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.
2) *Identify candidate influence efforts*. Once the coding scheme was developed, we examined 463 stories about influence efforts from 41 countries across a range of sources. We first reviewed material from major sources, including 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*. We then searched for additional information on media websites and expert blogs, including *Al-Monitor*, *Buzzfeed*, *Freedom House*, *Human Rights Watch*, *Medium* (including reports by DFRLabs), *Quartz*, *The Atlantic*, *The Daily Beast*, *The Daily Dot*, *The Hill*, *The Intercept*, *The New Republic*, *The Observer*, *The New Statesman*, *The Register*, and *The Verge*. Finally, we reviewed all working papers and articles by the Computational Propaganda Project of Oxford University and the Social Media and Political Participation (SMaPP) Lab of New York University.
3) *Code values for all FIEs*. We identified 93 candidate FIEs across the sources 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 Belarusian 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 "*Tuiteros Patriotas*" and "*Patria Ve*", 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

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', <https://www.thedailybeast.com/how-russia-exploits-american-white-suprema-cy-over-and-over-again?ref=author>.

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

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

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

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

Auchard, E. & Felix, B. (2017), 'French candidate Macron claims massive hack as emails leaked'. <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'. <https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G>.

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

Baroja, D. (2018), 'Troll tracker: Pro-Kremlin trolls deployed ahead of Syria strikes'. <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'. <https://medium. com/dfrlab/questionable-sources-on-syria-36fcabddc950>.

Barojan, D. (2018a), 'Balticbrief: NATO not planning to invade Belarus'. <https://medium.com/dfrlab/balticbrief-nato-not-planning-to-invade-belarus-d694d34f04ba>.

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

BBC (2017), 'Russia turns on Morgan Freeman over election 'war' video'. < https://www.bbc.com/news/world-europe-41348749>.

BBC (2018a), 'Jessikka Aro: Finn jailed over pro-Russia hate campaign against journalist'. <https://www.bbc.com/news/world-europe-45902496 >.

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

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

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

Bellingcat (2016), 'Behind the Dutch terror threat video: The St. Petersburg "troll factory" connection'. <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'. <https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons -and-ab-surdity-the-disinformation-campaign-against-the-white-helmets/>.

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

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

Bertrand, N. (2016), 'It looks like Russia hired Internet trolls to pose as pro-Trump Americans'. <https://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7>.

Black, P. (2018), 'Shocking Anakonda 2018 exercise's scenario'. <https://medium.com/@ paulblackjournalist/shocking-anakonda-2018-exercises-scenario-b8e58c1399ee>.

Blacktivist (2016), 'Republican investigation links Russian trolls to NODAPL movement'. <https://www.indianz.com/News/2018/03/01/republican-investigation -links-russian-t.asp>.

Blanco, P. (2019), '*Asıʹarruinaron los 'trolls' Rusos la vida de Jessikka Aro*'. <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), pp. 31-44.

Bogle, A. (2019), 'Twitter cracking down on political posts ahead of Australian election'. <https://www.abc.net.au/radio/programs/am/twitter-cracks-down-on-political-posts-ahead-of-election/10828096>.

Boyd, R. L., Spangher, A., Fourney, A., Nushi, B., Ranade, G., Pennebaker, J. & Horvitz, E. (2018), 'Characterizing the Internet research agency's social media operations during the 2016 US presidential election using linguistic analyses'.

Boylan, D. (2018), 'Fake news: Iranian propaganda reports of death of Saudi crown prince spark conspiracy theories'. <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'. <https://www.bbc.com/news/world-44070469>.

Brattnerg, E. & Maurer, T. (2018), 'Russian election interference: Europe's counter to fake news and cyber attacks'. <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'. <https://www. forbes.com/sites/thomasbrewster/2017/05/08/macron-emails-leaked-and-russia-is-the-chief-sus-pect/#6ec43ef168f4>.

Burgess, M. (2017), 'Here's the first evidence Russia used Twitter to influence Brexit'.<https://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency>.

Chen, A. (2015a), 'The agency'. <https://www.nytimes.com/2015/06/07/magazine/the-agency.html >.

Chen, A. (2015b), 'The agency'. <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?', T*he Electronic Journal of Information Systems in Developing Countries* 36(1), pp. 1-16.

Chulov, M. (2017), 'Sarin used in April Syria attack, chemical weapons watchdog confirms'. <https:!!www.theguardian.com!world!2017!jun!30!sarin-was-used-in -syria-khan-sheikhun-at-tack-says-chemical-weapons-watchdog>.

Clifton, D. (2017), 'Russian propagandists are pushing for Roy Moore to win'. <https:!! www.moth-erjones.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'. <https:!!sentinel.tw! chi-na-disinformation-tw!>.

Collins, B. & Wodinsky, S. (2018), 'Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist'.<https:!!www.nbcnews.com!tech!tech-news!exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871>.

Connell, M. & Vogler, S. (2017), Russia's approach to cyber warfare (1rev), Technical report, Center for Naval Analyses, Arlington,VA, US

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

Dave, P. & Bing, C. (2018), 'Facebook, Twitter dismantle disinformation campaigns tied to Iran and Russia'. <https:!!www.reuters.com!article!us-facebook-russia-usa!facebook -twitter-remove-pag-es-promoting-iranian-propaganda-idUSKCN1L62FD>.

Di Giovanni, J. (2017), 'Why Assad and Russia target the White Helmets'. <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'. <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'.<https:!!www.heraldscotland.com!news!16592877.fake-pro-independence-facebook-page-that-originated-in-iran-is-taken-down!>.

DiResta, R., Shaffer, D., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, D. & Johnson, B. (2018), 'The tactics & tropes of the Internet Research Agency'. <https:!! cdn2.hubspot. net!hubfs!4326998!ira-report-rebrand FinalJ14 .pdf >.

Eady, G., Nagler, J., Guess, A., Zilinsky, J. & Tucker, J. A. (2019), 'How many people live in political bubbles on social media? Evidence from Linked survey and Twitter data', *SAGE Open* 9(1).

Elliot, H. (2018), 'Twitter reportedly suspends network of bots pushing pro-Saudi disinformation on suspected Khashoggi murder'. <https://slate.com/news-and-politics/2018/10/twitter-reportedly-suspends-network-of-bots-pushing-pro-saudi-disinformation-on-suspected-khashoggi-murder.html>.

Emmott, R. (2017), 'Spain sees Russian interference in Catalonia separatist vote'. <https://www. reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalo-nia-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), pp. 50-61.

EUvsDisinfo (2019), 'Results of 2018 "EU versus disinformation" screening: Ukraine remains under fire through disinformation'. <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'. <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'. <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), pp. 139-46.

Forelle, M., Howard, P., Monroy-Hernndez, A. & Savage, S. (2015), 'Political bots and the manipulation of public opinion in Venezuela', *arXiv preprint arXiv:1507.07109*.

Frenkel, S. & Wakabayashi, D. (2018), 'After Florida school shooting, Russian 'bot' army pounced'. <https://www.nytimes.com/2018/02/19/technology/russian-bots-school -shooting.html>.

Friedersdorf, C. (2017), 'Is Russia behind a secession effort in California?'. <https://www.theatlan-tic.com/politics/archive/2017/03/is-russia-behind-a-secession-effort-in-california/517890/>.

Fubini, F. (2018), 'Tweet *populisti dalla* Russia *sulla politica Italiana. come negli* USA'. <https://www.corriere.it/politica/18 agosto 01/tweet-populisti-russia-voto-italiano-come-usa-f33df26c-95cc-11e8-819d-89f988769835 .shtml?refresh ce-cp>.

Gleicher, N. (2018a), 'Coordinated inauthentic behavior explained'. <https://newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/>.

Gleicher, N. (2018b), 'More information about last week's takedowns'. <https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/>.

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

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

Gomez, L. (2017), 'A Russian twitter bot promoted California secession, or Calexit'. <https://www.sandiegouniontribune.com/opinion/the-conversation/sd-russian-bot-pushed-calexit-move-ment-20171102-htmlstory.html>.

Gordon, G. (2018), 'Fake, misleading social media posts exploding globally, Oxford study finds'. <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'. <https://www.independent.co.uk/life-style/gadgets-and-tech/news/angela-merkels-instagram-bombarded-with-abuse-from-russian-troll-army -10303425.html>.

Guess, A., Nyhan, B. & Reifler, J. (2018), 'Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 US presidential campaign', *European Research Council* 9.

Guynn, J. (2018a), 'Facebook foils political influence campaigns originating in Iran, Russia ahead of U.S. midterms'. <https://www.usatoday.com/story/tech/2018/08/21/facebook-foils-political-in-fluence-campaigns-originating-iran-russia-ahead-u-s -midterms/1058233002/>.

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

Hegelich, S. & Janetzko, D. (2016), *Are social bots on Twitter political actors? Empirical evidence from a Ukrainian social botnet*, in 'Tenth International AAAI Conference on Web and Social Media'.

Hellman, M. & Wagnsson, C. (2017), 'How can European states respond to Russian information warfare? An analytical framework', *European Security* 26(2), pp. 153-70.

Henley, J. (2017), 'Russia waging information war against Sweden, study finds'. <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'.<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'. <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'. <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'. <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'. <https://assets.documentcloud.org/documents/5011321/Khusyaynova-Complaint.pdf>.

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J. & Francois, 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'. <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'. <https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html>.

Isikoff, M. (2019), 'Exclusive: The true origins of the Seth Rich conspiracy theory. a yahoo news investigation'. <https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html>.

Jazeera, A. (2017), 'Syria forces behind Khan Sheikhoun gas attack: Un probe'. <http://www.al-jazeera.com/news/2017/09/syria-forces-khan-sheikhoun-gas-attack-probe-170906115601017. html>.

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.

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

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

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

Kist, R. (2018), 'The fight against the trolls hardens'. <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'. <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'. <https://www.thedailybeast.com/mh17-russia-deployed-its-trolls-to-cover-up-the-murder-of-298-people?ref=home>.

Kroet, C. (2017), 'Russian fake news campaign targets Merkel in German election'. <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)'. <https://9gag.com/u/rudiskronitis>.

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

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

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

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

Linvill, D. L. & Warren, P. L. (2018), 'Troll factories: The Internet Research Agency and state-sponsored agenda building'.

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

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

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

Mason, M. (2018), 'Intelligence officials plan to repel fake news in Australian federal election'.<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'. <https://www.newsweek.com/brett-kavanaugh-has-huge-opposi-tion-us -russian-state-propaganda-loves-donald-1155046>.

Mele, C. (2017), 'Morgan Freeman angers Russians over video about 2016 election'. <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'. <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'. <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'. <https://www.reuters.com/article/us-france-russia-idUSKBN18P030>.

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

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

Muller, R. (2018), 'Conspiracy to commit an offense against the United States'. <https://www.jus-tice.gov/storage/report.pdf>.

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

Nassetta, J. & Fecht, E. (2018), *All the world is staged: An analysis of social media influence operations against US counterproliferation efforts in Syria*, Technical report, Middlebury Institute of International Studies at Monterey. <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'. <https://www.npr.org/sections/thetwo-way/2018/03/01/589787931/russias-fancy-bear-reported-ly-hacks-german-government-networks>.

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

NewsWhip (2018), 'Navigating the Facebook algorithm change: 2018 report.' <http://go.news-whip.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'. <https://medium.com/dfrlab/russian-nar-ratives-on-natos-deployment -616e19c3d194>.

Nimmo, B. (2018a), 'Iran's suspected information operation. assessing the main pages and accounts traced to Tehran by Fireeye'. <https://medium.com/dfrlab/trolltracker-irans-suspected-infor-mation-operation-153fc7b60126>.

Nimmo, B. (2018b), 'Putinatwar: Trolls on Twitter'. <https://medium.com/dfrlab/putinat-war-trolls-on-twitter-5d0bb3dc30ae>.

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

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

Nimmo, B. & Brookie, G. (2018b), 'Trolltracker: Facebook uncovers Iranian influence operation Iranian narratives buried in divisive content target United States and United Kingdom'. <https://medium.com/dfrlab/trolltracker-facebook-uncovers-iranian-influence-operation-d21c73cd71be>.

Nimmo, B., Brookie, G. & Karan, K. (2018a), 'Trolltracker: Twitter troll farm archives. Part one: Seven key take aways from a comprehensive archive of known Russian and Iranian troll operations'. <https://medium.com/dfrlab/trolltracker-twitter-troll-farm-archives-8d5dd61c486b>.

Nimmo, B., Brookie, G. & Karan, K. (2018b), 'Trolltracker: Twitter troll farm archives. Part three: Assessing an covert Iranian social media influence campaign'. <https://medium.com/dfrlab/troll-tracker-twitters-troll-farm-archives-17a6d5f13635>.

Nimmo, B., Brookie, G. & Karan, K. (2018c), 'Trolltracker: Twitter troll farm archives. Part two. How the Internet Research Agency regenerated on Twitter after its accounts were suspended'. <https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-8be6dd793eb2>.

Nimmo, B. & Francois, C. (2018), 'Trolltracker: Glimpse into a French operation'. <https://medi-um.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924>.

Nimmo, B. & Karan, K. (2018), 'Trolltracker: Favorite Russian troll farm sources. Measuring the websites and accounts the Internet Research Agency shared most'. <https://medium.com/dfrlab/trolltracker-favorite-russian-troll-farm-sources-48dc00cdeff>.

NWS (2018), 'Russian trolls active in Belgium and the Netherlands'. <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'. <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'. <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), pp. 59-68.

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

Peisakhin, L. & Rozenas, A. (2018), 'When does Russian propaganda work — and when does it backfire?'. <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'.<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'. <https://ww.kommersant.ru/doc/3607961#comments>.

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

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

Poulsen, K. (2018), 'Mueller finally solves mysteries about Russia's 'fancy bear' hackers'. <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'. <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'. <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'. <https://www.then-ational.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'. <https://www.businessinsider.sg/facebook-detects-information-campaigns-russia-iran-2018-8/>.

Radio, S. (2016), 'Russia's propaganda efforts underscored in Sapo report'. <https://sverigesradio. se/sida/artikel.aspx?programid=2054&artikel=6391875>.

RFE (2018), 'Russian trolls found amplifying U.S. Republican charge against FBI'. <https://www. rferl.org/a/russian-trolls-amplify-us-republican-charge-anti-trump-bias-at-fbi-/28986362.html>.

Risch, J. E., Rubio, I. M., Johnson, R., Flake, J., Gardner, C., Young, T., Barrasso, J., Isakson, J., Portman, R., Paul, R., Cardin, B. L., Menendez, R., Shaheen, J., Coons, C. A., Udall, T., Murphy, C., Kaine, T., Markey, E. J., Merkley, J. & Booker, C. A. (2018), *Putin's asymmetric assault on democracy in Russia and Europe: Implications for US national security*, Technical report.

Roberts, M. (2018), *Censored: Distraction and Diversion Inside China's Great Firewall*, Princeton University Press.

Rocha, R. (2018), 'Data sheds light on how Russian twitter trolls targeted Canadians'. <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'. <https://www.washingtonpost.com/technology/2018/12/22/facebook-suspends-five-accounts-including-social-media-researcher-mis-leading -tactics-alabama-election/?utm term=.8c4df3c6ce55>.

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

RT (2018), 'Russians view US, Ukraine and EU as country's main enemies – survey'. <https://www. rt.com/russia/415487-russians-us-ukraine-eu-enemies/>.

Ruediger, M. (2018), 'Electionwatch: FGV DAPP uncovers foreign Twitter influence in Brazil'. <https://medium.com/dfrlab/electionwatch-fgv-dapp-uncovers-foreign-twitter-influence-in-bra-zil-7ab24e34223>.

Sanger, D. E. (2018), 'Mystery of the midterm elections: Where are the Russians?'. <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'. <https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html>.

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

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

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

Schafer, B. (2017), 'Dashboards Hamilton 68 and Artikel 38'. <https://ecuringdemocracy.gmfus.org/securing-democracy-dispatch-10/>.

Sear, T. & Jensen, M. (2018), 'Russian trolls targeted Australian voters on Twitter via Auspol and MH17'. <https://theconversation.com/russian-trolls-targeted-australian-voters-on-twitter-via-aus-pol-and-mh17-101386>.

Shane, S. & Blinder, A. (2018), 'Secret experiment in Alabama senate race imitated Russian tactics'. <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'. <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'. <https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-be-came-a-global-hub-for-pro-trump-misinfo#.fu2okXaeKo>.

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

Snegovaya, M. (2017), 'Russian propaganda in Germany: More effective than you think'. <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'. <https://www.theguardian.com/world/2017/dec/18/syria-white-helmets -conspiracy-theories>

Soshnikov, A. (2017), 'Inside a pro-Russia propaganda machine in Ukraine'. <https://www.bbc.com/news/blogs-trending-41915295>.

Staff, M. (2018), 'Russia driving huge online "disinformation" campaign on Syria gas attack, says UK'. <https:!!www.middleeasteye.net!news!russia-driving-huge-online-disinformation-cam-paign-syria-gas-attack-says-uk>.

Stein, J. (2018), 'Tammy Baldwin seeks hearing after Russians pushed image of Obama in noose at Badgers game'. <https:!!www.jsonline.com!story!news!politics!2018!03!21!tammy-baldwin-calls-twitter-troll-hearing-russians-pushed-wisconsin -image-obama-noose!446618002!>.

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

Stojanovski, F. (2017), 'Fake news tries to link Austria's chancellor-to-be and philanthropist George Soros'. <https:!!www.stopfake.org!en!fake-news-tries-to-link-austria-s-chancellor-to-be-and-philanthropist-george-soros!>.

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

Subramanian, S. (2017), 'The Macedonian teens who mastered fake news'. <https:!!www.wired.com!2017!02!veles-macedonia-fake-news!>.

Summers, J. (2017), 'Countering disinformation: Russia's infowar in Ukraine'. <https:!! jsis.wash-ington.edu!news!russia-disinformation-ukraine!>.

Superlinear (2018), 'Social media disinformation: parallels between the US and South African experiences'. <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'.<https:!!www.manufacturing.net!news!2015!06!report-russian-internet-trolls-behind-louisiana-chemical-explosion-hoax>.

Szymánski, P. (2018), 'Finland: the fight against disinformation'. <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?'.<https:!!www.lawfareblog.com!macron-leaks-are-they-real-and-it-russia>.

Timberg, C. & Romm, T. (2018), 'These provocative images show Russian trolls sought to inflame debate over climate change, fracking and Dakota pipeline'. <https:// www.washingtonpost.com/

news/the-switch/wp/2018/03/01/congress-russians-trolls-sought-to-inflame-u-s-debate-on-climate-change-fracking-and-dakota-pipeline/>.

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

van der Noordaa, R. & van de Ven, C. (2019), 'The MH17 plot'. <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'. <https://www.reuters.com/article/us-france-election-cyber/u-s-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks -researchers-idUSKBN1820QO>.

Watts, C. (2017), 'Clint Watts' testimony: Russia's info war on the U.S. started in 2014'. <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'. <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'. <https://the-hill.com/policy/healthcare/406309-nearly-600-russian-troll-accounts-tweeted-about-obamacare-report>.

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

Withnall, A. (2018), 'Finland: Russian propaganda questioning our validity risks destabilising country'. <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'. <https://www.cnet.com/news/facebook-announces-removal-of-iranian-influence-cam-paign-as-midterms-near/>.

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

Yaron, O. (2018), 'Tel-Aviv times? Iran created fake Hebrew news sites in major "influence campaign"'.<https://www.haaretz.com/israel-news/.premium-israeli-cyber-security-compa-ny-iran-created-fake-hebrew-news-sites-1.6463020>.

Yong, C. (2018), 'Select committee on fake news: Russian trolls divided societies and turned countries against one another'. <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'. <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'. <https://www.nytimes.com/2019/05/06/us/russia-disinformation-black -activists.html>.

Table 1: Summary statistics

Variable	Freq.	Variable	Freq.
First sighting		Last sighting	
2013	1	2013	0
2014	9	2014	1
2015	10	2015	1
2016	15	2016	7
2017	12	2017	12
2018	6	2018	32

Variable	Mean	Variable	Mean
Actor		Platform	
Astroturf	0.08	Email	0.08
Company	0.40	Facebook	0.57
Cyber espionage group	0.08	Fake websites	0.15
Foreign government	0.17	Google	0.17
Intelligence Agency	0.19	Instagram	0.21
Real NGO	0.04	Line	0.02
Wealthyindividual	0.06	News outlets	0.64
Unknown	0.26	Other media	0.15
		Reddit	0.09
Strategy		Twitter	0.83
Defame	0.64	Whatsapp	0.04
Persuade	0.57	Wikipedia	0.02
Polarize	0.15	Youtube	0.26
Shift agenda	0.06		
Undermine institutions	0.06	Tactic	
		Bot	0.53
Approach		Fake account	0.55
Amplify	0.77	Hashtag hijacking	0.17
Create	0.98	Other tactics	0.23
Distort	0.72	Steal information	0.13
		Troll	0.85

Foreign influence efforts (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

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

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

Table 2.2: Tactic combination

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

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

Table 2.3: Platform combination

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

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

Figure 1: Relational database structure

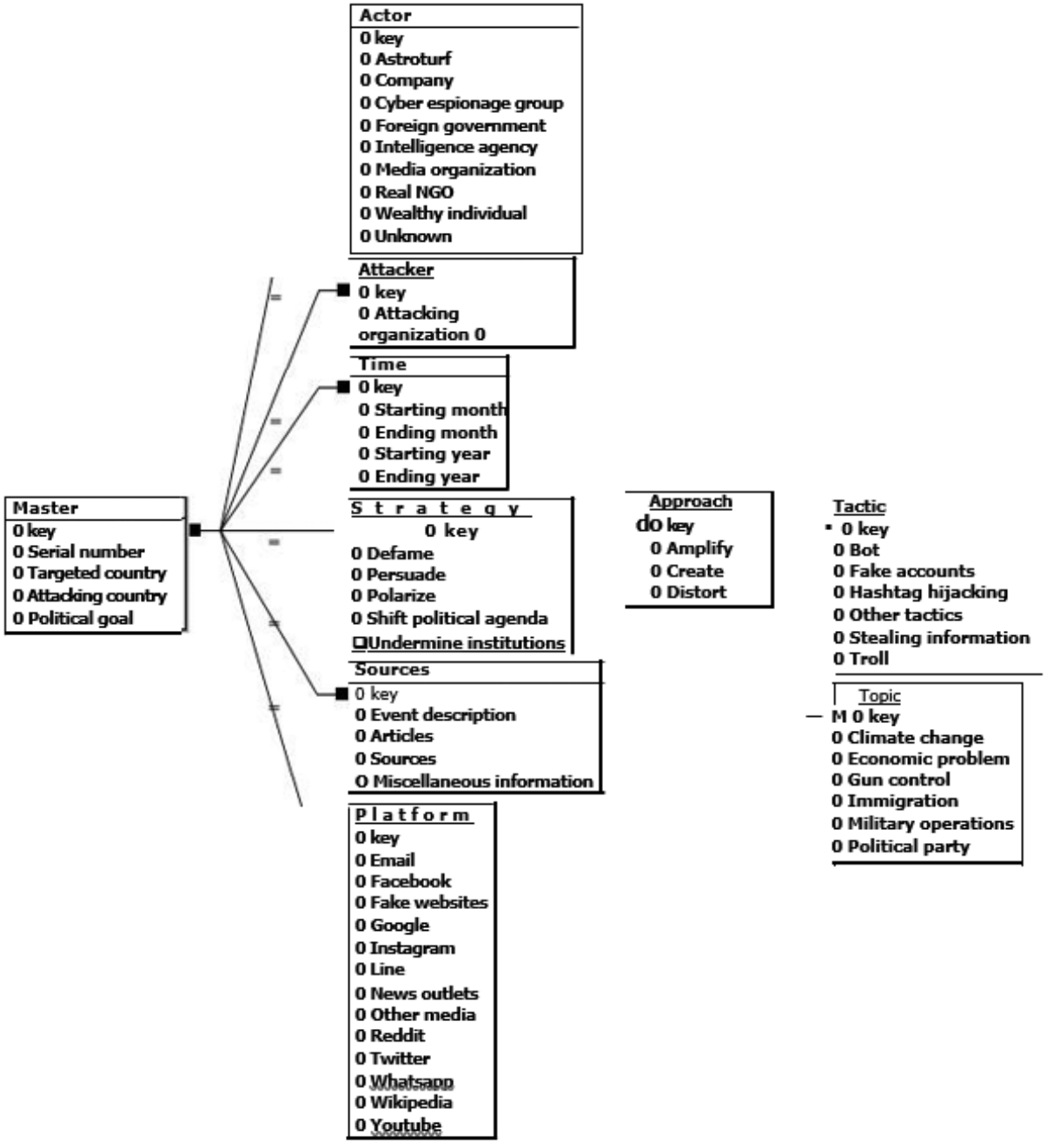


Figure 2: Approach

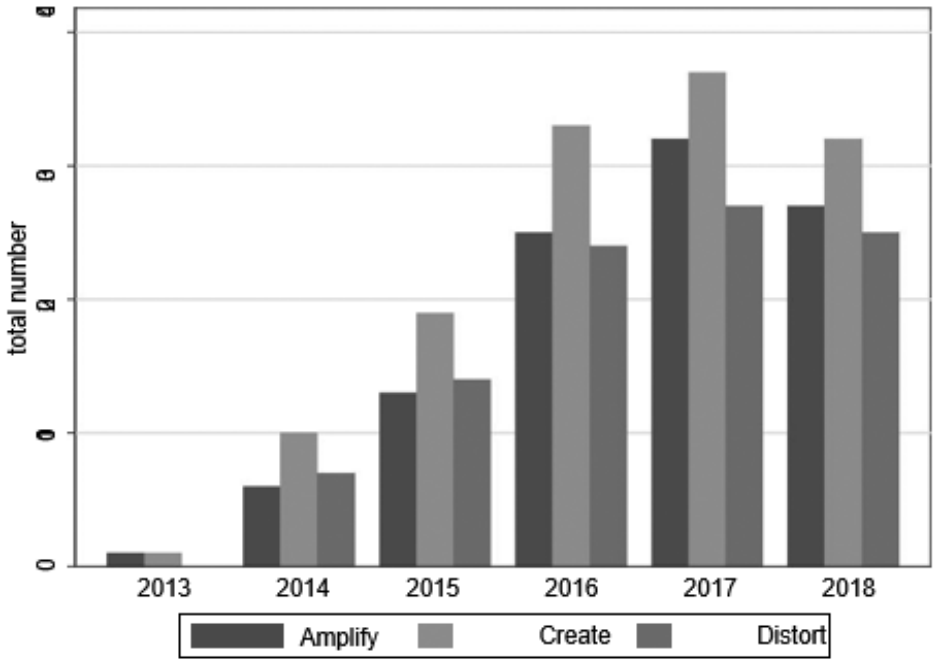


Figure 3: Origin of the attacks

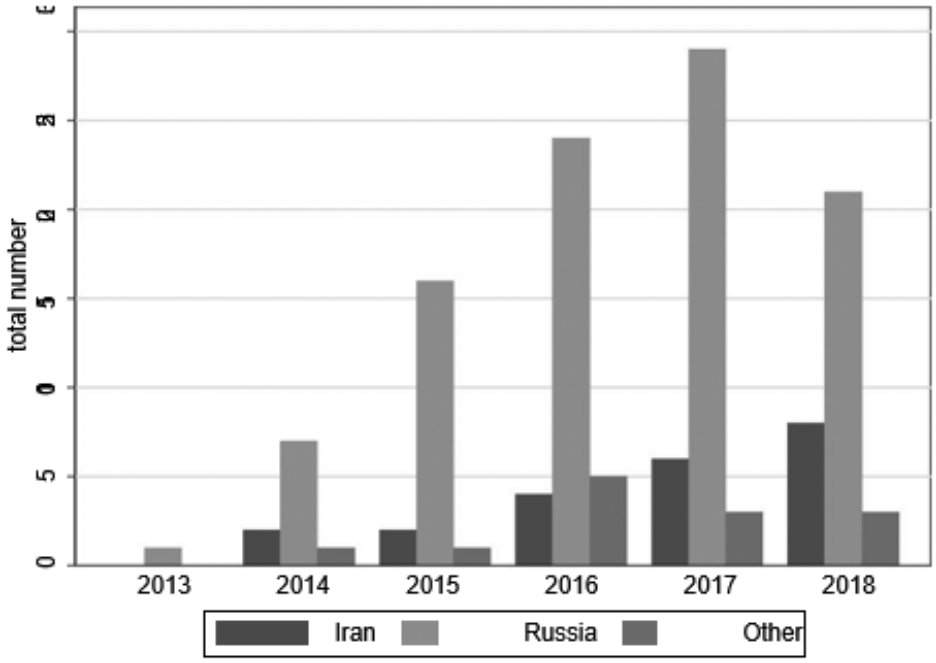
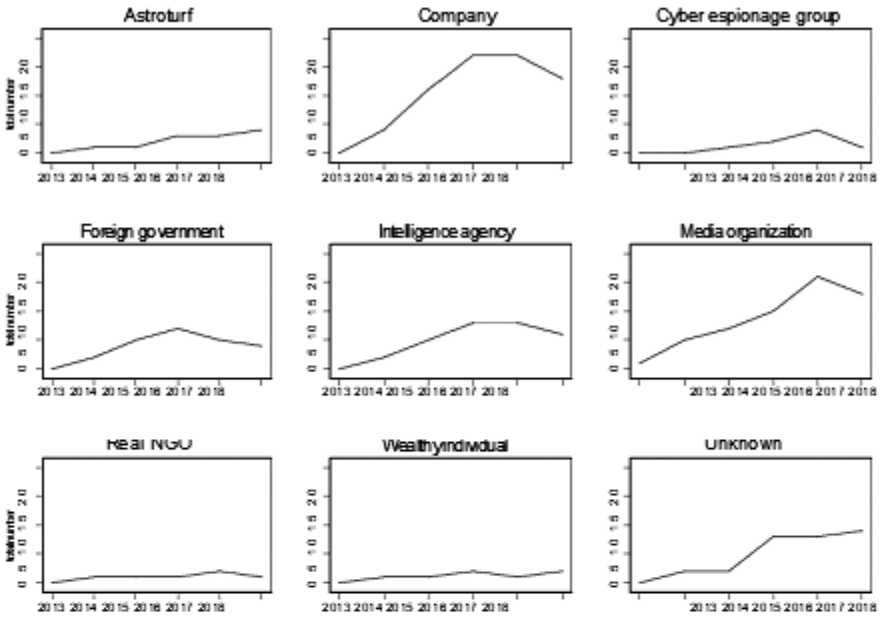
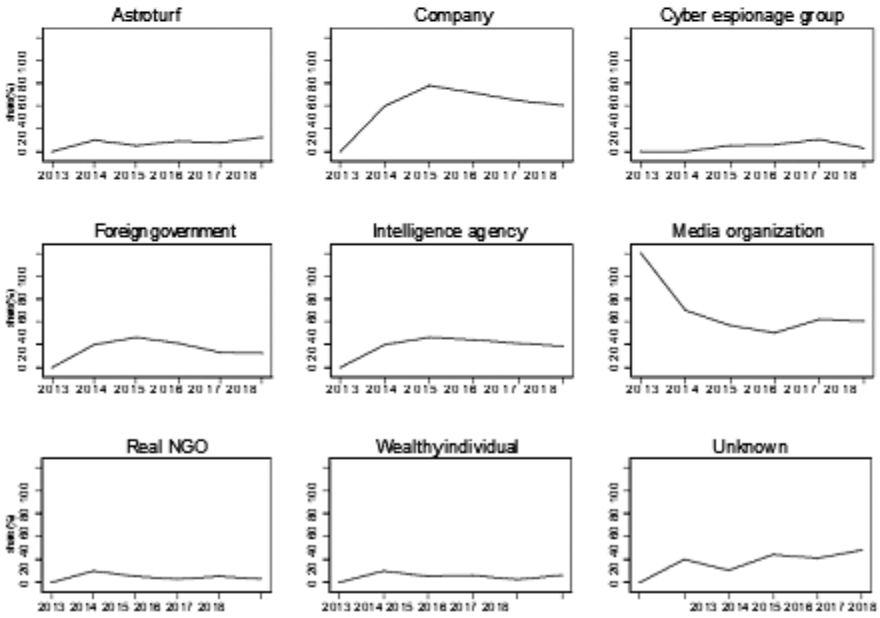


Figure 4: Actors

Panel A: Total number of attacks per actor



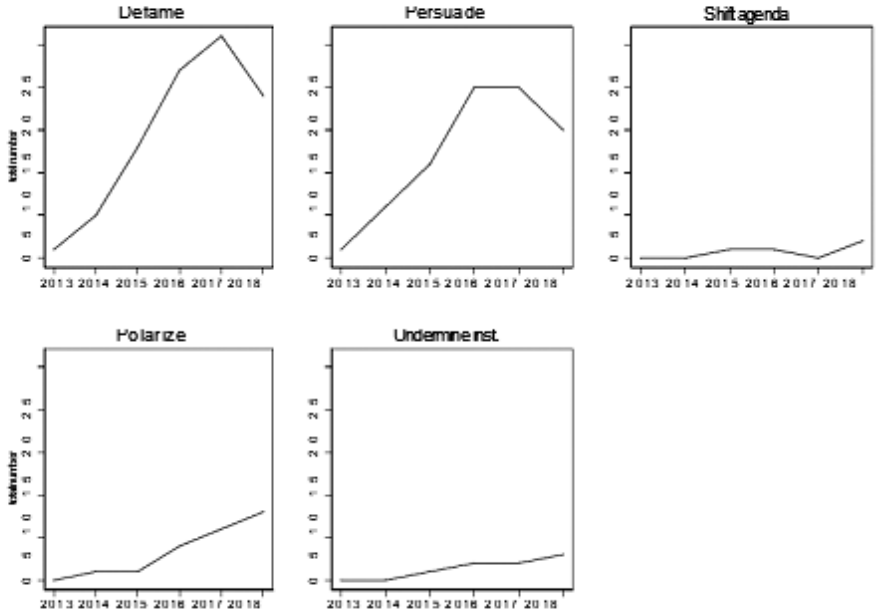
Panel B: Share of attacks involving actors



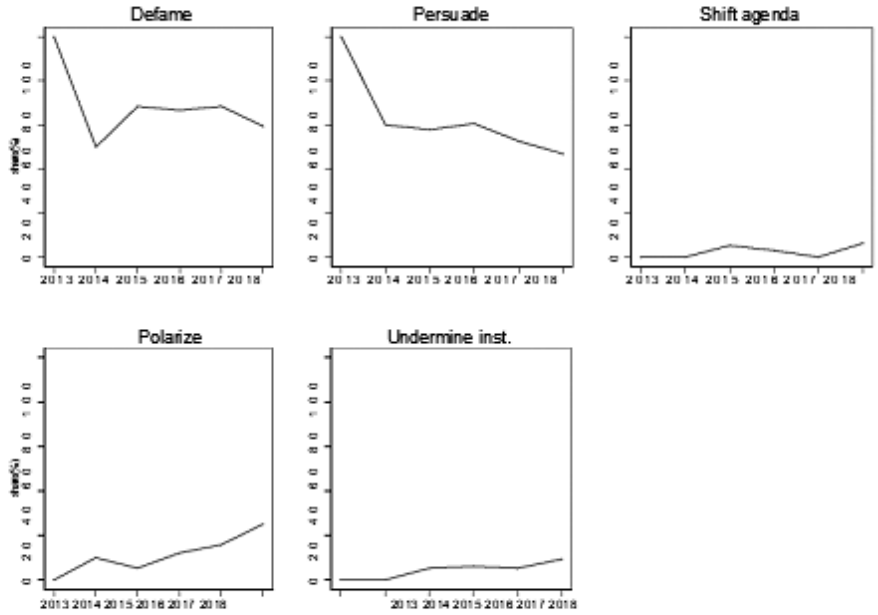
Panel A shows the total number of foreign influence efforts (FIEs) per actor. Panel B presents the share of the number of efforts made by one actor on the total efforts in each year. For example, total number of FIEs using company in 2014 divided by total number of cases in 2014. Each category is not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

Figure 5: Strategy

Panel A: Total number of attacks per strategy

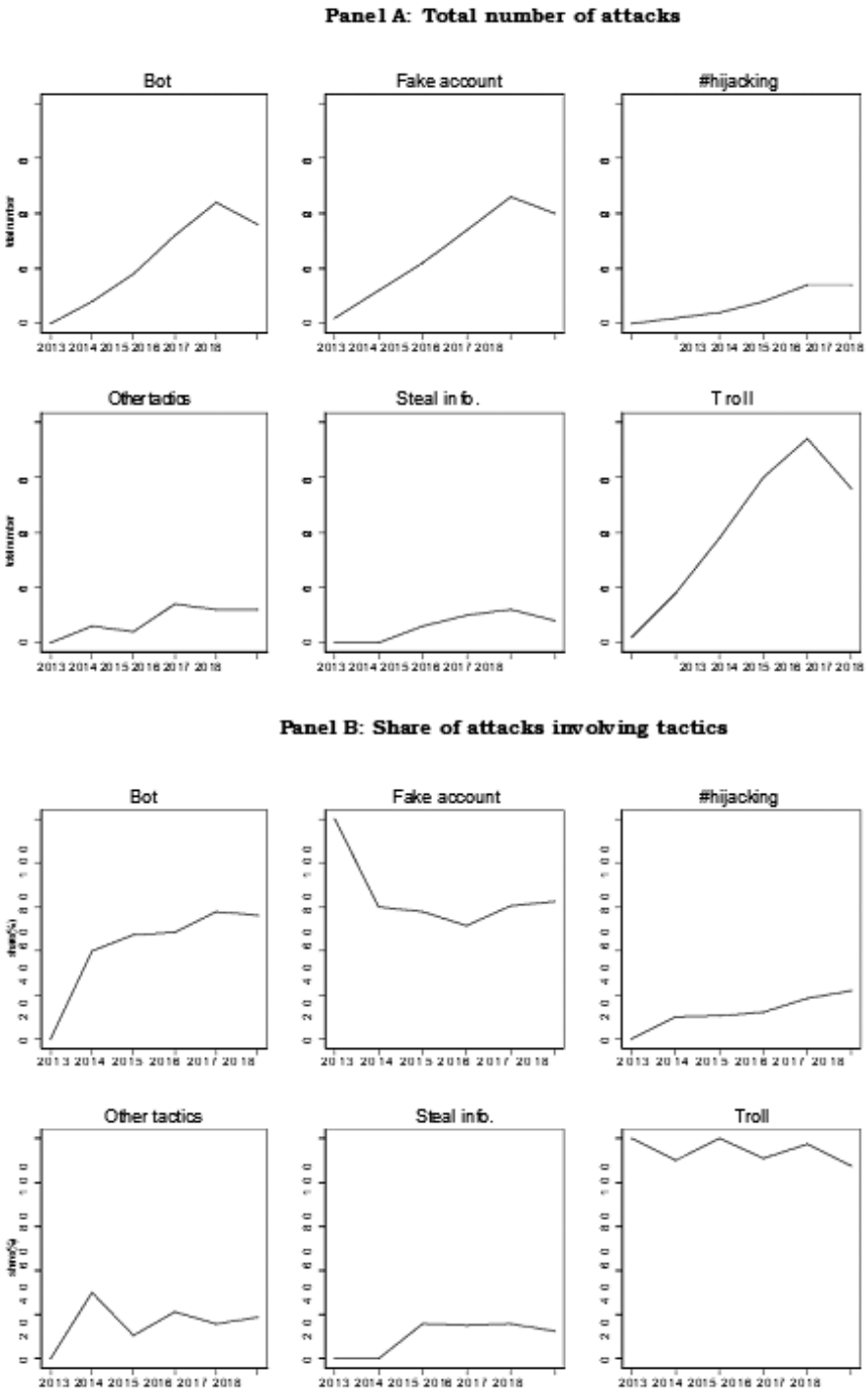


Panel B: Share of attacks involving strategies



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.

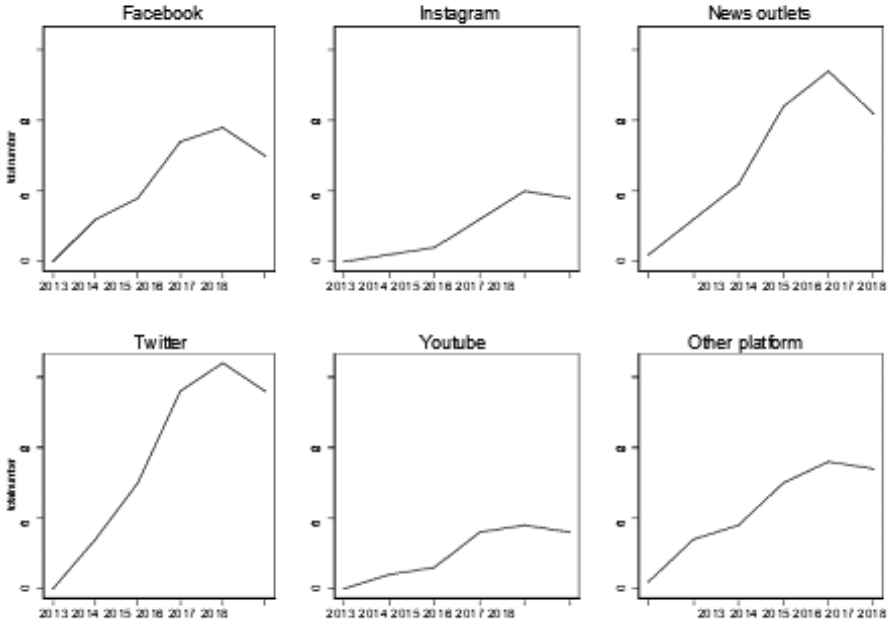
Figure 6: Tactic



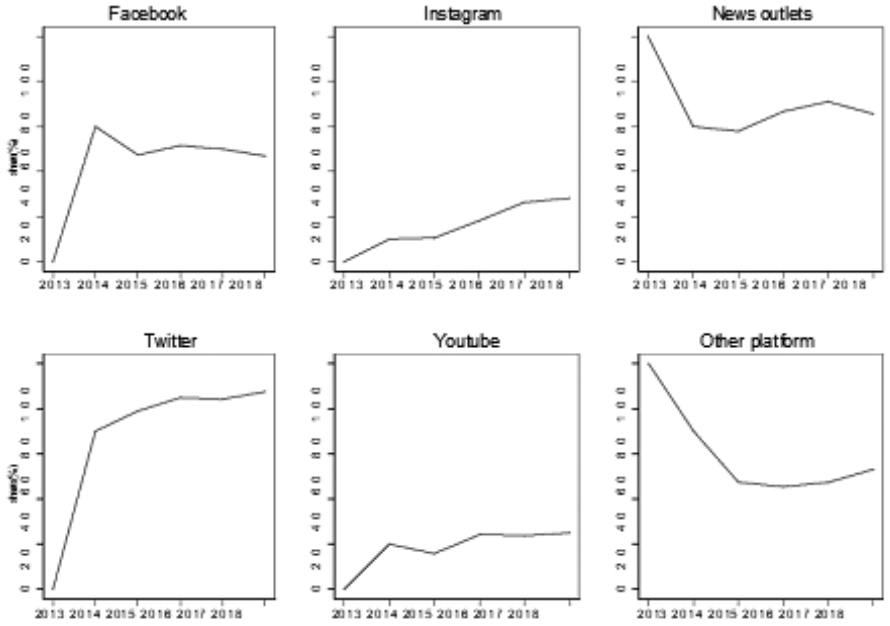
Panel A shows the total number of foreign influence efforts (FIEs) per tactic. Panel B presents the share of the number of efforts made by one tactic on the total efforts in each year. For example, total number of FIEs using trolls in 2014 divided by total number of cases in 2014. Each category is not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