaigns despite the fact that they are not technically challenging to conduct, and illustrate the broad spectrum of their political objectives. This paper, and the data described herein, offer high-level context for the growing literature about state-sponsored disinformation campaigns.

The remainder of the paper proceeds as follows. Section 2 describes the coding rules, inclusion criteria, and process for creating our data on FIEs. Section 3 provides descriptive statistics and highlights trends over time. Section 4 discusses implications of these trends and potential future research directions.

**Foreign Influence Effort Database**

We define FIEs 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, (iii) by producing content designed to appear indigenous to the target state. To be included in our data, FIEs must meet all three criteria.

Under this definition, FIEs are distinct from both traditional propaganda and disinformation (or ‘fake news,’ to use a colloquial term). The former involves political information provided by country X about country Y in ways which do not seek to mask its origin (such as Voice of America broadcasts about the U.S.S.R. during the Cold War) and may be true or false. Our definition also excludes local political activity, such as disinformation about country X produced by political actors in country X and spread on social media. Finally, the veracity of the content being promoted is not part of the definition. FIEs may involve promoting solely true content, solely false or misleading information, or some combination of the two.

**Data development**

Our data draw on a wide range of media reports to identify FIEs, track their progress, and classify their features. Drawing on more than 460 news articles (full list available), we identified 53 FIEs targeting at least 24 different countries from 2013 through 2018. We also looked for information in a wide range of previous academic research, building a database of 326 pieces studying online propaganda, influence operations and media consumption of voters (e.g. the Australian Strategic Policy Institute’s review of efforts to influence elections in democracies, Hanson et al. 2017). In total, 72% of the campaigns we identified were conducted by Russia. China, Iran, and Saudi Arabia accounted for most of the remainder. We also identified more than 40 distinct influence efforts which met some, but not all, of our inclusion criteria. In 2016, for example, Pro-Kremlin and Russian state-funded media wrote negative stories against NATO’s operation in Estonia, many of which contained clear falsehoods (Nimmo 2017). This information operation involved spreading incorrect information on social media but
was not an FIE under our definition because the content was not meant to appear as though it were produced in Estonia.

We built our data in three steps following standard practice:

1) **Develop a coding schema.** Our database reflects the influencer’s strategic decisions as well as operational choices that have to be made by any organization conducting multiple distinct influence campaigns over time (e.g. which platforms to target in a given effort), as the Russian Internet Research Agency (IRA) did from mid-2014 through at least 2018 (Mueller 2019, pp. 4-8, pp. 14-35). Such campaigns require country-specific strategies along several dimensions, including topics to post about, platforms to use, tactics to employ, and so on. Figure 1, below, summarizes the relational database we developed to categorize FIEs.


3) **Code values for all FIEs.** We identified 93 candidate FIEs across the sources described above. Of those, 53 met our inclusion criteria based on sources in English as well as Arabic, French, Spanish, and Russian, as appropriate. Each FIE was reviewed and evaluated by one of the authors as well as two student research assistants. The 53 identified cases from 2013 through the end of 2018 surely represent a lower bound on the number of distinct FIEs to date; media reporting in languages we could access may not have captured all FIEs within this time frame, and there may be some FIEs which went undetected.

Our methodology is similar to that of some other efforts. Bradshaw & Howard (2018), for example, report on domestically-produced propaganda in which 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 in that they look for information in the news, review the cases with help from a research team, and check the results with experts. Woolley & Howard (2017) use a different approach to study 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.

**Key fields**

Each FIE is identified as an attacker-target-political goal triple. This design allows us to draw
inferences about changes in tactics over time as well as the allocation of effort by attacking organizations, which must make tradeoffs between time spent on different political goals. For each FIE we record the following fields:

- **Political Goal.** Describes the objective of the effort. While we did not choose a fixed set of potential values for this variable, we sought homogeneity across countries in order to compare FIEs around the world.

- **Attacking Party.** The “Attacker” variable identifies one or more organizations and key individuals involved in each FIE. The “Actor” variable designates which types of organizations were involved in the FIE. We do not distinguish between which organizations directed the FIE and which carried it out given the difficulty of disentangling lines of authority with the available information.

- **Platform.** We record which media platforms were used in conducting the FIE, such as Facebook, Twitter, and so on. We do not judge the extent to which different platforms were used in carrying out the FIE.

- **Sources.** We provide brief descriptions of each event and a list of URLs for the main articles and reports relevant to that case. Only cases with at least three sources were included in the final database.

- **Strategy.** Records the overarching method(s) used in the attack, including defamation, persuasion, polarization, agenda shifting, or undermining political institutions.

- **Topic.** Contains a list of topics discussed within each FIE. As with “Political Goal,” it is an open-ended field created from patterns observed over time and across various attacks.

- **Approach.**Records measurable actions undertaken by actors to implement their strategies. These include three categories: amplifying existing content, creating new content, and producing distorted information about verifiable facts.

- **Tactics.** Identifies concrete actions used to pursue an approach, such as use of bots, fake accounts, stealing information, and trolling.

**Trends in Foreign Influence Efforts**

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

While we believe our attribution of targets is reliable, 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.

**Attackers and timing**

These efforts engaged various types of actors, platforms, strategies, approaches, and tactics, as illustrated in Table 1, which presents summary statistics of the FIE database from 2013-2018.
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). The efforts lasted for an average of 2.2 years; 70% of cases began between 2015 and 2017. Several FIEs were ongoing as of the end of 2018, including Russia promoting content undermining the Belarusian government and working to reduce support for the Donbas conflict among Ukrainian citizens.

Private companies (47%), media organizations (39%), and intelligence agencies (22%) were the most common actors involved in FIEs. Media reporting was insufficiently detailed to clearly identify the responsible actors in one fourth of FIEs. In the 2017 German federal election, for example, some posts seemingly created by U.S. social media users were suspected to be part of a Russian interference campaign (Hjelmgaard 2017). In such unclear cases, we do not assign responsibility to a specific actor.

**Strategies, approaches, and tactics**

FIEs have employed a wide range of strategies. While we do not see clear trends over time, our findings contradict the notion that FIEs are most often employed to polarize public opinion (see, for example, Aceves 2019.). The most commonly-used strategy is “defamation” (65%), defined as attempts to harm the reputation of people or institutions. The next most salient strategy is “persuasion” (55%), defined as trying to move the average citizen to one side of an issue. Notably, only 15% of FIEs used “polarization” — efforts to shift opinions to the extremes on one or more issues.

There is much less heterogeneity in which approaches have been used over time. Three in five cases employ all three approaches—“amplify,” “create,” and “distort”—in the same operation. Ninety-nine percent of the cases involved creation of original content, 78% amplification of pre-existing content, and 73% distortion of objectively verifiable facts (for specific examples of how different approaches were used in Russian FIE targeting the U.S., see, for example, Stewart et al. 2018).

We observed a great deal of variance in tactics employed, but few distinct trends over time. Approximately half of the attacks since 2014 employed automation, as seen in Figure 6, panel B. Just over half the FIEs used fake accounts, a number which has remained stable since 2014. We record a fake account as being involved only if one of the sources on the FIE directly makes that claim.

Twitter has been the most commonly-used platform (83%), followed by news outlets (66%), and Facebook (50%). Both Facebook and Twitter are commonly used by political supporters to distribute junk news (Narayanan et al. 2018). This pattern may reflect these platforms’ large market share and easy accessibility, which makes them ideal platforms for pushing propaganda masked as organic political activism. However, the apparent pattern may also be an artifact of these platforms’ transparency. Both Twitter and Facebook released a great deal of data about Russian attacks on the 2016 U.S. presidential election (NewsWhip 2018), making it easier to report how FIEs have used them. These platforms may be over-represented in our data as a result.

**Combinations across fields**

Table 2.1 displays the percentage of cases that involved each combination of two strategies. “Defame” and “persuade” (47%) was the most common combination, followed by “undermine institu-
tions” and “shift the political agenda” (33%). Analogously, Table 2.2 shows that trolling, bots, and hashtag hijacking (97%) were typically used together. Finally, Table 2.3 highlights that Twitter, Facebook, Instagram, and e-mail are used together most of the time.

**Figure 2** demonstrates “creation of new content” has been the most common approach every year. Since 2016, “amplification” has been more commonly used than “distortion.”

**Attacker patterns**
Panel A in **Figure 4** presents the number of attacks involving each type of actor from 2013 through 2018. Most attacks involved companies, foreign government officials, intelligence agencies, and media organizations. Panel B also highlights a shift from identified firms to unknown actors after 2015. This may reflect FIE actors’ increasing proficiency in masking their responsibility.

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

The share of attacks using various tactics has been relatively consistent since 2014, as **Figure 6**, panel B shows. Trolling is present in almost all FIEs (94% overall), but only approximately half of attacks in most years involve bots and fake accounts. Hashtag hijacking appears to steadily increase over time but even in recent years it was used in only 20% of FIEs.

Facebook, Twitter, and news outlets were the most common platforms for FIEs, as **Figure 7** shows. Other potential platforms included email, Google, fake websites, Line, and other media, such as radio, TV, newspapers, Reddit, Whatsapp, and Wikipedia. Instagram and Youtube have been used in an increasing share of attacks over time, as panel B shows. Despite these apparent trends, it is important to note the use of platforms in FIEs is distinct from the measure of user interaction with FIE content. Assessing the latter, Allcott et al. (2019) find that interactions with false content increased on Facebook between 2015 and 2016 but then decreased in the following two years.

**Attacking countries**
Russia has been the main country launching FIEs to date, as **Figure 3** demonstrates. By 2017 we estimate Russia had engaged in 29 distinct campaigns around the world. Iran was involved in 2 cases between 2014 and 2015, but steadily increased its activity through 2018, targeting 8 other nations. China, Iran, and Saudi Arabia each initiated FIEs during our study period. These findings are supported by other studies as well; Vilmer et al. (2018), for example, report European authorities attribute 80% of influence efforts to Russia, with the remaining 20% coming from China, Iran, and ISIS, a non-state actor.

Overall, Russia has conducted 14 distinct FIEs targeting the U.S.; three targeting Great Britain; two respectively against Australia, Germany, Netherlands, and Ukraine (one of which has been ongoing since 2015); and one FIE in each of the following countries: Austria, Belarus, Brazil, Canada, Finland, France, Italy, Lithuania, Poland, Sweden, South Africa, Spain, and Syria. Their
political goals have been diverse, as summarized below:

- **Discredit and attack:** American institutions, conservative critics of Trump, the Democratic party in U.S. presidential (2016) and midterm elections (2018), Emmanuel Macron in the 2017 French elections, Hillary Clinton in the 2016 U.S. presidential election, the White Helmets, Theresa May, and U.S. military operations in various locations around the world.
- **Polarize:** American politics (for example, by 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 U.S., Alternative for Germany (AfD) in the German federal elections (2017), Brexit referendum, Catalonia independence vote, Donald Trump in the 2016 U.S. presidential election, Donald Trump’s nominees for the U.S. 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, and the annexation of Crimea by the Russian Federation.
- **Undermine and reduce support:** for Angela Merkel and her political decisions, the Belarussian government, Sebastian Kurz after 2017 presidential elections in Austria, the Australian government, Barack Obama, the relationship between Poland and Ukraine.
- **Other political goals:** for instance, criticizing U.K. participation in the Syrian conflict; discrediting people identifying Russian propaganda; distorting perceptions of the relationship between Lithuania and Belarus; influencing Brazilian elections; influencing public opinion on various issues; promoting Russian propaganda; reducing support in Ukraine and Europe for Ukrainian action in the Donbas conflict; spreading false reports about a wide range of topics, including a chemical plant explosion in Louisiana, an Ebola outbreak, and a police shooting in Atlanta during the first half of 2011.

In the 2016 U.S. presidential elections, for example, Russian trolls promoted and attacked both Donald Trump and Hillary Clinton. Then-candidate Trump received more support and fewer attacks compared with Clinton (Nimmo & Karan 2018). During the same election and afterward, Russian-managed bots and trolls sought to push voters in opposite ideological directions on subjects such as race, immigration, healthcare policy, police violence, and gun control, among others. This strategy appears to have inspired Iranian trolls who pursued similar strategies, though no evidence has come to light of a company running operations as the Internet Research Agency did for Russia. Unlike Russian FIEs, Iranian trolls have attacked President Trump, the Republican party, and Secretary of State Mike Pompeo, though both have produced content supporting Brexit.

In the MENA region, both Russian and Iranian trolls have worked to obscure evidence of the Syrian government’s violence and to promote narratives favorable to the Syrian armed forces, while also pushing their own agendas (Barojan 2018b, Nimmo & Brookie 2018b). Iranian trolls have also attacked both the Israeli and Saudi Arabian governments (Kanishk et al. 2019). In Latin America, we found some evidence of influence efforts, but not with the level of coordination seen in the U.S., Europe, and the MENA region (Nimmo 2018a).
Online Appendix B to Trends in Online Foreign Influence Efforts provides brief summaries of each FIE included in our data.

**Discussion**

A great deal of media and scholarly attention has been devoted to Russian attacks on the 2016 U.S. presidential elections and to subsequent high-profile efforts to polarize American and European politics. Our research illustrates that FIEs are a much wider spread phenomenon.

When reviewing our data on FIEs, the ubiquity of attacks initiated by Russia presents an interesting puzzle. Despite the obvious similarities between widely understood techniques used in political campaigns and online marketing on the one hand, and the kinds of political influence efforts detailed above on the other, the set of countries employing FIEs remains small. Russian efforts still comprise the vast majority of such operations. Investigating the underlying drivers of this discrepancy may help further inform responses to FIEs while shedding light on the likelihood that a broader range of actors may employ them in the future.

Many seeking to explain the prevalence of Russian FIEs point to Russia’s long history of domestic information campaigns. The Russian government has interfered on Russian social networks for many years to divert attention from various social and economic problems (Sobolev 2019). Like others, we suspect this prior experience served as the basis for initiating campaigns around the world. Watts (2017), for example, argues that Soviet Active Measures strategies and tactics have been updated and enhanced for the modern Russian regime and the digital age. Blank (2013) also claims that its historical experience and legacy of Soviet thinking about information warfare has led Russia to view social media as a new means to conduct large-scale campaigns to reshape the thinking of entire political communities.

Media reporting supports this notion by illustrating the highly developed infrastructure supporting Russian FIEs. Workers at the Internet Research Agency (IRA), for example, were reportedly hierarchically organized according to English language proficiency and systematically reacted to daily political developments in the United States (Troianovski 2018). Existing scholarship also highlights the IRA’s sophisticated organization; DiResta et al. (2018), for example, provide an excellent analysis of the group’s operations in the U.S. from 2014 to 2017, and find these campaigns exploited political and social divisions between American voters through a combination of disinformation, hate speech, and promotion of true-but-divisive content.

Given the Russian government’s experience using information influence campaigns at home, it may be particularly effective at deploying them abroad. Beyond employing information-based FIEs, Russian efforts to shape politics in targeted countries have also included direct support for foreign political parties, especially right-wing parties in countries of geopolitical interest. In Germany, for example, Russia has supported the Alternative for Germany (AfD) party; and, in Italy, Russian-managed accounts supported the Five Star Movement (M5S) and far-right Lega Nord party. There are, however, also cases of Russia supporting left-wing movements, such as the Catalan independence effort in Spain. Rather than following a fixed political ideology, Russian FIEs appear highly pragmatic in pursuing their geopolitical goals.
Explanations for Russia’s frequent use of FIEs which rest on its particular expertise fall short when one considers that other countries do have such capacity. China, for example, has large, state-run media organizations that spread propaganda locally, as well as social media organizations which conduct influence operations on their own citizens (see, for example, Roberts 2018). Yet the country has not been nearly as active as Russia in conducting FIEs. This may be because their citizens do not commonly use the same media platforms as Westerners, making it more difficult to leverage their domestic organizations to run foreign operations. (Consistent with that interpretation, there have been campaigns targeting Chinese communities in Australia using Line and WeChat.) Or, it may reflect a strategic decision to avoid the negative international reaction to FIEs.

And other countries also clearly have the infrastructure to execute influence campaigns overseas should they wish to. In preliminary research, we have identified a number of Domestic Influence Efforts (DIEs) in which states target their own populations online using content intended to appear organic. Venezuelan President Nicolas Maduro, for example, has employed fake activity on social media to amplify his propaganda and attack opponents since at least 2015 (Forelle et al. 2015). The Venezuelan government deposited money on online applications to users who, after registering in a platform, would re-tweet or reply to messages from Twitter accounts such as “Tuíteros Patriotas” and “Patria Vé”, the latter of which published more than 95,600 tweets and was mentioned in almost 10 million tweets by approximately 4 million users (Peñarredonda & Karan 2019).

While FIEs by countries other than Russia have been less sophisticated, they have employed similar tools and techniques to attack democratic elections and day-to-day politics elsewhere (see, for example, Watts & Weisburd 2016, Kroet 2017, Watts 2017, Karp 2018, Nimmo & Brookie 2018a, Yourish et al. 2018, Zaveri & Fortin 2019). Iran, for example, used a range of strategies in attempts to undermine the political systems of its regional competitors. In contrast to Russian efforts, however, there is less evidence of coordination across different campaigns, and the participation of the Iranian government is less clearly documented. And recently revealed Saudi Arabian FIEs were on a much smaller scale and involved subcontracting to local marketing firms.

**Conclusion**

Foreign Influence Efforts (FIEs) have targeted at least 24 different countries around the world since 2013. While Russia has been the most active user of this new form of statecraft, other countries are following suit. Iran and China have deployed similar tactics beyond their own borders, and even democratic states such as Mexico appear to have adapted these techniques for internal purposes (Melendez 2018, Love et al. 2018, Linthicum 2018).

This paper provides useful background for those studying these trends. In conducting this work, we identified two major challenges that should inform future work:

- Lack of shared definitions: Developing a specific vocabulary for various types of influence operations would help in understanding and countering these issues. Currently, many investigations of influence campaigns focus on the nature of the content—such as “Fake News,” election interference, or bots and social media influence campaigns—without distinguishing between domestic influence efforts (DIEs), foreign influence efforts (FIEs),
and traditional propaganda campaigns. Each of the three entails distinct strategic considerations and may reflect different sets of political goals, strategies, and tactics. Future research should disaggregate various types of influence campaigns using specific and concrete definitions.

- Identification and Attribution: FIEs are subversive operations that are inherently challenging to detect and identify. Those challenges are magnified in conflict zones where reliable reporting mixes with intense propaganda campaigns to a greater extent than in peaceful situations. We studied several conflicts around the world, examining various sources in an attempt to attribute FIEs to specific country actors. The Syrian conflict, for example, has multiple players: the Syrian government; its allies; and multiple rebel groups, such as the Free Syrian Army (FSA) in Syria; as well as foreign parties such as Iran, Russia, Turkey, and the U.S. All of these players engage in information operations, some of which meet our definition of FIE. The study of influence campaigns in conflict zones would be enhanced if reporting on the social media landscape in these conflicts included more thorough consideration of which narratives were consistent with which actors’ political goals.

Future research should also seek to investigate the relationship between the employment of DIEs and FIEs by a given country. We suspect the evidence base on DIEs is modest right now because attribution efforts and reporting have focused on the role of foreign actors.

Furthermore, it is imperative that more work be done to investigate the impact of such campaigns on political behavior. While there has been some excellent work to date (for example, Guess et al. 2018, Eady et al. 2019), much more can be done. In particular, measuring political activity at scale over time via browser-tracking software or data from social media platforms can provide revealed preference measures of political information consumption. When matched with data on influence campaigns, such data could enable reliable estimation of short-term treatment effects.

Finally, reviewing reporting on FIEs and measures to combat them shows that much has already been done. During the 2018 U.S. 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). More could be done, however, to improve cooperation across platforms to combat influence efforts. As others have argued, a collective response that integrates actions by government, the private sector, and civil society groups will make it harder for foreign nations to interfere and shape the politics of their adversaries. The more difficult it is for inorganic activity to escape notice, the more expensive it will be for the Russian government and other actors to accomplish their goals. And while influencers can always move to new platforms, pushing them to more fringe sites will make it more expensive to reach a critical mass of voters, and thus less likely that the influencers will even try.

**Acknowledgements**

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

References


Aro, J. (2015), ‘Yle Kioski traces the origins of Russian social media propaganda – never-before-seen material from the troll factory’.


Recent Trends in Online Foreign Influence Efforts


Recent Trends in Online Foreign Influence Efforts


Recent Trends in Online Foreign Influence Efforts


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


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


Recent Trends in Online Foreign Influence Efforts


Recent Trends in Online Foreign Influence Efforts


34 Journal of Information Warfare


Recent Trends in Online Foreign Influence Efforts


Recent Trends in Online Foreign Influence Efforts


Troianovski, A. (2018), ‘A former Russian troll speaks: It was like being in Orwell’s world’. <https://www.youtube.com/watch?v=9CKYAzPhFAo>.


### Table 1: Summary statistics

<table>
<thead>
<tr>
<th>Variable</th>
<th>Freq.</th>
<th>Variable</th>
<th>Freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>First sighting</td>
<td></td>
<td>Last sighting</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>1</td>
<td>2013</td>
<td>0</td>
</tr>
<tr>
<td>2014</td>
<td>9</td>
<td>2014</td>
<td>1</td>
</tr>
<tr>
<td>2015</td>
<td>10</td>
<td>2015</td>
<td>1</td>
</tr>
<tr>
<td>2016</td>
<td>15</td>
<td>2016</td>
<td>7</td>
</tr>
<tr>
<td>2017</td>
<td>12</td>
<td>2017</td>
<td>12</td>
</tr>
<tr>
<td>2018</td>
<td>6</td>
<td>2018</td>
<td>32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Mean</th>
<th>Variable</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td></td>
<td>Platform</td>
<td></td>
</tr>
<tr>
<td>Astro turf</td>
<td>0.08</td>
<td>Email</td>
<td>0.08</td>
</tr>
<tr>
<td>Company</td>
<td>0.40</td>
<td>Facebook</td>
<td>0.57</td>
</tr>
<tr>
<td>Cyber espionage group</td>
<td>0.08</td>
<td>Fake websites</td>
<td>0.15</td>
</tr>
<tr>
<td>Foreign government</td>
<td>0.17</td>
<td>Google</td>
<td>0.17</td>
</tr>
<tr>
<td>Intelligence Agency</td>
<td>0.19</td>
<td>Instagram</td>
<td>0.21</td>
</tr>
<tr>
<td>Real NGO</td>
<td>0.04</td>
<td>Line</td>
<td>0.02</td>
</tr>
<tr>
<td>Wealthy individual</td>
<td>0.06</td>
<td>News outlets</td>
<td>0.64</td>
</tr>
<tr>
<td>Unknown</td>
<td>0.26</td>
<td>Other media</td>
<td>0.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reddit</td>
<td>0.09</td>
</tr>
<tr>
<td>Strategy</td>
<td></td>
<td>Tactic</td>
<td></td>
</tr>
<tr>
<td>Defame</td>
<td>0.64</td>
<td>Whatsapp</td>
<td>0.04</td>
</tr>
<tr>
<td>Persuade</td>
<td>0.57</td>
<td>Wikipedia</td>
<td>0.02</td>
</tr>
<tr>
<td>Polarize</td>
<td>0.15</td>
<td>Youtube</td>
<td>0.26</td>
</tr>
<tr>
<td>Shift agenda</td>
<td>0.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undermine institutions</td>
<td>0.06</td>
<td>Bot</td>
<td>0.53</td>
</tr>
<tr>
<td>Approach</td>
<td></td>
<td>Fake account</td>
<td>0.55</td>
</tr>
<tr>
<td>Amplify</td>
<td>0.77</td>
<td>Hashtag hijacking</td>
<td>0.17</td>
</tr>
<tr>
<td>Create</td>
<td>0.98</td>
<td>Other tactics</td>
<td>0.23</td>
</tr>
<tr>
<td>Distort</td>
<td>0.72</td>
<td>Steal information</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Troll</td>
<td>0.85</td>
</tr>
</tbody>
</table>

*Foreign influence efforts (FIEs) are defined as coordinated campaigns by one state to impact politics in another state through media channels, including social, in a manner which involves producing content that appears indigenous to the target state. In total, 53 FIEs. Each category is not mutually exclusive.*
### Table 2.1: Strategy combination

<table>
<thead>
<tr>
<th>Defame</th>
<th>Persuade</th>
<th>Polarize</th>
<th>Shift agenda</th>
<th>Undermine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defame</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persuade</td>
<td></td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polarize</td>
<td>9</td>
<td>3</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Shift agenda</td>
<td>6</td>
<td>7</td>
<td>12</td>
<td>100</td>
</tr>
<tr>
<td>Undermine</td>
<td>9</td>
<td>3</td>
<td>25</td>
<td>33</td>
</tr>
</tbody>
</table>

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

### Table 2.2: Tactic combination

<table>
<thead>
<tr>
<th>Bots</th>
<th>Fake account</th>
<th>#Hijacking</th>
<th>Other tactics</th>
<th>Steal info</th>
<th>Trolls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bots</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake account</td>
<td>65</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>#Hijacking</td>
<td>21</td>
<td>14</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other tactics</td>
<td>25</td>
<td>17</td>
<td>11</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Steal info</td>
<td>14</td>
<td>17</td>
<td>22</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>Trolls</td>
<td>93</td>
<td>90</td>
<td>100</td>
<td>58</td>
<td>86</td>
</tr>
</tbody>
</table>

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

### Table 2.3: Platform combination

<table>
<thead>
<tr>
<th>email</th>
<th>Facebook</th>
<th>Fake websites</th>
<th>Google</th>
<th>Instagram</th>
<th>Line</th>
<th>News outlets</th>
<th>Other media</th>
<th>Reddit</th>
<th>Twitter</th>
<th>Whasapp</th>
<th>Wikipedia</th>
<th>Youtube</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>75</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake websites</td>
<td>50</td>
<td>20</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>25</td>
<td>50</td>
<td>12</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td>0</td>
<td>30</td>
<td>25</td>
<td>44</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>News outlets</td>
<td>50</td>
<td>50</td>
<td>25</td>
<td>78</td>
<td>73</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other media</td>
<td>0</td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>7</td>
<td>0</td>
<td>16</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reddit</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>33</td>
<td>18</td>
<td>0</td>
<td>12</td>
<td>12</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td>100</td>
<td>87</td>
<td>100</td>
<td>88</td>
<td>91</td>
<td>0</td>
<td>70</td>
<td>75</td>
<td>100</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whasapp</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>12</td>
<td>0</td>
<td>5</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wikipedia</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>20</td>
<td>2</td>
<td>0</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Youtube</td>
<td>0</td>
<td>30</td>
<td>12</td>
<td>56</td>
<td>45</td>
<td>0</td>
<td>29</td>
<td>50</td>
<td>10</td>
<td>32</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>

The table shows the percentage of foreign influence efforts (FIEs) that use the platform of the row at the same time as the platform of the column. Numbers are the percentage rounded to the closest integer. Each category is not mutually exclusive. 53 FIEs.
Figure 1: Relational database structure
Recent Trends in Online Foreign Influence Efforts

Figure 2: Approach

![Figure 2: Approach](image)

Figure 3: Origin of the attacks

![Figure 3: Origin of the attacks](image)
Figure 4: Actors

Panel A. Total number of attacks per actor

Panel B. Share of attacks involving actors

Panel A shows the total number of foreign influence efforts (FIEs) per actor. Panel B presents the share of the number of efforts made by one actor on the total efforts in each year. For example, total number of FIEs using company in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive.
Figure 5: Strategy

Panel A: Total number of attacks per strategy

Panel B: Share of attacks involving strategies

Panel A shows the total number of foreign influence efforts (FIEs) per strategy. Panel B presents the share of the number of efforts made by one strategy on the total efforts in each year. For example, total number of FIEs using defame in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive.
Figure 6: Tactic

Panel A: Total number of attacks

Panel B: Share of attacks involving tactics

Panel A shows the total number of foreign influence efforts (FIEs) per tactic. Panel B presents the share of the number of efforts made by one tactic on the total efforts in each year. For example, total number of FIEs using trolls in 2014 divided by total number of cases in 2014. Each category is not mutually exclusive.
Figure 7: Platform

Panel A: Total number of attacks per platform

Panel B: Share of attacks involving platforms

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