Online Appendix for Online Political Influence Efforts Dataset Version 3.0

(not for publication)

Diego A. Martin* Jacob N. Shapiro† Julia G. Ilhardt‡

Last revised: December 7, 2021

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

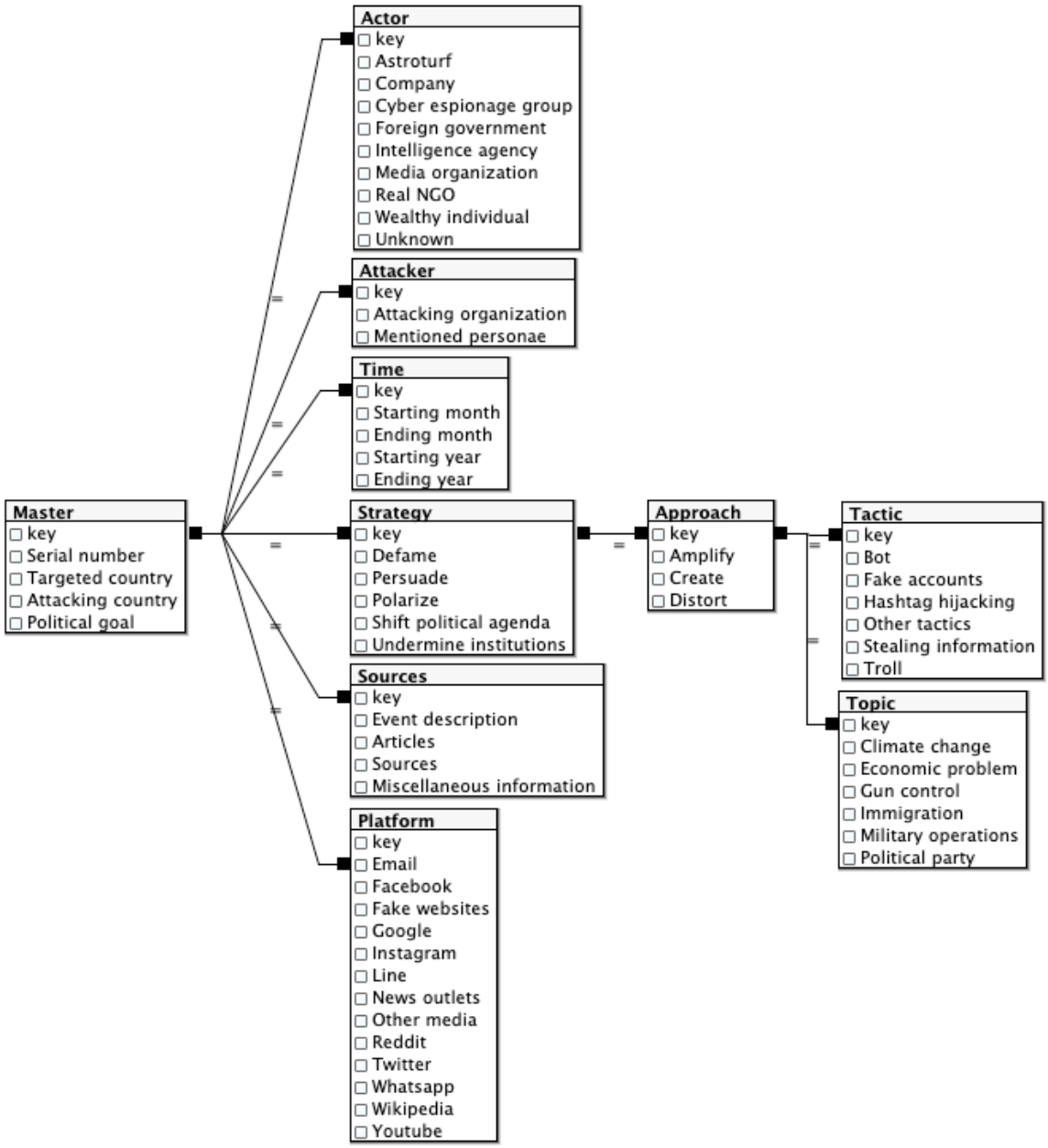
†Princeton University, School of Public and International Affairs, Princeton, NJ 08544. Email: jns@princeton.edu.

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

A Codebook

This section provides a detail description of the variables in our IE database. We build the codebook using a combination of tables in a relational database. The first draft of the codebook aimed at emulating the whiteboard of an influence operation. We complement the codebook with feedback from scholars and research in the industry of analysing misinformation operations, as well as, studying the most famous cases in Russia (Mueller, 2019) and China (Nimmo, Francois, Eib, Ronzaud, Ferreira, et al., 2020). Figure A-1 presents the relational structure of the tables in our database:

Figure A-1: Relational structure of the IE database



Each IE is identified as an *attacker-target-political goal* triple. This design allows us to draw inferences about changes over time in tactics and about the allocation of effort by attacking organizations, which have to make tradeoffs between time spent on different political goals. The following is an overview of the tables in the IE database:

- **Political goal:** This table contains a broad description of the objective of the effort. While we did not choose a fixed set of potential values, we did look for homogeneity across countries so that we could compare the IEs around the world. Polarizing domestic politics, for example, has been a political goal of attacks against Australia, Canada, Germany, Latvia, South Africa, and the US. After initial case coders select a political goal, subsequent reviewers classify the case into one of six broad categories:

  (i) Discredit: the IE aims mainly to defame a politician, political party, government, dissidents, political protesters, etc.

  (ii) Hinder: the campaign aims to distort the relationship between a state and the international community.

  (iii) Polarize: the operation amplifies content on both sides of one or more political issues.

  (iv) Spread: the IE propagates misinformation in order to sow fear and discord.

  (v) Support: the campaign aims to promote politicians, policies, or movements.

  (vi) Influence: the IE aims to shift political discussion in a specific direction.

We record a series of 0/1 variables for whether particular types of organizations, strategies, approaches, tactics and platforms.

- **Actor:** In this table we record a series of 0/1 variables for whether particular types of organizations were engaged in the effort. We define seven actors: "astroturf" (e.g. fake grass-roots organizations created as part of the influence effort), company, cyber espionage group, government, intelligence or military agency, media organization, real NGO and wealthy individual. We mark unknown as an actor when there is not enough information to discover at least one of the operators in the campaign.

  We identify these categories based on the US Department of Justice investigation about the emblematic case of the Russian Internet Research Agency (IRA) aimed at meddling the US elections from mid-2014 through at least 2018 (Mueller, 2019), detail reports of influence operations (Nimmo, Francois, Eib, Ronzaud, Ferreira, et al., 2020; Nimmo, Francois, Eib, & Ronzaud, 2020b), and feedback from scholars and researchers working on identifying misinformation campaigns.

  We do not distinguish between principals, those who order the attacks, and agents, those who execute them, because it is rarely possible to disentangle lines of authority with the available information. One campaign could also contain more than one actor.

- **Time:** We track the first and last time an influence campaign operation was seen based on the different sources. Some cases are ongoing and we code them with the current year (i.e., 2022). Although we also code the starting month and ending month, this level of precision on time is difficult to extract for some IE cases.

  We record a series of 0/1 variables for whether particular types of organizations, strategy, approach, tactic and platforms in the following tables:

- **Attacker:** We identify organizations by name and record key people and organizations mentioned as being part of the effort. We linked the name of the attacker to the actors. For example, in the Russian campaign targeting the US elections, we code IRA (Company) and Cyber espionage group (Fancy Bear or APT28) in the table of "Attacker".

- **Strategy:** Strategy is the broad method taken to advance the political goal. We identify four strategies: (1) defamation for operations aiming to discredit a politician, political party, journalist, etc.; (2) persuasion for operations trying to build support in favor of a political figure, country, set of policies, etc.; (3) polarization for efforts which push on opposite sides of an issue or both support and discredit the same political figure at the same time; (4) agenda shifting for efforts to change the set of issues that are on the political agenda; and (5) undermining political institutions for operation that seek to discredit political organizations such as public agencies, courts, or political parties.

- **Approach**: Approach codes the measurable things done to advance the strategy. These include amplifying existing content, creating new content, and producing distorted information about verifiable facts.

- **Tactic**: Tactics are concrete actions that people or organizations can take as part of an IE. These include using bots, fake accounts, hashtag hijacking, stealing information, and trolling.

- **Platform:** Platform records the social media involved in each IE (e.g. Facebook, Twitter, etc.). We make no judgment about the extent to which different platforms are used.

- **Topic**: Topic records the issues discussed in each attack. As with political goals it is an open-ended field in which we sought to use the same terminology for broadly-similar topics. Topic and Strategy are at the same level in the relational database.

- **Source**: Provides URLs for the main articles, news, reports, working papers, and journal articles relevant to that case. Only cases with at least three sources are included in the final database.

Table A-1 provides a detailed description of each variable with specific examples.

Table A-1: Codebook

Variable	Definition	Example
	Master	
Serial number	Four-digit code showing the order in which we found the observations.	0001 is the first identified effort against a country. The serial number starts again from 0001 for a new targeted country.
Targeted country	Country being attacked (use the International Standards Organization (ISO) 3-digit alphabetic codes). Select MUL (multiple targeted countries) when the political goal targets more than one country. Select UNK when the targeted country is unknown.	(i) Russia operated an influence effort during the U.S. elections in 2016 and France's elections in 2017 (i.e. RUS). (ii) Select MUL for cases Facebook removed pages aiming to amplify content from the Kremlin's media agency targeting 13 countries in Central Asia (i.e. MUL).
Attacking country	Country planned and/or ordered the attack. Select MUL when there is evidence of a coordinated attack (e.g. using the same firm) with the same political goal from two or more countries. Select unknown attacker (UNK) in cases which match the procedures of prior IEs and line up with foreign policy goals of their proponents.	(i) Russia hired people in Macedonia to produce fake news targeting the U.S. The attack is coded as RUS (for Russia), not MKD (for Macedonia). (ii) An Egyptian digital marketing company called New Waves as well as a United Arab Emirates company called Newave were paid to spread organic-looking pro-military messages on social platforms (i.e. MUL). (iii) While there is no direct evidence that the Venezuelan bots worked on behalf of a particular government or entity, the approach here is consistent with state-sponsored activities and consistent with Russian foreign policy goals. We therefore include the case as a state-sponsored IE, but code the attacker as 'unknown'.
Political Goal	Open-text field describing the broad political objective of the effort. This is the primary thing the attacker wants to accomplish as best can be inferred from the preponderance of the reporting on that effort. Include citations for each article or source of information.	(i) Supporting a specific individual or party in an election in a foreign country. Changing U.S. policy in Syria/Ukraine/Balkans/etc. (ii) Undermine trust in the political system. (iii) With Brexit, the political objective was to get the UK to vote to leave the EU. (iv) With many 2016 election efforts in the U.S., the goal was to get President Trump elected or to foster support for Roy Moore's re-election campaign in the Sep. '17 special election in Alabama.

	Time	
Starting month	The earliest month where the attack started (code using numbers e.g. write 1 for January).	The earliest attack was in January.
Ending month	The latest month where the attack was made (code using numbers e.g. write 3 for March).	The latest attack seen was in March.
Starting year	The earliest year where the influence effort was made.	Document methods employed by Internet Research Agency (IRA) to influence the political agenda of the U.S. from June 19, 2015 to December 31, 2017 (i.e. 2015).
Ending year	The latest year where the influence effort was made.	Document methods employed by IRA to influence the political agenda of the U.S. from June 19, 2015 to December 31, 2017 (i.e. 2017).
	Actor	
Astroturf	Equal to 1 when a false organization or social movement is being created as part of the attack.	Philando Castile was shot by a police officer. In response, the Black Lives Matter movement organized a protest in front of the governor's mansion in Minnesota, according to Mica Grimm, an activist in this group. At the same time, a mysterious group used the death of Castile to create a movement called 'Don't Shoot' and organized protests outside the police department where the officer who shot Castile works. When people from CNN and Black Lives Matter tried to look for the origin of Don't Shoot, they found that it was a fake website run from Russia.
Company	Equal to 1 when a person working for a company orders or directs part or all of an operation to influence political decisions in a foreign country or when a company directly carries out an IE. The company must appear affiliated with state actors and carry out operations consistent with an attacking country's political goals.	The IRA is a company working for the Russian state. Yevgeny Prigozhin is a Russian businessman with ties to Russian president Vladimir Putin. Prigozhin controls "a network of companies" including three accused of interference in the 2016 United States elections.

Cyber espionage group	Equal to 1 when an attack is conducted by a group that engages in a range of cyber activities.	According to Microsoft, APT28, a group included in the Fireye list and publicly linked to a Russian intelligence agency, creates websites to steal information from conservative groups which criticized U.S. President Donald Trump.
Media organization	Equal to 1 when one of the actors in the effort is an established media organization, with an installed capacity in terms of employment and buildings. It is not a news web page working for a short period of time or closed after the influence effort concludes.	(i) RT (formerly Russia Today) is a Russian International television network funded by the Russian government. RT is directed at audiences outside of Russia, with content produced in languages including English. (ii) Macedonian media attorney Trajche Arsov created the media organization called usapoliticstoday.com to spread fake news about the elections in the U.S.
Intelligence or Military agency	Equal to 1 when attack conducted by an intelligence or military agency of a country or a directly controlled subsidiary	(i) Bots from the Internet Research Agency "troll army" amplified the hashtag #Brexit over two months to encourage voting in favor of Brexit. Press reports suggest this activity was directed by the Main Intelligence Directorate of the General Staff GRU.
Government	Equal to 1 when politicians order the influence effort or when they are part of the strategy. Coded 1 for DIE if there is reliable evidence that government agencies were involved.	The Grand Jury for the District of Columbia said the Russian Federation operated a military intelligence agency called the Main Intelligence Directorate of the General Staff. This is evidence that a foreign government was the actor of this influence effort.
Real NGO	Equal to 1 when the attack is executed by an activist group that is neither government nor a for-profit corporation.	This category includes Wikileaks, Openleaks, AJTransparency, Globalleaks.com, Balkanleaks.eu, etc. Maria Katasonova launched what she referred to as a Twitter "flash mob" under the hashtag #dislikeMacron. She is a Russian nationalist who works for a high-ranking politician and is part of a Russian patriotic artists' collective, heading up the "Women for Marine" movement.

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

Strategy		
Defame	Equal to 1 when there is a direct attack against a person, intended to discredit him or her.	Trolls from the Internet Research Agency (IRA) create fictitious social-media personas to spread falsehoods and promote messages against Hillary Clinton.
Persuade	Equal to 1 when there is an influence effort in which the goal appears to be to directly shift political views about an issue or actor in an identifiable direction (the goal is to shift the median voter in one direction).	Trolls create blogs and fake news to incentive people to vote in favor of Donald Trump. These trolls do not push the Hillary Clinton campaign at the same time.
Polarize	Equal to 1 when an attack aims to create polarization on issues. This is persuasion on both sides of an issue to move individuals to the extremes. This affects the variance of the decision because it looks for pushing one political goal in two opposite directions.	Nearly 600 Russia-linked accounts tweeted about the US Affordable Care Act (ObamaCare). The majority of the nearly 10,000 tweets on the Affordable Care Act seemed intended to pit one side against the other, not to advance a particular policy with respect to the ACA.
Shift political agenda	Equal to 1 when the effort aims to change the agenda (putting something new on the political agenda).	As an exporter of energy, Russia desires to eliminate or mitigate the American energy threat, . In the case of building the Dakota Access Pipeline, for example, Russia run IE to stop this project saying that Native Americans would be in danger because the Pipeline would cross their territory.
Undermine institutions	Equal to 1 when the objective is to reduce the credibility/reputation of one or more institutions in the target country.	This category includes Armed Forces (including the FBI), the national congress (but individual parties are not institutions), and system justice (including courts). Russian media outlets, for example, circulated a false story about a state prosecutor in Berlin failing to prosecute an alleged rape by immigrants.

	Approach	
Amplify	Equal to 1 when the individual (Trolls or Bots) work to promote specific content, whether real or fake.	A suspected network of 13,000 Twitter Bots retweeted and shared media in favor of Brexit before the referendum.
Create	Equal to 1 when the effort is to create an entirely new narrative around a set of events. May or may not include creating false information.	Aleksei, a troll from St. Petersburg, said the first task assigned to all new employees was to create three identities on Live Journal, a popular blogging platform.
Distort	Equal to 1 when a person or a group creates false information about objectively verifiable facts. This includes promoting conspiracy theories.	A well-known Russian twitter account said "Muslim woman pays no mind to the terror attack, casually walks by a dying man while checking phone." This message was amplified by a Russian network on social media, though the woman targeted in the attack denied the claim.
	Tactic	
Bot	Equal to 1 when an automated account is used, e.g. to retweet or share misinformation or fake news on a preset schedule or in response to identifying specific signals.	Bot-like accounts are those with number and ratio of tweet to retweets much higher than the average accounts. An account tweeted 3,176 times, at an average rate of 453 a day. Of those tweets, 3,122 were retweets, a rate of 98%.
Fake accounts	Equal to 1 when the effort employs fake accounts of fictitious personas.	@SouthLoneStar was a fake account used for amplifying racist messages in the Brexit election. FB reported they took down more than 1B fake accounts in 2018.
Hashtag hijacking	Equal to 1 when attackers use hashtags to amplify their propaganda.	Russian twitter accounts amplified the #NotInMyNameTheresaMay, after Rachael Swindom, a prominent Labor party campaigner, tweeted out a poll asking if Twitter users support Theresa May's plans to "bomb Syria".

Other tactics	Equal to 1 when tactics are neither using trolls, bots, micro-profiling, Hashtag hijacking, stealing information, nor fake accounts.	Russia uses TV programming to encourage people in Crimea to vote in favor of becoming part of Russia.
Stealing information	Equal to 1 when a person tries to steal information from emails, personal websites or group pages.	Phishing emails sought to access conversations between Hillary Clinton and her team during the 2016 U.S. elections.
Troll	Equal to 1 when a person (or people) create a large volume of content for executing influence operations. Can be independent or contractor. The distinguishing characteristic is the volume of content and focus of the content and the fact that it is produced and disseminated manually.	Lyudmila Savchuk spent most of her time at the troll farm writing as an imaginary Russian woman on the LiveJournal blogging platform, widely used across Russia.
	Platform	
Email	Equal to 1 when the attack involves emails with misinformation or emails attempting to steal information.	Phishing emails to access to conversations between Hillary Clinton and her team in the elections.
Facebook	Equal to 1 when an attack involves Facebook.	Facebook identified the Internet Research Agency as a prime source of provocative posts on divisive content during the 2016 presidential election.
Google	Equal to 1 when an attack involves Google platforms.	Google identified the Internet Research Agency as a prime source of provocative posts on divisive American issues.

Fake websites	Equal to 1 when the attack involves the creation of fake websites to steal information or send a message pretending to be a different persona or institution. This category does not include news pages on social media.	GRU cloned the access web page to the official site of the Democratic Party, and when the participants of this political party entered their personal data, the hackers stole their information.
Line	Equal to 1 when an attack involves activity on Line.	Line was used to falsely claim that the central government of China was planning to impose draconian restrictions on pensioners.
News outlets	Equal to 1 when the attack involves the creation of news websites. This category does not include news pages on social media.	Trolls in Macedonia created news websites against the Hillary Clinton campaign during the U.S election.
Other media	Equal to 1 when an attack involves other media such as TV, newspapers and radio.	News providers in Ukraine that had a Russian shareholder or partner tended to be more restrained in their criticism of Russia than comparable news providers without such support from Moscow.
Reddit	Equal to 1 when the attack involves Reddit.	Reddit accounts were involved in spreading messages against Hillary Clinton and in favor of Donald Trump during the 2016 elections.
Twitter	Equal to 1 when the attack involves Twitter.	Twitter released data from more than 10 million tweets that had been circulated by propaganda farms and their associated puppet accounts.
WhatsApp	Equal to 1 when the attack involves WhatsApp.	Using WhatsApp, Russia spread rumors saying that Hillary Clinton was in favor of White Americans.
Wikipedia	Equal to 1 when an attack involves manipulating results on Wikipedia.	Russian Trolls created Wikipedia web pages about conservative critics of Trump, such as Marco Rubio, saying that they were fake conservatives.
YouTube	Equal to 1 when an attack involves YouTube.	Iranian Trolls created YouTube propaganda against Donald Trump, saying that Trump wastes the public resources of the United States.

	Topic (selected list)	
Economic issues	Equal to 1 when an attack exploits an economic issue.	Russian trolls used the Keystone XL pipeline in Canada to generate division in the country.
Gun control	Equal to 1 when an attack exploits debates over gun control.	Russian media organization created posts claiming that Sweden sells weapons to the Islamic state.
Immigration	Equal to 1 when an attack exploits propaganda against immigration.	In the Brexit Referendum, trolls posted several tweets claiming that people would migrate to England if the UK did not leave the Europe Union.
Military operations	Equal to 1 when an attack exploits military operations.	Russian trolls used the NATO's military exercises in Estonia to claim that the country was preparing an attack against Russia.
Political party	Equal to 1 when an attack exploits politicians and political parties.	Russian trolls attacked Hillary Clinton while simultaneously supporting Donald Trump.
	Source	
Event description	Succinct 1-3 sentence description about the objective, political goal, and topic of the attack.	People in the troll factory created fake social media accounts and wrote blog posts meant to sow divisions in the U.S. and turn Russians against Americans.
Miscellaneous information	Relevant information about classification of any variables.	Melvin Redick is one of the accounts Russia used to spread the emails stolen from Hillary Clinton campaign.
Source	Provide link to where news and media sources related to the influence effort can be found. Include at least three sources per influence effort	`https://www.justice.gov/file/1080281/download`
Articles	Provide full citation to articles related to the influence effort. Each effort will have multiple associated articles.	Boatwright, B. C., Linvill, D. L., & Warren, P. L. Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building. `http://pwarren.people.clemson.edu/Linvill_Warren_TrollFactory.pdf`

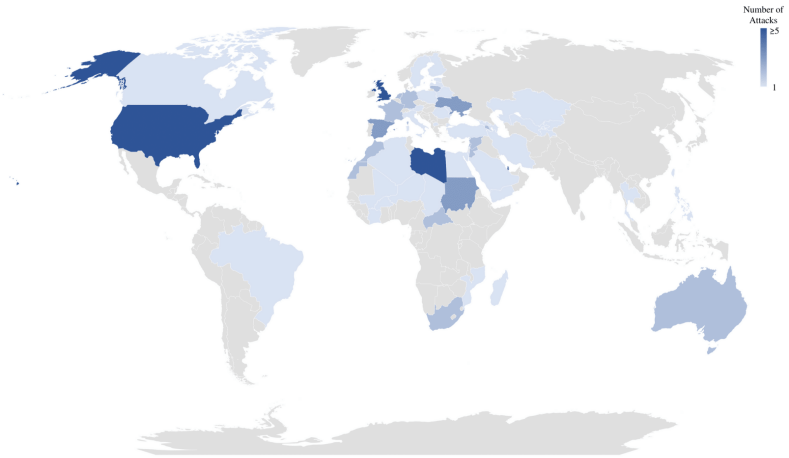
Notes: For each attack we code both the principal ordering the attack and the agent(s) responsible for carrying it out in the table Actor. In the future we may seek to make a distinction between principles and agents.

B Analysis of the IE dataset

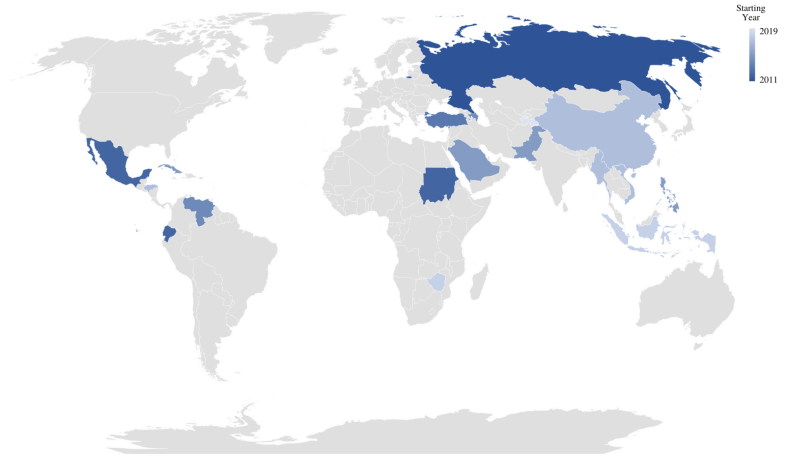
This section describes the principal trends in our IE database. Figure A-2 provides maps showing the distribution of countries targeted by FIEs and DIEs.

Figure A-2: Distribution of influence efforts

Panel A: Countries targeted by foreign influence efforts



Panel B: Domestic influence efforts by year of origin



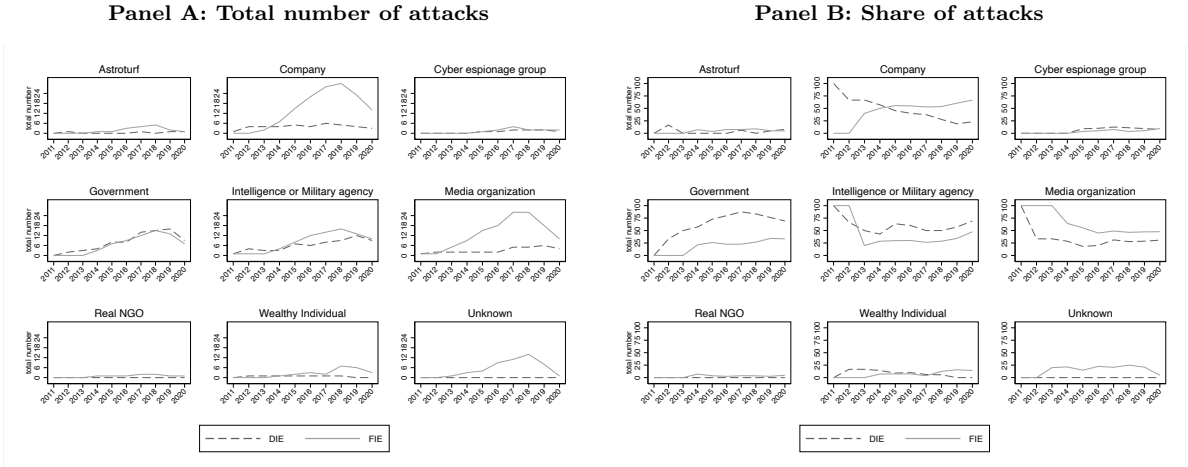
Panel A: This map includes all countries which have been targeted by FIEs, colored according to the number of attacks.For cases attacking multiple countries simultaneously, we have included all known targets. Countries falling into the ≥ 5 category are the United States (21 FIEs), the United Kingdom (7 FIEs),and Libya (6 FIEs). *Panel B*: Countries in this map are colored according to the earliest known year in which domestic influence efforts (DIEs) were active. For countries with multiple DIEs, coloring reflects the start year of the earliest DIE.

B.1 Actors

Panel A in figure A-3 below presents the number of attacks involving each type of actor from 2011 through 2020, divided into FIEs and DIEs. Whereas the number of FIEs involving unknown actors increased to a peak of about 14 cases in 2018, no DIEs have included unknown actors. This may reflect FIE actors' increasing proficiency in masking their responsibility. As shown in Panel B, the relative share of FIEs involving each attacker remained fairly stable after 2015, though 2019 saw a mild uptick in the involvement of companies and governments. Conversely, the share of DIEs involving companies has declined significantly, while the share of DIEs involving government actors increased to approximately 82% by 2017.

A number of IEs in the database involve an unknown attacking country, including an effort supporting Catalonia's independence movement in 2017 (Lesaca, 2017). These operations are included only when the evidence is consistent with and strongly suggestive of state-sponsored activities. An effort from an unknown attacker to polarize German politics was excluded because evidence pointed to the involvement of right-wing political groups in the United States, but not a state actor (Hjelmgaard, 2017).

Figure A-3: Actors



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

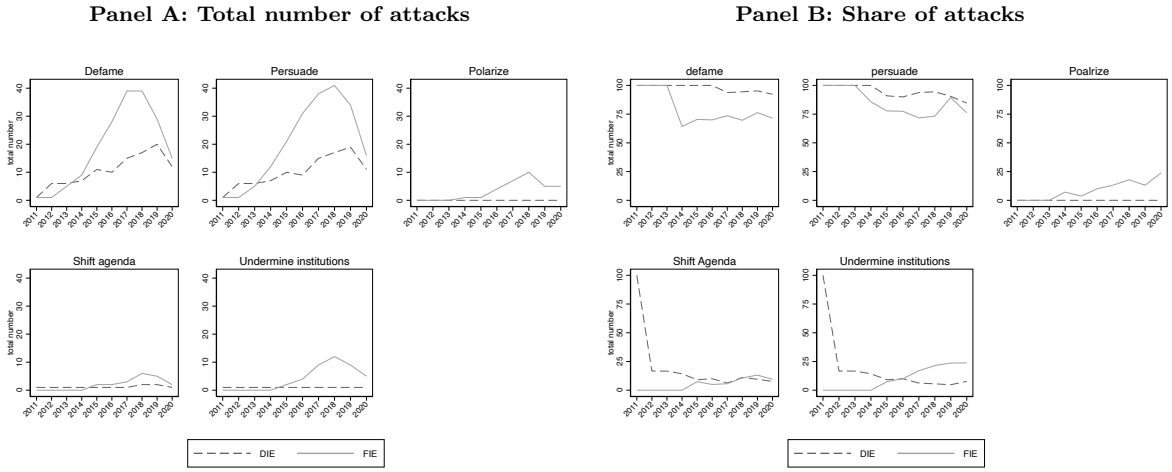
B.2 Strategies and tactics

IEs have employed a wide range of strategies and we do not see clear trends over time. Below, figure A-4, panel A presents the total number of attacks employing each strategy during the study period. Defame and persuade were used in a majority of IEs throughout the period. Although the number of cases involving polarization is modest – only 10 cases by 2020 – they were an increasing share of active efforts until 2018, as Panel B shows. Efforts to shift the political agenda and undermine institutions have been rare across all IEs.

The most commonly-used strategy is persuasion, which we define as trying to move the

average citizen to one side of an issue, used in 78% of FIEs and 93% of DIEs. Defamation, defined as attempts to harm the reputation of people, is used in 72% of FIEs and 95% of DIEs. Furthermore, only 13% of FIEs use polarization – defined as trying to move opinion to the extremes on one or more issues – and no DIEs use this strategy (see figure A-4, panel B below). These findings contradict the idea that IEs most often work to polarize public opinion (see e.g., (L. G. Stewart et al., 2018)).

Figure A-4: Strategy

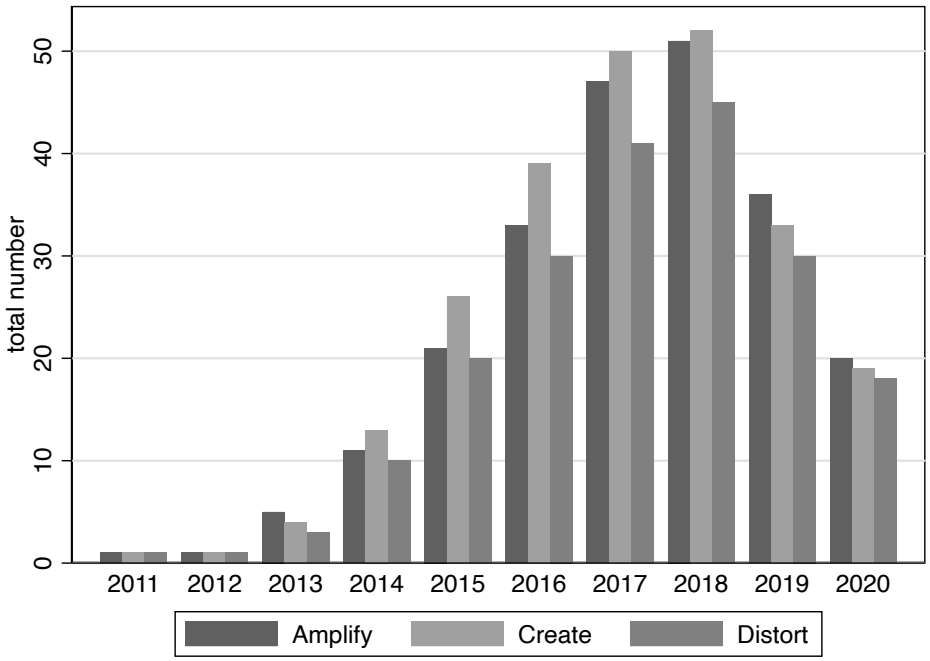


Panel A shows the total number of influence efforts (IEs) divided into foreign influence efforts (FIEs) per strategy and domestic influence efforts (DIEs) per strategy. Panel B presents the share of total efforts made by a particular strategy per year. For example, the total number of FIEs using a polarization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

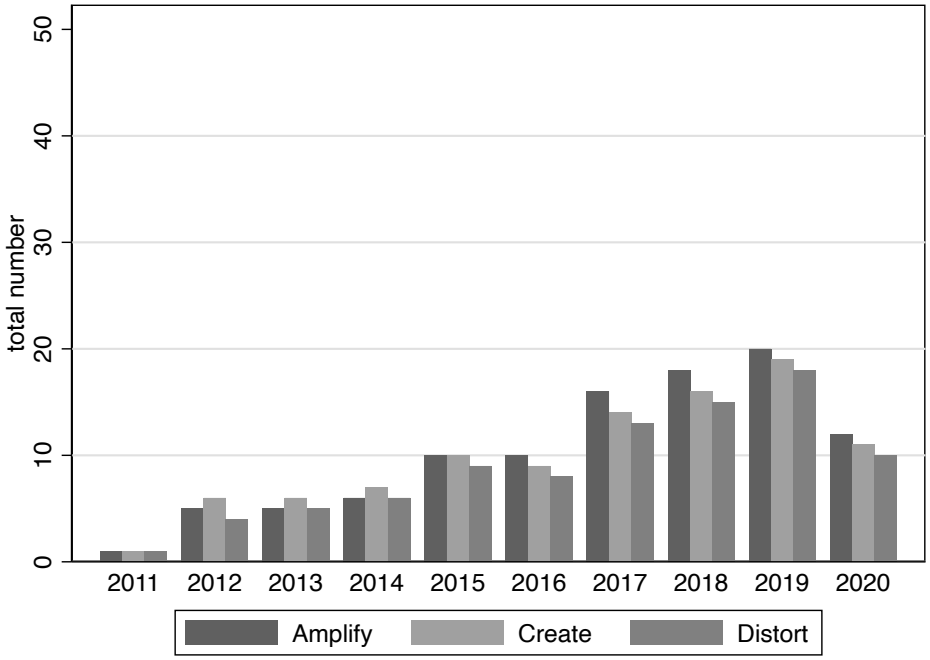
There is much less heterogeneity in which approaches have been used over time. About 63% of FIEs include all three approaches — amplify, create, and distort content — in the same operation, as do 73% of DIEs. 92% each of the FIEs use creation of original content, 92% FIEs and 88% DIEs amplification of pre-existing content, 81% of FIEs and 77% of DIEs distortion of objectively verifiable facts (see figure A-5 below, with panel A showing FIEs and panel B showing DIEs).

Figure A-5: Approach

Panel A: Foreign influence efforts



Panel B: Domestic influence efforts

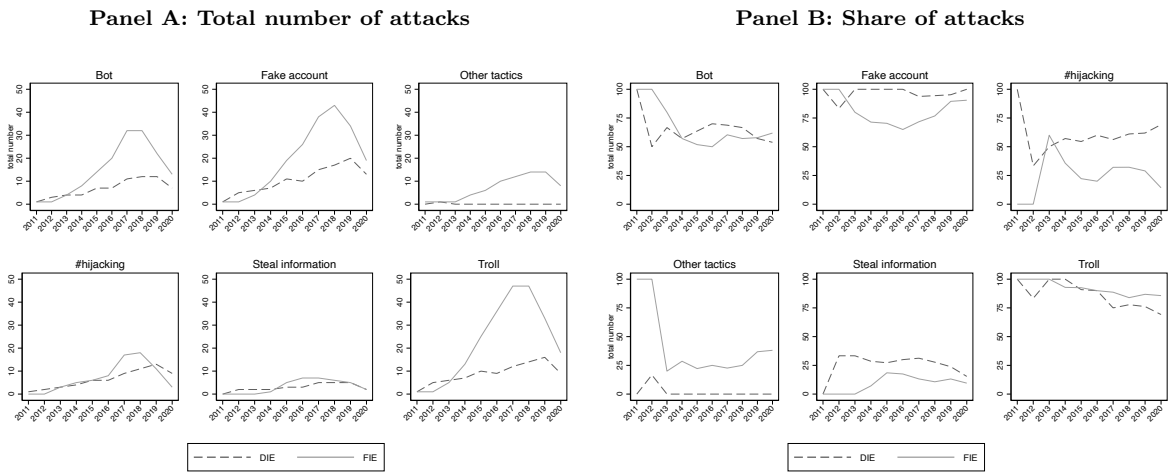


Panel A (B) shows the total number of foreign (domestic) influence efforts (FIEs) (DIEs) per approach and year. Number of FIE is 78 and DIE is 25, for a total number of 999 IEs

When it comes to tactics, there is a great deal of variance, but few distinct trends over time. Fully 85% FIEs and 77% DIEs use trolls (see figure A-6, panel A below). About half of the FIEs and DIEs use bots. The share of IEs doing so has been fairly stable

since 2014, as we see in figure A-6, panel B. 73% FIEs use fake accounts and 92% DIEs, a number which has remained stable since 2014.

Figure A-6: Tactic



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

B.3 Platforms

Twitter, Facebook, and news outlets are the most common platforms used in FIEs, as figure A-7 shows below. In DIEs, the most common platforms are Facebook, Twitter, and Instagram. Twitter is used in 87% of FIEs and 77% of DIEs, while Facebook is used in 77% of FIEs and 92% of DIEs.

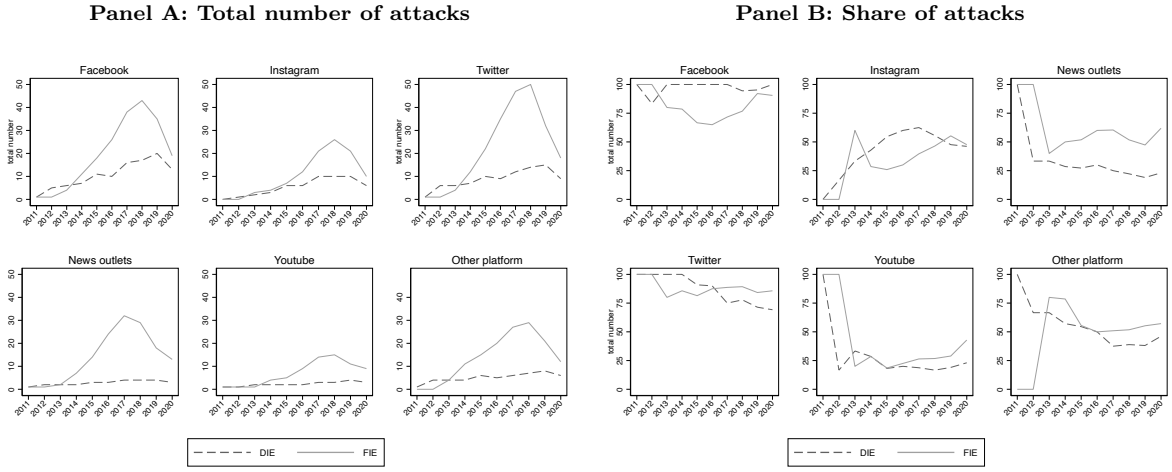
This pattern likely reflects Facebook and Twitter's market shares as well as the fact that both platforms offer free access and have historically had low capacity to screen content, though that is changing. All three of these characteristics make them good platforms for sending propaganda masked as indigenous political activism.

However, the pattern may also be an artifact of these platforms' transparency. Both Twitter and Facebook have released a great deal of data about nation-state operations on their platforms. During the 2018 US midterm election, for example, Facebook employed a large team to analyze different types of media information, identify what they termed "coordinated inauthentic activity" (mostly from Russia), and reduce viewership of that content in the run up to the election (Kist, 2018). Data releases from Facebook and Twitter make it easier to report on how IEs have used the social media platforms, which in turn leads them to be highly represented in our data.

As figure A-7, Panel B shows below, Instagram has been used in an increasing share of all IEs since 2014, and YouTube has been used in an increasing share of FIEs. Despite these apparent trends, it is important to note that the use of platforms in furtherance of IEs is distinct from an assessment of interaction of IE content on those platforms. Assessing the latter requires approaches akin to those deployed in (Allcott et al., 2019) who find that interaction with false content increased on both Facebook and Twitter between 2015 and

2016. Interactions with false content continued to increase on Twitter in the following two years but fell on Facebook.

Figure A-7: Platform



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

B.4 Combinations across strategies, tactics and platforms

The following analysis considers the combination of strategies, tactics, and platforms within individual IEs. For instance, table A-2 below shows the percentage of cases that combine two strategies. Defame and persuade (74% of FIEs and 92% of DIEs) is the most commonly-used combination, followed by undermine institutions and shift the political agenda (38% of FIEs and 50% of DIEs).

Table A-2: Strategy combination

Panel A: Foreign influence efforts

	Defame	Persuade	Polarize	Shift agenda	Undermine
Defame	100				
Persuade	74	100			
Polarize	9	3	100		
Shift agenda	11	12	10	100	
Undermine	23	21	30	38	100

Panel B: Domestic influence efforts

	Defame	Persuade	Polarize	Shift agenda	Undermine
Defame	100				
Persuade	92	100			
Polarize	0	0	.		
Shift agenda	8	9	.	100	
Undermine	4	4	.	50	100

Notes: Given the total number of foreign or domestic influence efforts (FIEs or DIEs), panel A and panel B, respectively, using the strategy listed in the column, the table shows the percentage of cases also using the strategy listed in the row. For example, out of 9 FIEs that include polarization, 3 also include efforts to undermine institutions (33%). Numbers are the percentage rounded to the closest integer. The number of FIEs is 78 and DIEs is 25, for a total of 103 influence efforts (IEs).

Analogously, table A-3 presents that trolling is usually used in conjunction with bots, fake accounts, and hashtag hijacking. Finally, table A-4 demonstrates that Twitter, Facebook, Instagram, and e-mail are used together most of the time.

Table A-3: Tactic combination

Panel A: Foreign influence efforts

	Bots	Fake account	#Hijacking	Other tactics	Steal info.	Trolls
Bots	100					
Fake account	80	100				
#Hijacking	41	28	100			
Other tactics	22	26	10	100		
Steal info.	12	14	14	15	100	
Trolls	85	86	86	70	90	100

Panel B: Domestic influence efforts

Bots	100					
Fake account	100	100				
#Hijacking	71	57	100			
Other tactics	0	0	0	100		
Steal info.	29	17	23	100	100	
Trolls	86	78	85	0	67	100

Notes: Given the total number of foreign or domestic influence efforts (FIEs or DIEs), panel A and panel B, respectively, using the tactic listed in the column, the table shows the percentage of cases also using the tactic listed in the row. For example, out of 22 FIEs that include hashtag hijacking, 19 also include trolling (86%). Numbers are the percentage rounded to the closest integer. The number of FIEs is 78 and DIEs is 25, for a total of 103 influence efforts (IEs).

As for the coordination use of platforms, table A-4 below demonstrates that Twitter, Facebook, Instagram, and e-mail are used together most of the time.

Table A-4: Platform combination

	e-mail	Facebook	Fake websites	Google	Instagram	Line	News outlets	Other media	Reddit	Twitter	Whatsapp	Wikipedia	Youtube
e-mail	100												
Facebook	83	100											
Fake websites	50	13	100										
Google	17	13	23	100									
Instagram	0	46	31	45	100								
Line	0	1	0	0	0	100							
News outlets	33	42	46	73	42	100	100						
Other media	0	18	8	9	18	100	26	100					
Reddit	0	6	0	27	5	0	9	5	100				
Twitter	100	84	100	91	82	100	87	84	100	100			
Whatsapp	0	13	15	0	8	0	9	5	0	11	100		
Wikipedia	0	0	0	0	0	0	2	0	17	1	0	100	
Youtube	0	27	15	55	28	100	30	37	67	28	36	0	100

Given the total number of influence efforts (IEs) using the platform listed in the column, the table shows the percentage of cases also using the platform listed in the row. For example, out of 7 IEs that include the use of Reddit, 5 also include the use of YouTube (71%). The table combines foreign influence efforts (FIEs) and domestic influence efforts (DIEs), and numbers are the percentage rounded to the closest integer. The number of FIEs is 78 and DIEs is 25, for a total of 103 influence efforts (IEs).

B.5 Changes in 2020

Over the course of 2019-20, we observed a number of notable new trends in both the tactics and objectives employed by IEs. First, in 2019 IEs originating in Russia, the Middle East, and elsewhere frequently involved the use of commercial bot networks and marketing firms. This obscured the involvement of state actors and, in some cases, made it impossible to attribute campaigns to particular countries. Second, we observed several new cases where states targeted multiple countries with common content. Third, a series of seemingly related efforts originated in Russia which interfered in the elections and domestic politics of African countries where Russian firms have significant mining interests.

Before 2019, only 2 out of 54 FIEs involved multiple targeted countries. In 2019, however, 9 out of 23 newly identified FIEs sought to simultaneously influence several countries. A number of these cases involved common content with country-specific distribution networks pushing the same policy agenda across targets. For example, a broad campaign associated with government actors and marketing firms in Saudi Arabia amplified pro-Saudi narratives in countries including Qatar, Saudi Arabia, and UAE (Gleicher, 2019d). In 2020, Russia and China continued to execute FIEs in pursuit of long-term political goals, such as disrupting US elections in the case of Russia (Nimmo, Francois, Eib, & Ronzaud, 2020a) or undermining the Taiwanese government in the case of China (Monaco et al., 2020). Strategies and aims remained largely similar from 2019 to 2020. The exception in 2020 was France's effort to influence politics in Africa (Gleicher & Agranovich, 2020). This was the first known FIE perpetrated by a democratic state since 2011.

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

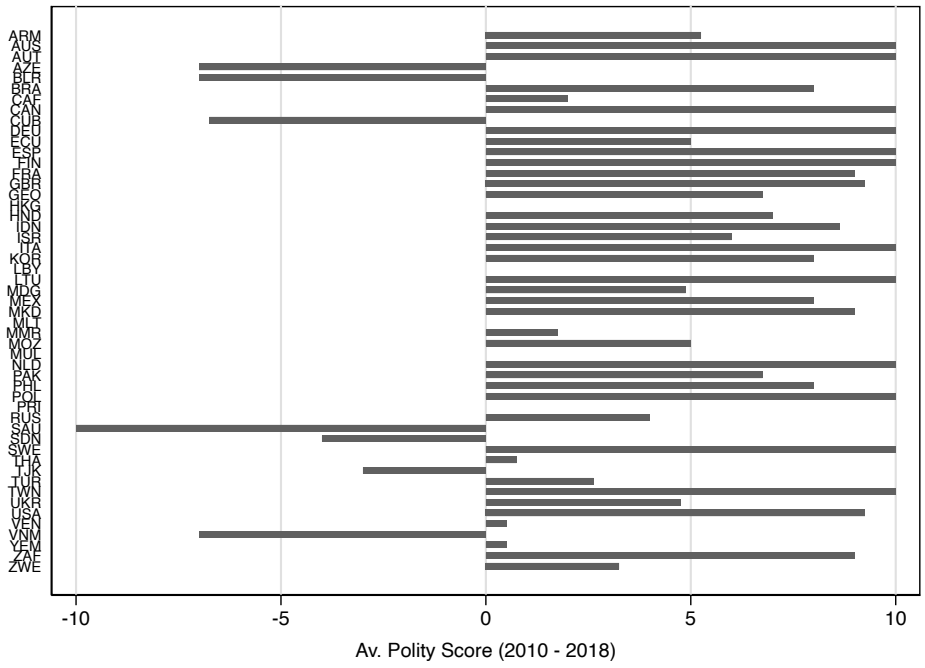
Twenty four different countries engaged in 25 total DIEs, including 11 democratic and 13 authoritarian regimes. Sustained domestic interference can inhibit the use of social media for personal expression or political discourse (Morales, 2020), and has been employed to influence elections in both democratic and authoritarian states. More than half of observed DIEs began in 2017 or later. Our research therefore suggests states are increasingly using social media manipulation to shape domestic politics.

B.6 Autocracies and influence efforts

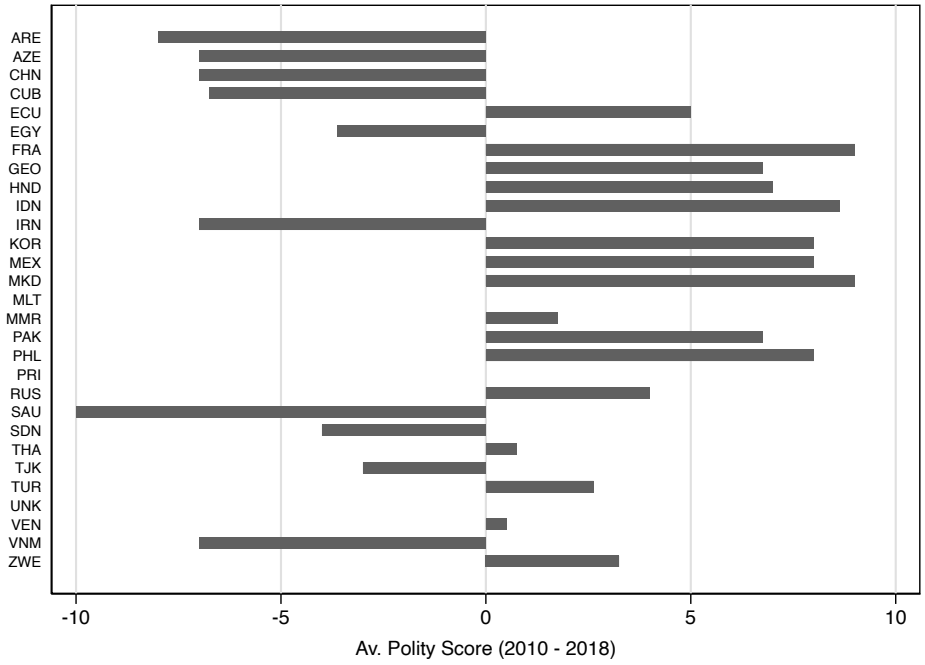
Of the 51 countries targeted by influence campaigns, including FIEs and DIEs, 12% are autocracies, 31% are anocracies, and the rest are classified as democracies. As for the countries operating IEs, 17 out of 29 are autocracies or anocracies (see panel A and B in figure A-8). Furthermore, around half of the countries operating IEs had a below average GDP per capita between 2010 and 2019. This contradicts the hypothesis that only wealthy economies engage in influence operations (see figure A-9).

Figure A-8: Polity score and influence efforts

Panel A: Targeted country

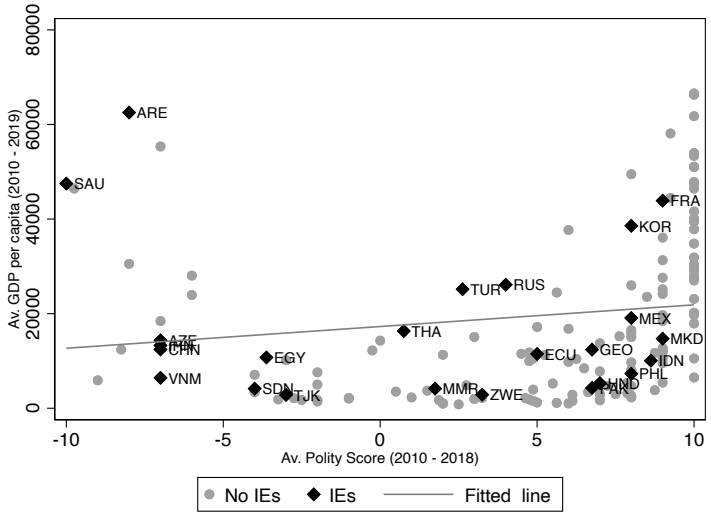


Panel B: Attacking country



Notes: Revised Combined Polity Score (polity2) ranges from -10 to +10, with -10 to -6 corresponding to autocracies, -5 to 5 corresponding to anocracies, and 6 to 10 to democracies (Marshall et al., 2019). 48 countries are targeted by IEs.

Figure A-9: Attacking countries



Notes: Revised Combined Polity Score (polity2) ranges from -10 to +10, with -10 to -6 corresponding to autocracies, -5 to 5 corresponding to anocracies, and 6 to 10 to democracies (Marshall et al., 2019). 48 countries are targeted by IEs. The figure excludes three outliers with Av. GDP over 8,0000: Qatar with Polity Score equal to -10, Singapore with -2, and Luxembourg with 10.

Indeed, table A-5 presents below the correlation between running an IE and being an autocracy, controlling for population, real GDP per capita, and trade as a percentage of GDP. The models include fixed effects for region and income. Autocratic countries are 10 percentage points (pp) more likely to operate FIEs and no more likely to operate DIEs.

Table A-5: What explains to run an IE

Dep. var: Running a (2010 - 2020)	IE	FIE	DIE
	(1)	(2)	(3)
Autocracy (2010 to 2018)	0.11	0.10**	0.06
	(0.08)	(0.05)	(0.08)
Log. Av. Population (2000 to 2009)	0.08***	0.04***	0.06***
	(0.02)	(0.02)	(0.02)
Log. Av. Real GDP per-capita (2000 to 2009)	0.06	0.06	−0.01
	(0.09)	(0.05)	(0.08)
Constant	−1.43	−1.11**	−0.60
	(0.92)	(0.54)	(0.90)
Adj. R-squared	0.13	0.19	0.08
Attacking countries	22	7	18
Observations	154	154	154

Notes. Robust standard errors shown in parentheses. Autocracy is equal to one when Polity Score is smaller than zero. All panels include region fixed effects, income group fixed effects, average percentage of urban population between 2000 to 2009, trade as percentage of GDP between 2000 to 2009. *** is significant at the 1% level, ** is significant at the 5% level, * is significant at the 10% level.

Nevertheless, autocratic countries are 14 pp less likely to be targeted by FIEs (see table A-6). We also find that countries with larger populations are more likely to operate IEs and to become targets of both FIEs and DIEs. Real GDP is slightly correlated with running IEs, but it does not increase the probability of being targeted by IEs.

Table A-6: Being targeted by IEs

Dep. var: Being targeted of a (2010 - 2019)	IE	FIE	DIE
	(1)	(2)	(3)
Autocracy (2010 to 2018)	−0.14	−0.14*	0.04
	(0.09)	(0.07)	(0.08)
Log. Av. Population (2000 to 2009)	0.10***	0.05**	0.07***
	(0.02)	(0.02)	(0.02)
Log. Av. Real GDP per-capita (2000 to 2009)	0.01	0.11	−0.02
	(0.10)	(0.09)	(0.08)
Constant	−1.60	−1.74*	−0.63
	(1.04)	(0.95)	(0.90)
Adj. R-squared	0.17	0.19	0.10
Targeted countries	48	31	19
Observations	154	154	154

Notes. Robust standard errors shown in parentheses. Autocracy is equal to one when Polity Score is smaller than zero. All panels include region fixed effects, income group fixed effects, average percentage of urban population between 2000 to 2009, trade as percentage of GDP between 2000 to 2009. *** is significant at the 1% level, ** is significant at the 5% level, * is significant at the 10% level.

C Annotated List of Influence Efforts

This section summarizes key details of all 103 influence efforts included in the database. The references and details are not exhaustive. For full details please consult data at this link. Each IE has a unique identifier which concatenates the ISO3 code for targeted country, the ISO3 code for the attacking country, and a sequential serial number based on the order in which we found the IE. ARMRUS0001, for example, is the first FIE we identified in which Armenia was targeted by Russian actors. For DIE, the code is simplified since the targeted country is equal to the attacking country. CHN0001, for example, is the case in which the Chinese government sought to discredit prominent dissidents in its territory. In cases where there were multiple targeted countries in one FIE on a particular political issue we created the 3-letter code MUL, which is not assigned to any country in the ISO3 list.

The following annotated lists are organized by this code. Sub-section C.1 (C.2) presents the event description for 78 (25) foreign (domestic) influence efforts.

C.1 Foreign Influence Efforts

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

In 2017, a Russian-led Twitter bot campaign sought to undermine faith in Armenia's parliamentary elections by promoting a narrative of interference by the United States. The 2017 election was the first vote under a new law which marked the transition towards a parliamentary system of rule (Nimmo & Barojan, 2017). Initially, the circulation of a fake letter from the United States Agency for International Development (USAID) by tens of Twitter users posting in Russian was debunked due to several grammatical and spelling errors as well as the association with a Gmail account (Nimmo & Barojan,

2017). The letter supposedly provided instructions on how to meddle in Armenia's election. A corrected fake letter was then shared on pastebin.com on March 29, 2017 and amplified by Twitter bots. An investigation of the Russian bot network showed that all accounts were created around the same time, had very few followers, and tweeted similarly worded messages linked to the USAID letter (Nimmo & Barojan, 2017). The Russian-language profiles frequently made use of the hashtag #armvote17 to promote the narrative (Mackinnon, 2017). Twitter attempted to remove these Russian accounts a day before the election, but inadvertently took down the accounts of several prominent Armenian journalists (Khana, 2017).

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

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

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

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

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

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

The campaign involved a range of actions on social media. Two Facebook sites, for

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

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

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

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

A study of the spread of misinformation in Brazil from August to September 2018 showed an effort on Twitter, Facebook and Whatsapp to influence Brazilian elections (Ruediger, 2018; Benevides, 2018). Analysts identified a group of 232 profiles previously active in other countries which spread messages involving Jair Bolsonaro, Luiz Inácio Lula da Silva and fake news about pedophilia. The group produced 8,185 Twitter posts related to Brazilian politics in Portuguese between August 1 and September 26, 2018 (Ruediger, 2018).

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

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

Occasionally, the Facebook network published pro-opposition content, but the vast majority of material supported Russia's actions in the CAR and tried to distort local political discourse. In addition to social media interference, Wagner Group, a Russian private military contractor, has been active in the CAR since 2017, acting as a security detail for President Touadéra or guarding Russian mining sites (Reynolds, 2019). A Prigozhin-linked mining company also established the radio station Radio Lengo Songo in the CAR (Searcey, 2019), and the account behind one of the inauthentic Facebook pages claimed to be a journalist from this station (Grossman et al., 2019).

This campaign extended into 2020, when Facebook removed competing influence operations from France and Russia, both of which sought to influence domestic politics in the CAR. According to Facebook, "this Russian network was an attempt to rebuild their operations after our October 2019 takedown" (Gleicher & Agranovich, 2020). Russia employed local nationals to manage social media content and produce journalistic articles, and one Facebook page amassed over 50,000 followers (Graphika & Stanford Internet Observatory, 2020). Content primarily sought to promote the re-election bid of President Faustin-Archange Touadéra while attacking French influence in the country, directly commenting and posting on social media assets operated in France.

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

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

DEURUS0001. Targeted country **Germany**. Attacking country **Russia**. Political goal **Support Alternative for Germany (AfD) for the Federal Elections in 2017**:

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

DEURUS0002. Targeted country **Germany**. Attacking country **Russia**. Political goal **Undermine Angela Merkel and her political decisions**:

Russia started targeting German Prime Minister Angela Merkel in 2015 in a manner similar to their later actions against Hillary Clinton in the 2016 US presidential election. According to German officials, the cyber espionage group APT28 tried to steal information from Germany's lower house of parliament, the Bundestag, and Angela Merkel in 2015 (Neuman, 2018). Just days after Merkel set up an Instagram account, thousands of Russian trolls began insulting the people in Merkel's pictures. One of the comments tells Merkel that the Russians "will soon be in Berlin again." A picture of the Chancellor meeting Ukrainian president Petro Poroshenko received several comments comparing the two leaders to Nazis, making personal insults about Merkel's appearance, and using aggressive sexual threats. The only positive comments in Russian were added to an image

of Merkel and Russian President Vladimir Putin (A. Griffin, 2015). The campaign also included the creation of around 2,500 fake news posts, aiming to contradict Merkel's policy toward refugees (Kroet, 2017). These posts were coordinated with content on Russian media outlets that systematically challenged key decisions of Merkel's CDU party, especially by calling into question her controversial decision to allow thousands of refugees to enter Germany in August 2015 (Brattnerg & Maurer, 2018). At least some of the anti-Merkel content on Twitter came from bot accounts and trolls that also backed Donald Trump in the 2016 US election (Snegovaya, 2017).

ESPRUS0001. Targeted country **Spain**. Attacking country **Russia**. Political goal **Support Catalonia's independence in 2017**:

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

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

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

The Venezuelan social media effort sought to undermine confidence in Spanish law enforcement and promote pro-independence narratives, primarily by amplifying articles from state-linked Russian media outlets RT and Sputnik (Lesaca, 2017). This suggests that the campaign originated in Russia and employed a Venezuelan bot network. A small amount of polarizing content content also criticized the movement, highlighting how Catalonia's independence would hurt the Spanish economy. Some content was unrelated to Russian sources, with accounts frequently pushing the hashtag #VenezuelaSalutesCatalonia (Alandete, 2017).

While there is no direct evidence that the Venezuelan bots worked on behalf of a particular government or entity, the approach here is consistent with state-sponsored activities and consistent with Russian foreign policy goals. We therefore include the case as a state-sponsored IE, but code the attacker as 'unknown'.

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

Leading up to Spain's parliamentary elections in April of 2019, researchers identified a network of Twitter bots and inauthentic accounts promoting Islamophobic content and messages in favor of the far-right Vox political party (Peinado, 2019). The accounts had produced 4.4 million pro-Vox tweets since 2018 and Islamophobic tweets dating back to 2017. Though the origins and funding of this network are unclear, the accounts were orig-

inally established to attack the Maduro government in Venezuela but began focusing on Spain following a 2017 terrorist attack (Applebaum, 2019). The network has also consistently promoted Venezuelan opposition YouTuber Alberto Franceschi, a vocal supporter of Vox. In addition to Twitter, disinformation supporting Vox or Vox's political agenda frequently spread via WhatsApp and Facebook preceding the 2019 election (Smith, 2019).

While there is no direct evidence that the Venezuelan bots worked on behalf of a particular government or entity, the approach here is consistent with state-sponsored activities and consistent with Russian foreign policy goals. We therefore include the case as a state-sponsored IE, but code the attacker as 'unknown'.

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

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

FRARUS0001. Targeted country **France**. Attacking country **Russia**. Political goal **Discredit President Emmanuel Macron**:

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

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

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

The operation continued until 2020. Facebook took down pages that were attributed to "individuals associated with past activity by the Russian Internet Research Agency (IRA)." The network largely served to amplify a website called peacedata that claimed to be an independent news outlet working in English and Arabic (Nimmo, Francois, Eib, & Ronzaud, 2020a). Some accounts attacked France in general and President Emmanuel Macron in particular, and accused them of an "imperialist" approach toward Africa (Nimmo, Francois, Eib, & Ronzaud, 2020a).

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

A network of accounts on Facebook spread propaganda, mostly in French, from mid-2017 to November 2018 attacking Emmanuel Macron (Nimmo & Francois, 2018; Gleicher, 2018b). Macron Leaks had similarities to Russia's 2016 US interference. Most of the material came from the hacked Gmail accounts of people connected to Emmanuel Macron's campaign, and was extensively promoted on Twitter by bots (Volz, 2017). This effort strongly resembled Russian activities in the US and elsewhere, but while there are sources saying that Russia is behind the attack, there is no concrete evidence to prove the claim, and French officials have expressed uncertainty about who is responsible for the attack (Poulsen, 2018).

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

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

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

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

Among the 654 accounts taken down by Facebook in 2018, several promoted a page called Free Scotland 2014. With more than 20,000 followers, the Iranian-backed page was one of the most popular of those devoted to Scottish independence. It was one of several pages connected to fake "news" sites, including one linked to Iran's main propaganda source, Press TV (Dick, 2018). Nearly 1,000 Twitter and YouTube profiles linked with Iran were eventually taken down (C. Michel, 2018). The page, which has since been removed, was caught up in Facebook's recent dragnet of fake pages, accounts and campaigns. Facebook announced its largest haul to date, removing more than 650 pages and accounts. Twitter and YouTube followed suit, bringing the total to nearly 1,000 social-media profiles (C. Michel, 2018).

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

On May 28, 2019, Facebook took down 92 accounts, pages, and groups linked with Iran, some of which curated organic-looking content for the U.K. (Gleicher, 2019f). These personas criticized the supposed corruption of the royal family, contrasted with poverty

and health issues (Karan, Kaul, & Nimmo, 2019). Some accounts photoshopped images of the royals or overlayed pictures with comments about unreasonable costs on pages made to look as if they originated in the U.K. Personas sometimes posed as journalists to conduct interviews with made up UK-based individuals. The Facebook takedown closely followed and was related to Twitter's May 2019 removal of 4,800 Iranian-linked accounts (BBC, 2019b).

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

Thousands of Russia-linked Twitter bots promoted messages in favor of Brexit in the weeks leading up to the June 2016 referendum (Burgess, 2017). A "troll-army" of over 13,000 bots re-tweeted and shared messages that contained racist and anti-immigrant rhetoric. 400 Russian trolls using fake Twitter accounts also produced divisive and racist rhetoric to persuade voters in favor of leaving the European Union. Many of these accounts were tracked back to the Internet Research Agency (IRA). Some of these accounts promoted anti-immigrant sentiments and shared posts aiming to incite political discord between those in favor of Brexit and those opposed (Burgess, 2017).

The pro-Brexit campaign continued for some time after the referendum. And, as in the case of the US 2016 presidential elections, the Russian trolls opportunistically used real events to promote their pro-Brexit message. After the June 2017 terror attack on the London Bridge, for example, an account linked to the Russian effort used a photograph of a Muslim woman looking at her phone walking along the bridge to stir anti-Islamic sentiment, claiming that the woman ignored the injured (Ball, 2017; Hern, 2017).

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

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

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

state-supported outlets.

GBRRUS0004. Targeted country **Great Britain**. Attacking country **Russia**. Political goal **Inflame Brexit-related tensions**:

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

To date, researchers have been unable to identify a specific entity behind the Second Infektion operation, though similar social media campaigns have focused on topics including Ukraine, the US, European disunity, Russian dissidents, and anti-Islamic sentiment (Nimmo, Francois, Eib, Ronzaud, Ferreira, et al., 2020).

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

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

In 2020, Facebook took down a network of more than 300 Instagram and Facebook accounts originating in Iran and primarily targeting Israel. Facebook found links to individuals associated with EITRC, an IT company based in Tehran (Facebook, 2020c). Beginning in February 2020, the accounts began posting about Israel's response to COVID-19. In July, the network started using Hebrew in an effort to appear indigenous (Ronzaud, Hubert, & Nimmo, 2020). The campaign focused on attacking Prime Minister Benjamin Netanyahu, posting in support of the "Black Flags" protest movement.

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

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

tions on Russia, and have appeared on Kremlin-backed media including RT and news agency Sputnik (News, 2018).

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

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

In December 2020, Facebook removed an additional network of accounts, some of which sought to influence domestic politics in Libya. These accounts promoted the LNA and Gaddafi and in some cases, employed media staff from the LNA's Moral Guidance Department (Cryst, 2020). The network was linked to a daily podcast brand called Stop Terror, and accompanying Twitter accounts amplified the same content. The Russian network also targeted the Libyan Political Dialogue Forum (LPDF) in November 2020, which aimed to create a unity government during a ceasefire. According to a report from the Stanford Internet Observatory, "sockpuppet accounts pretending to be Libyans played an active role in amplifying the perception that the LPDF was taken over by Muslim Brotherhood elements" (Cryst, 2020). Media outlets Aljamahiria TV and Jana News Agency amplified similar messaging.

LTURUS0001. Targeted country **Lithuania**. Attacking country **Russia**. Political goal **Distort relationship between Lithuania and NATO**:

Russia engaged in an extended campaign to discredit NATO in Lithuania and other Baltic states.[1] The Russian campaign against European countries hosting NATO's operation in their territory has included spreading content intended to look like it was created in the targeted countries. Barojan (2018a), for example, describes how pro-Kremlin hackers placed an English article in the Lithuanian news outlet Kas Vyksta Kaune (What is Happening in Kaunas in English) on October 25, 2018. The article, an exact translation from the pro-Kremlin blogger Rudis Kronitis, claimed that Anakonda 2018, a NATO exercise in Lithuania, aimed at occupying Belarus. Fake accounts and news outlets such

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

as Paul Black, The Russophile and Russia News Now spread the article. Kas Vyksta Kaune pulled down the article when it learned it had been hacked.

Russia, through a variety of sources, has pushed narratives of Lithuania as a failed state alongside promoting anti-Western sentiment. A large portion of the content in these information campaigns is targeted at the military and joint operations with NATO, in an attempt to create political rifts around joint exercises. These appear to be the overarching themes of the Russian disinformation campaigns in the country which are reported to be "carried out on a daily basis" (Bankauskaitė, 2019).

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

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

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

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

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

In spite of Russia's interference effort, Macedonia formally changed its name and signed the Prespa Agreement with Greece in June 2018. Macedonia became a formal NATO member in March 2020.

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

A network associated with Russian oligarch Yevgeny Prigozhin interfered in Mozam-

bique's 2019 presidential elections on behalf of incumbent candidate Filipe Nyusi from the Frelimo party (Grossman et al., 2019). Prigozhin has close ties with Russian President Putin. The group created fake Facebook pages to amplify Nyusi support, praise the government's efforts to fight an Islamist insurgency, and defame the opposition Renamo party. Another entity associated with Prigozhin — the International Anticrisis Center — conducted an illegal poll and amplified results supposedly predicting a victory for Nyusi (Lister & Shukla, 2019).

MULARE0001. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Promote pro-United Arab Emirates (UAE) narratives in Iran, Qatar, and Turkey, among others**:

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

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

MULARE0002. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Isolate Qatar diplomatically and economically**:

Less than 48 hours after President Trump visited Saudi Arabia in May of 2017, the Qatar News Agency (QNA) and its associated social media pages were hacked. A fake speech was attributed to Qatar's Emir in which he praised Iran as well as Islamist groups Hamas, Hezbollah and the Muslim Brotherhood (Pinnell, 2018). An Al Jazeera investigation linked the hack to Saudi Arabia, though US intelligence found evidence of senior UAE officials discussing the attack a day before it occurred (DeYoung & Nakashima, 2017). Various countries including Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain used this fake story as a justification to break ties with Qatar and isolate the country diplomatically. The fake story was reported as fact by media outlets in the UAE and Saudi Arabia, and Twitter bots amplified anti-Qatar narratives both within Qatar and across the region (Jones, 2019).

Disinformation relating to Qatar has continued to circulate in the years following the QNA hacking, and in 2019, Facebook removed a commercial bot network associated with the companies "Newave" in the UAE and "New Waves" in Egypt which frequently aimed to

denigrate Qatar. Another Facebook takedown linked to the UAE included fake accounts targeting Qatar's Emir and news websites accusing Qatar of sponsoring terrorism (Karan, Rizzuto, & Kann, 2019). Although a number of Arab states participated in the attacks on Qatar, there is no clear evidence that the UAE coordinated with other countries.

MULARE0003. Targeted country **Multiple**. Attacking country **United Arab Emirates**. Political goal **Influence Libyan politics within Libya and internationally**:

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

In addition, UAE-based networks sought to influence international opinion towards the conflict in Libya and to distort public debate on the conflict there. A network of Twitter accounts which could not be definitively linked to the UAE amplified similar pro-Haftar and pro-UAE messaging in French and English. Consistent with the political agenda of the UAE's government, this campaign also attacked Qatar for supporting terrorism in Libya, targeted the Muslim Brotherhood, and criticized Turkey (Kassab & Carvin, 2019). Along with accounts from Saudi Arabia and Egypt, bots and influencers from the UAE used Arabic-language hashtags and local media outlets to promote Haftar. Pro-Haftar messaging dated as far back as 2013 and has continued with Haftar's subsequent efforts to seize power, with added emphasis on defaming Libyan Prime Minister Fayez al-Sarraj (Grossman, H., DiResta, Kheradpir, & Miller, 2020).

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

In 2019, Twitter released data on a series of removed accounts linked to state actors from the People's Republic of China. The network consisted of fake accounts and suspected bots which promoted content consistent with the interests of the Chinese government. According to analysis by the Australian Strategic Policy Institute (ASPI), accounts in the network were created as early as 2007 and acted as spam or marketing bots, but linguistic and behavioral data suggest the accounts were purchased and re-purposed by actors in China around mid-2017 (Uren et al., 2019).

From 2017 onward, tweets were primarily in Chinese and English, as well as Indonesian, Arabic, and several other languages. The self-reported locations of the accounts ranged around the world, but concentrated in the United States and Europe. Prior to 2019, campaigns focused on defaming prominent Chinese dissidents such as Guo Wengui, a Chinese businessman who fled to the United States and frequently speaks about corruption in the Chinese government. ASPI reported that the network sought to "influence the opinions of overseas Chinese diasporas, perhaps in an attempt to undermine critical coverage in Western media of issues of interest to the Chinese government" (Uren et al., 2019). In 2019, the Twitter campaign turned its attention to disrupting the pro-democracy protests

in Hong Kong, likely primarily targeting Hong Kong residents but also the international diaspora (Karan & Zhang, 2019). Based on a dataset from April 2020, researchers found inauthentic Chinese social media accounts promoting pro-China narratives related to Taiwan, responses to COVID-19, and George Floyd protests in the United States (Wallis et al., 2020).

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

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

In April of 2019, Libyan General Khalifa Haftar announced that the Libyan National Army (LNA) would pursue an offensive on the capital city of Tripoli. In the weeks preceding and following this announcement, disinformation campaigns originating in a variety of countries began promoting similar political narratives related to Libya. Commercial bot networks from Egypt posted and amplified hashtags in support of Haftar, including accounts linked to a technology company called DotDev which has offices in Egypt and the UAE (FSI, 2019). Elements of this campaign sought to influence public opinion within Libya. One suspected DotDev account impersonated a real LNA spokesperson, while another claimed to be "The Official page of General Khalifa Haftar."

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

MULFRA0001. Targeted country **Multiple**. Attacking country **France**. Political goal **Support Malian and French armed forces and counter Russian influence in Africa**:

In December of 2020, Facebook removed more than 100 assets linked with the French military and found to be engaging in coordinated inauthentic behavior targeting African countries (Gleicher & Agranovich, 2020). The earliest accounts in this network were created in May of 2018 and focused on military and security in Mali. A second network appeared in 2019 and focused on the Central African Republic. According to a report from Graphika and The Stanford Internet Observatory, "the French operation was, in part, a direct reaction to the exposure of Prigozhin's troll operations in Africa in 2019 by Facebook" (Graphika & Stanford Internet Observatory, 2020). Accounts used stolen or AI-generated profile pictures to appear organic and amplified the same content, often criticizing Russia's involvement in the CAR. The network also included at least one

YouTube channel and Twitter account. According to Facebook, "this was the first time our team found two campaigns — from France and Russia — actively engage with one another, including by befriending, commenting and criticizing the opposing side for being fake" (Gleicher & Agranovich, 2020).

MULRUS0001. Targeted country **Multiple**. Attacking country **Russia**. Political goal **Discredit the White Helmets Syrian civil defense organization**:

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

In the Khan Sheikhoun gas attack, around 6,000 Twitter accounts covering the attack were directly related to Kremlin. In some cases, the tweets called the chemical attacks a "false flag." A Twitter account, for example, says "CW used by #AlQaeda not by #Assad #Khansheikun was falseflag of alqaeda linked fake aid organisation #whitehelmets" (Jindia et al., 2017). In other cases they blamed SCD or other organizations with a low probability of working togethe (Bellingcat, 2018). Bots also amplified the misinformation campaign against the White Helmets with almost 150 tweets per day (Solon, 2017). The profiles suggest the accounts were tweeting independently from London, Berlin, Barcelona, Istanbul, New York, Chicago, Marseilles, and other places (Jindia et al., 2017).

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

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

MULRUS0002. Targeted country **Multiple**. Attacking country **Russia**. Political goal **Discredit Turkish political decisions:**

In November of 2015, Turkey shot down a Russian warplane at the Turkey-Syria border. Following this incident, Russia launched a news and social media campaign attacking the Turkish government, drawing links between Turkey and the Islamic State, and post-

ing false English-language articles designed to appear organic (Nimmo, Francois, Eib, Ronzaud, Ferreira, et al., 2020). Since then, Russian influence efforts have consistently criticized Turkish President Recep Tayyip Erdogan and Turkey's involvement in Syria and Libya. Facebook assets removed in September of 2020 incorporated this theme into inauthentic English and Arabic posts (Nimmo, François, Eib, Ronzaud, & Carter, 2020), as did Facebook and Twitter accounts removed in December of 2020 which targeted Libya, Sudan, and Syria (Grossman, Jonsson, et al., 2020). Networks were found to be affiliated with the Internet Research Agency (IRA) and Russian businessman Yevgeny Prigozhin. As with previous IRA influence efforts, operations employed local actors in Africa to create fake accounts and disseminate targeted content (Grossman, Jonsson, et al., 2020).

MULRUS0003. Targeted country **Multiple**. Attacking country **Russia**. Political goal **Discredit individuals raising awareness about Russian propaganda efforts**:

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

Finnish journalist Jessikka Aro was similarly targeted after her research on the location of IRA's headquarters was released in 2015 (Aro, 2015). This campaign was highly responsive, with participating trolls posting immediately after Aro's appearance on TV or radio (Blanco, 2019).[2]

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

MULRUS0004. Targeted country **Multiple**. Attacking country **Russia**. Political goal **Spreading misinformation in Central Asia and amplifying content of Sputnik**:

In January 2019, Facebook removed 289 Facebook pages, 75 Facebook accounts, and several Instagram accounts which originated in Russia (Satariano, 2019). The pages' main objective was to amplify content from two of Russia's state-backed media outlets, Sputnik and the video service TOK. Both outlets are associated with Rossiya Segodnya,

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

the Kremlin's media agency (Aleksejeva et al., 2019). The social media effort represented a systematic campaign to spread the content of the agency across 13 countries in Central Asia, namely Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, Armenia, Azerbaijan, Georgia, Moldova, Romania, Belarus, Estonia, Latvia, and Lithuania (Gleicher, 2019b). Pages and accounts were linked to employees of Sputnik and frequently posted about topics like anti-NATO and anti-corruption sentiment. The social media content and personas were adapted for local audiences and obscured any connection to Rossiya Segodnya. In some cases, the accounts claimed to be people indigenous to the target country.

All of these pages shared content from Sputnik and TOK, and in total the network amassed 853,413 followers. This represented a significant increase in audience compared to Sputnik's official following across the Central Asian countries. Over one-quarter of the pages were created in October 2017, with 32 produced in a single day. Moreover, some pages in the network cross-posted videos from Sputnik and TOK, indicating coordination (Aleksejeva et al., 2019).

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

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

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

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

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

In addition, a 2019 Twitter takedown of accounts created by the state-backed Saudi Arabian digital marketing company Smaat promoted similar political narratives aligned with

the Saudi Arabian government, though most Smaat content was commercial in nature (DiResta, Grossman, et al., 2019). Political accounts frequently focused on Khashoggi and criticizing the governments of rival countries Qatar, Turkey, and Iran. These accounts usually posted in Arabic and English but also Japanese, Russian, Spanish, and other languages (Gleicher, 2019d; DiResta, Grossman, et al., 2019).

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

As early as April of 2017, a network of Twitter bots primarily originating in Saudi Arabia was established to criticize Qatar and Iran and praise President Trump prior to his visiting Riyadh (Chappelle, 2018). In May of 2017, the Qatar News Agency (QNA) and its associated social media pages were hacked. A fake speech was attributed to Qatar's Emir in which he praised Iran as well as Islamist groups Hamas, Hezbollah and the Muslim Brotherhood (Pinnell, 2018). An Al Jazeera investigation linked the hack to Saudi Arabia, though US intelligence found evidence of senior UAE officials discussing the attack a day before it occurred (DeYoung & Nakashima, 2017). Various countries including Saudi Arabia, the United Arab Emirates, Egypt, and Bahrain used this fake story as a justification to break ties with Qatar and isolate the country diplomatically.

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

This operation extended into 2020, when Twitter removed 33 accounts linked to the Saudi Arabian government which sought to interfere in Qatari politics and undermine Qatar's government (Grossman, Khadija, et al., 2020). In some cases, Saudi accounts posed as members of the Qatari royal family and Qatari officials in exile. The Saudi network was also linked to a fabricated coup attempt in Qatar which was reported on social media and spread to news outlets around the world, "creating the impression that the Qatari state is weak and unstable" (Jones, 2020).

MULSAU0004. Targeted country **Multiple**. Attacking country **Saudi Arabia**. Political goal **Influence Libyan politics and regional views of the conflict there**:

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

In addition, campaigns linked with Saudi Arabia have aimed to influence domestic public

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

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

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

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

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

PHLCHN0001. Targeted country **PHL**. Attacking country **CHN**. Political goal **Support the Philippine Government**:

In 2020, Facebook removed 155 accounts, 11 Pages, 9 Groups and 6 Instagram accounts with links to the Chinese government for engaging in coordinated inauthentic behavior (Gleicher, 2020b). Following a U.S. commitment to defend the Philippines in the South China Sea in 2018, a share of this Chinese influence operation began focusing on territorial disputes and the Philippines, posting in support of President Rodrigo Duterte and other politicians favorable to China (Nimmo, Eib, & Ronzaud, 2020). A number of assets posted in Filipino, but also in Chinese, English, and Indonesian. According to The Diplomat, the Philippines "provided an ideal target for China to exercise its capabilities in foreign influence operations and is uniquely susceptible to manipulation through Facebook" (Winger, 2020). Accounts and pages in the network attracted millions of interactions, also advancing "pro-Beijing disinformation on sensitive geopolitical issues such as the South China Sea disputes and Hong Kong; denigrating liberal media personalities and platforms; and support for Sara Duterte's possible candidacy in the 2022 presidential

election" (Heydarian, 2020).

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

Shortly after the Maidan protests began in Kiev, a wave of anti-Ukrainian propaganda started to appear on the web in 2013 as noted by analysts from Poland (Savytskyi, 2016). The trolls consistently repeated the views of Russian authorities on places such as the Internet forum of the Russian-Polish Radio Sputnik Polska. Their posts in the fall of 2013 were primarily aimed at agreeing with and amplifying anti-Ukrainian stories (Savytskyi, 2016).

SAUIRN0001. Targeted country **Saudi Arabia**. Attacking country **Iran**. Political goal **Criticize the Saudi Arabian government**:

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

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

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

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

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

From at least 2017 onward, former Sudanese President Omar al-Bashir maintained a close relationship with Russia. Also during this period, the Kremlin-linked paramilitary organization Wagner Group trained local Sudanese forces (Grossman et al., 2019). With

the outbreak of anti-government protests in late 2018, a network associated with Russian oligarch Yevgeny Prigozhin created a strategy to maintain Bashir's power. The Russian mining company M-Invest, which has an office in the Sudanese capital of Khartoum, was the source of the proposal (Lister et al., 2019). Leaked documents reveal that the Russian network sought to discredit Sudanese protests through a disinformation campaign on social media, linking demonstrations to Israel and anti-Islamic sentiment. The proposal suggested building social media teams to attack protesters in parallel and support the government. In addition, the Russian network designed news websites such as Sudan Daily which frequently reposted content from the Russian outlet Sputnik (Alba & Frenkel, 2019).

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

In December of 2020, Facebook removed an additional network of IRA-linked accounts targeting Sudan and employing fake news websites in a similar manner to the 2019 campaign (Cryst, 2020). The accounts focused on Sudan's economic crisis, and also praised paramilitary forces, Russian involvement in the country's mining industry, and a potential Russian naval base to be established in Sudan.

In May 2021, Facebook removed more Sudanese pages linked to Russia. The pages look like the ones Facebook took down before, but the content was explicitly in favor of Russian interests (Facebook, 2021). In particular, these Facebook pages aimed at persuading the Sudanese people and to accept the Russian naval base in east Sudan (Suliman, 2021).

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

In 2018 Swedish officials stated they were seeing an increase in hacking and dissemination of fake news with the goal of undermining the stability of Swedish society (Brattberg & Maurer, 2018). They highlighted misleading media reports that were being used to "frame NATO as an aggressor and military threat, the EU as in terminal decline, and Russia as under siege from hostile Western governments" (Brattberg & Maurer, 2018). There is also evidence identifying "troll armies" targeting Swedish journalists and academics, hijacked Twitter accounts, and pro-Kremlin NGOs operating in Sweden (Henley, 2017). According to the Swedish Security Service, Russian tactics ranged from online trolls and disinformation campaigns to efforts to demonize Swedish politicians and authorities (Radio, 2016).

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

Facebook took down a number of pages accused of "coordinated inauthentic behavior," based in Thailand but with substantial connections to Russia (Poulsen, 2019). The pages' spread content supportive of Russian foreign policy preferences while masquerading as organic Thai individuals. This network of 22 fake profiles drove people to off-platform blogs pretending to be local news outlets and claiming to have Thailand-based writers. Stories often countered the narratives of American media outlets or criticized Western

influence in Southeast Asia. One page, for example, shared a story claiming that "the US and its allies are also busy locking up journalists like Julian Assange for exposing their own extensive right violations," a form of "human rights hypocrisy" (Gleicher, 2019c). Another article was titled "Why is the Financial Times Smearing Thailand?"

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

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

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

China attempted to sow discord in Taiwan's 2018 presidential elections through the use of Facebook bots, Weibo, Line, and other platforms (Kurlantzick, 2019). In Taiwan's 2020 general election, researchers again linked online interference efforts with China, noting that the CCP "owns many information operation units and outsources its missions" (Lee et al., 2020). The network aimed to undermine the campaign of incumbent President Tsai Ing-Wen and support a Beijing-friendly candidate (Kurlantzick, 2019). While direct attribution of influence efforts can be challenging, a 2020 report found that extensive, coordinated disinformation targeted Taiwan's democratic governance in recent years had typical signatures of Chinese operations (Monaco et al., 2020).

In 2020, Taiwanese officials accused China of propagating misinformation about the COVID-19 pandemic in Taiwan, although China denied these claims (Reuters, 2021). As one report explains, "Taiwan is on the frontlines of the Chinese Communist Party's (CCP) international influence operations, and what happens on the island often serves as a harbinger for how China will operate elsewhere" (Monaco et al., 2020).

UKRRUS0001. Targeted country **Ukraine**. Attacking country **Russia**. Political goal **Reduce support for Donbass conflict**:

Since 2014, Russian information operations have supported the country's military activities in Ukraine. The operation included common propaganda aimed at discrediting

the Ukrainian government—through, for example, claims that Ukraine is ruled by "successors of the Nazis" (Sazonov et al., 2016; EUvsDisinfo, 2019b)—alongside a campaign pretending to be organic from Ukraine, where Russian trolls used social media to blame Ukrainian government for the Donbass conflict (Andrusieczko, 2019).[3]

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

In 2020, Facebook removed additional accounts promoting Russian propaganda and disinformation in Ukraine (Facebook, 2020a). Pages within this network included "Donbass Back to Russia" with more than 6,000 followers, primarily amplifying content from the Russian outlet News Front (Karan et al., 2020). News Front arose as a Russian federal agency outlet in 2015, and although it claims to have become independent, some have linked the outlet to funding from the Russian intelligence services.

UKRRUS0002. Targeted country **Ukraine**. Attacking country **Russia**. Political goal **Support the Annexation of Crimea to Russia**:

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

On April 30, 2020, Facebook also took down 140 assets connected to Russian propaganda outlets News Front and South Front which engaged in coordinated inauthentic behavior (Facebook, 2020a). The fake accounts posted about an array of political topics around the world, including the annexation of Crimea (Karan et al., 2020).

USACHN0001. Targeted country **United States**. Attacking country **Russia**. Political goal **Polarize American politics**:

Beginning in 2017, a small network of inauthentic social media accounts linked with the Chinese government began posting about U.S. politics in English and Chinese. The accounts posed "as politically engaged users on both sides of the partisan divide" (Nimmo, Eib, & Ronzaud, 2020). Researchers identified a group named Trump KAG 2020 that claimed to support U.S. President Donald Trump's re-election, while a group named Biden Harris 2020 largely criticized Trump. The U.S. oriented operation did not survive long enough to amass a significant following or to articulate a clearly defined political goal.

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

Facebook removed the network of Facebook and Instagram assets in September of 2020 (Gleicher, 2020b). Nimmo et al. (2020) add that it is "possible that the intention was to further polarize America's political landscape by affirming each side's view of the other, but in that case, it is strange that the operation paid no attention to more progressive groups and candidates, such as senators Bernie Sanders and Elizabeth Warren."

In the days leading up to the 2020 U.S. presidential election, the Crime and Security Research Institute identified a network of inauthentic Twitter accounts producing both anti-Trump and anti-Biden content, though emphasis was placed on anti-Trump posts (Crime and Security Research Institute, 2021). Accounts posted in both English and Chinese, and although they could not be definitively linked to the Chinese government, operational patterns suggested official oversight. The network sought to avoid detection through subtle coordination and a lack of hashtags. A U.S. Intelligence report released in March of 2021 found that China did not attempt to interfere in the 2020 elections (Cohen & Herb, 2021), however a significant body of evidence documented inauthentic activity linked to the Chinese state.

Also in 2020, social media accounts associated with the 'Spamouflage Dragon' network began posting in English and attacking the administration of President Trump (Nimmo, François, Eib, & Ronzaud, 2020). Accounts impersonated Americans and sought to avoid detection through the use of AI-generated profile pictures on Twitter and YouTube. This network also criticized U.S. foreign and domestic policy, the closure of the Chinese consulate in Houston, Texas, and threats against the video platform TikTok (Nimmo et al., 2019).

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

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

On March 10, 2020, the National Intelligence Council (NIC) released a declassified report on Foreign Threats to the 2020 US Federal Elections, which stated that Iran launched an influence campaign to sow division between races (National Intelligence Council, 2021).

Leading up to the presidential election in 2020, Twitter removed 368 accounts which originated in Iran and sought to interfere in campaigns. Most of the accounts attacked Donald Trump using the hashtag "Resistance," but a small number of accounts supported Trump's reelection (Goldstein & Hundley, 2021).

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

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

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

On March 10, 2021 the National Intelligence Council (NIC) released a declassified report on Foreign Threats to the 2020 US Federal Elections. The NIC stated that Iran launched an influence campaign against President Trump's reelection, although the network did not directly promote Trump's presidential rivals. The campaign also aimed to "undermine public confidence in the electoral process and US institutions" (National Intelligence Council, 2021).

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

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

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

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

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

A network thought to be of Iranian origin created social media personas posing as Americans, including journalists and Republican candidates for the U.S. House of Represen-

tatives in 2018 (Revelli & Foster, 2019). These accounts posted general pro-Iranian messages, including anti-Saudi, anti-Israeli, and pro-Palestinian themes (Revelli & Foster, 2019). They also posted in opposition to President Trump, and in some later cases posted anti-Iranian messaging, perhaps to build a broader audience or foster polarization. The accounts impersonating American political candidates directly plagiarized tweets and pictures from the real candidates and created original content about the Kavanaugh hearings as well as typical pro-Iranian messages (Timberg & Romm, 2019).

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

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

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

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

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

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

The Main Intelligence Directorate of the General Staff (GRU) engaged in a concerted long-term effort to damage the political prospects of Democratic Party candidates in two elections cycles. A key method in 2016 was releasing documents stolen through computer intrusions. A group of at least 13 Russians, including businessman and Putin groupie Yevgeny Prigozhin, were indicted for their efforts to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC). The attackers used the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page,

to steal DCCC credentials and modify the DCCC website, redirecting visitors to the actblues.com domain. They stole approximately 2.5 gigabytes of data, including donor records and personal identifying information from more than 2,000 Democratic donors. This information was transferred to registered state lobbyists, as well as senior members of the Trump presidential campaign and online sources of political news (Muller, 2018).

The campaign included fake accounts on social media trying to persuade voters not to choose the Democratic Party.[4] A Russian-created Twitter account, for example, tweeted in February 2018: "The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals and dead voters." Another account tweeted instructions for Americans to donate money to defeat Democratic candidates such as Maxine Waters, Elizabeth Warren, and Nancy Pelosi. Russian trolls also defamed Democrats with tweets, using the term "rapefugees", to associate democratic candidates with cases of sexual assault by migrants (Nimmo, Brookie, & Karan, 2018c).

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

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

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

A coordinated campaign sought to discredit the US Federal Bureau of Investigations (FBI) from 2017 onwards, especially its research on Russian influence operations. This was part of a larger campaign to discredit American institutions (Boatwright et al., 2018; Nimmo, Brookie, & Karan, 2018a). For example, Russian trolls promoted the effort to force the release of classified documents which allegedly show bias against President Trump at the Justice Department by promoting the hashtag #releasethememo in early-2018 (e.g. by driving a thousandfold increase in the hashtag's prominence on January 19, 2018) (RFE, 2018). Trolls linked to the Internet Research Agency (IRA) also specifically targeted African Americans and Mexican Americans in an apparent effort to reduce their respect for government institutions (Howard et al., 2019).

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

Private firms in Russia, i.e. 'troll factories', were paid by the Russian government to spread pro-Trump propaganda on social media (Chen, 2015; Bertrand, 2016). The trolls, for example, used Facebook to organize more than a dozen pro-Trump rallies in Florida during the 2016 election, which were then promoted online by local pro-Trump activists (Poulsen et al., 2017). A typical post by a Kremlin troll called "Bertha Malone", who

[4]See DiResta et al. (2019) for a detailed analysis of the specific content behind this campaign and other Russian ones targeting the US.

had at least 400 posts on Facebook, said on this: "if only media had been as bothered by Obama's ties to the Muslim Brotherhood as they are by Trump's fake ties to Russia" (Poulsen & Ackerman, 2018). Using data from Facebook, Google, Instagram, Twitter and Youtube between 2015 and 2016, Howard et al. (2019) conclude that the messages created by the IRA were primarily designed to benefit the Republican Party and then-candidate Donald Trump.

Leading up to the 2020 U.S. presidential election, a network of Russian accounts was operated by the Newsroom for American and European Based Citizens (NAEBC), an organization run by people linked to the Russian Internet Research Agency (IRA) (Stubbs, 2020). As in 2016, this campaign promoted Trump's reelection, targeting far-right users on social media and fake websites (Graphika Team, 2020). This was also the first time that a Russian operation employed the platforms Gab and Parler. According to the U.S. National Intelligence Council, the Russian government and Russian President Putin were responsible for operations aimed at attacking the Biden campaign and supporting Trump (National Intelligence Council, 2021).

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

Between 2016 and 2018, a number of websites operated with the aim of stealing information from conservative groups critical of then-US President Donald Trump. The targets were former Trump supporters who had subsequently called for more sanctions against Russia. Research by Microsoft pointed out that the websites were created by the group of hackers APT28, which has been publicly linked to a Russian intelligence agency and actively interfered in the 2016 presidential election (Sanger & Frenkel, 2018).

As part of a Russian state-backed campaign, an online article titled "Paul Ryan Opposes Trump's immigration Cuts, Wants Struggling American Workers to Stay Poor" was manufactured. In it, House Speaker Paul Ryan, a key congressional ally of Trump's whose 2016-era opposition faded after election day, was to be branded "a complete and absolute nobody incapable of any decisiveness" (Holt, 2017).

Another online article, titled "Pro-Amnesty Sen. Marco Rubio: Trump's immigration Bill Will not Pass the Senate," circulated, in which another one-time Trump rival turned supporter, Sen. Marco Rubio of Florida, was supposedly "exposed as a fake conservative who is a traitor to Republican values who in his soul despises the American Constitution and civil liberties" (Holt, 2017).

Yet another online article, titled "McCain says Thinking a Wall Will Stop illegal immigration is Crazy," was posted, targeting the late senator John McCain. The article was intended to brand McCain "as an old geezer" who belongs in a nursing home. McCain's "pathological hatred" of Trump was a potent area of emphasis, with such "dishonorable scoundrels, such as McCain, immediately aim[ing] to destroy all the conservative voters' hopes as soon as Trump tries to fulfill his election promises" (Holt, 2017).

A similar online article, titled "Dobbs Slams McConnell, Says it is time to Ditch Mitch", pushed the view that it was time for Senate Republicans leader Mitch McConnell to retire (Holt, 2017).

USARUS0007. Targeted country **The United States**. Attacking country **Russia**.

Political goal **Polarize American Politics**:

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

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

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

The propaganda included a social media operation run from Ghana which targeted black communities in the US. A deep analysis of the operation's content concluded that the Ghanian NGO was a front for the Russian IRA (Nimmo, François, Eib, Ronzaud, Smith, et al., 2020).

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

Following the 2011 protests against Syrian President Bashar Assad, Russian operatives enhanced social media efforts promoting "anti-Western, anti-rebel, and pro-Assad narratives" (DiResta & Grossman, 2019). The Russian military intelligence service (GRU) created fake media outlets such as Inside Syria Media Center (ISMC) and associated social media profiles which produced content in English and Arabic. Manufactured journalistic personas published articles across a number of mainstream media websites in the U.S. (St. Clair & Frank, 2018). In 2020, Facebook removed 214 accounts, 35 pages, 18 groups and 34 Instagram accounts associated with this operation (Nimmo, François, Eib,

Ronzaud, & Carter, 2020).

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

In 2020, Facebook removed an additional network of accounts linked to the Russian GRU, with some content focusing on Syria and the United States (Gleicher, 2020c). This campaign rarely focused on domestic U.S. politics, but some assets targeted U.S. involvement in the Middle East. For instance, one Facebook page was called "USA out of Syria" and purported to show a mural of George Floyd in Syria (Nimmo, François, Eib, Ronzaud, & Carter, 2020). At the same time, these accounts praised Syrian President Bashar Al-Assad and Russian involvement in the conflict.

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

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

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

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

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

In the 2017 Alabama special election for a US Senate seat, Kremlin-linked news sites and trolls supported Roy Moore, the Republican candidate accused of sexual misconduct against multiple women (Clifton, 2017). 20,000 to 25,000 tweets were sent out daily using the hashtag #alabamasenaterace from approximately 600 twitter accounts. These

accounts were being monitored by the cyber security research project Hamilton 68. It was reported that "Among pro-Moore articles, close to 70% attacked the credibility of the accuser(s), 38% attacked the media, the Washington Post in particular, and one story attacked Lindsey Graham for not defending Moore" (Schafer, 2017). Not all the support that Moore received on the Internet came from Russia. The New York Times reported that a group of "Democratic tech experts" used Russian-style disinformation tactics during Alabama's 2017 special election in an attempt to splinter support for Moore (Shane & Blinder, 2018). The Washington Post also reported that Facebook suspended accounts used by five people involved in the project (Romm & Timberg, 2018). Although the tactics were similar to those used by Russian trolls, they were not part of this FIE.

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

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

Ahead of the 2020 U.S. presidential election, a Russian campaign again sought to attract far-right American voters. The media organization Newsroom for American and European Based Citizens (NAEBC), which was run by people associated with the Internet Research Agency, was at the center of this influence effort. The website mainly republished articles from conservative media and created original content in favour of white supremacy (Stubbs, 2020). Russian operatives also established profiles on the platforms Gab and Parler (Graphika Team, 2020).

USARUS0013. Targeted country **The United States**. Attacking country **Russia**. Political goal **Spreading misinformation in the US**:

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

USARUS0014. Targeted country **The United States**. Attacking country **Russia**. Political goal **Attack Joe Biden in the 2020 U.S Presidential election**:

In 2020, the U.S. Office of the Director of National Intelligence stated that Russia was employing a range of measures to target Joe Biden ahead of the presidential election. This effort included pro-Russia Ukrainian officials who propagated false information about corruption and scandals within the Biden campaign (Evanina, William, 2021). Facebook removed a number of accounts associated with this campaign, linking operators to the Russian Internet Research Agency. This is the first IRA-linked operation in which

Facebook accounts were found using AI-generated profile pictures, and the network often promoted a fake news outlet called peacedata.net which posted in English and Arabic (Nimmo, Francois, Eib, & Ronzaud, 2020a). In addition to attracting a left-wing audience and criticizing the Biden campaign, the network posted about race protests, accusations of U.S. war crimes, and corruption. Attacks on liberal candidates and policies are consistent with the IRA's activities in 2016 which targeted then-candidate Hillary Clinton (Nimmo, Francois, Eib, & Ronzaud, 2020a). Related accounts were removed from Twitter and LinkedIn, attempting to build personas which appeared authentic (Allyn, 2020).

Russian military hackers associated with the group known as Fancy Bear or APT28 also targeted Ukrainian gas company Burisma where Joe Biden's son, Hunter Biden, served on the board (Greenberg, 2020). According to The New York Times, the attack seemed aimed at producing "embarassing material on the Bidens," similar to emails obtained by Russian hackers from the Hillary Clinton campaign in 2016 (Perlroth & Rosenberg, 2020).

An additional component of undermining the Democratic presidential candidacy was supporting the campaign of Senator Bernie Sanders (Harris et al., 2020). Sanders received a disproportionate amount of positive coverage on Russian news agencies RT and Sputnik as well as inauthentic social media accounts on Facebook and Instagram (Mak, 2020).

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

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

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

The Guardian identified more than 150 domains registered in Veles, Macedonia, that published political news about the United States. Headlines included "Hillary's Illegal Email Just Killed Its First American Spy", "This is How Liberals Destroyed America", and "This Is Why We Need Trump in the White House" (Petreski & Karan, 2019). Articles on the website appeared to use sensationalist headlines to obtain traffic, similar to clickbait. The websites received some engagement on social media platforms Twitter and Facebook, but most traffic to the website was direct (Petreski & Karan, 2019; Subramanian, 2017).

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

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

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

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

The Rhodes Must Fall and Fees Must Fall Movements in South Africa resemble The Black Lives Matter movement in America. Russian operatives engaged both movements in a minor way. Of the 3 million tweets written by Russian trolls identified by Twitter in 2018, some consisted of info-graphics that misrepresented land or race facts in South Africa (Boatwright et al., 2018). The accounts also spread a white genocide meme, with the intent of polarizing opinions over race (Superlinear, 2018). Yevgeny Prigozhin, indicted for his leadership of the Internet Research Agency, has reportedly opened technology centers in Central Africa, where his team will research and send out social media messages about the upcoming elections to try and make people vote for Pro-Russian relations in Africa (Pertsev, 2018).

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

Leading up to South Africa's presidential election in May of 2019, a Russian network sought to promote disinformation and influence voters. A campaign associated with Russian oligarch Yevgeny Prigozhin, a Russian NGO called the Association for Free Research and International Cooperation (AFRIC), and the International Anticrisis Center worked to support South Africa's ruling African National Congress (ANC) party (Haffajee, 2019). Leaked documents reveal a proposal to disseminate pro-ANC videos and use social media to defame opposition leaders. Some fake Twitter accounts were established for the ANC, but ultimately the Russian campaign seemed to have little effect on the election (BusinessTech, 2019). The ANC has maintained a positive relationship with Moscow since the era of fighting against the apartheid regime (Burke & Harding, 2019).

C.2 Domestic Influence Efforts

AZE0001. Targeted country **Azerbaijan**. Political goal **Support Azerbaijan government and discredit its opponent**:

As early as 2014, researchers documented a social media manipulation network operated by a section of Azerbaijan's ruling party, the Youth Union of New Azerbaijani Party (YAP). Pearce (2014) identified state-affiliated Facebook and Twitter accounts trolling political dissidents, hijacking or amplifying hashtags, and coordinating posts. The author also found that party members would "create or purchase fake Twitter accounts... to both tweet messages on a particular hashtag and to 'follow' the pro-government youth group users."

In August of 2019, a Facebook employee alerted the company of this domestic influence effort (J. C. Wong & Harding, 2021). The operation used both fake accounts and induced genuine users to set up inauthentic profiles, which supported the ruling party and attacked opposition on social media platforms (Silverman & Mac, 2020). In November of 2020, Facebook took down 589 accounts, 7,665 pages, and 437 accounts on Instagram linked to the operation, which posted primarily in Azerbaijani during normal work hours (Gleicher, 2020a). In April of 2021, The Guardian reported that the Azerbaijani troll network has returned to the platform (J. C. Wong & Harding, 2021).

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

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

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

In 2021, Wikipedia banned accounts for bullying editors promoting Democracy in Beijing. The blocked accounts also supported the Chinese government in the platform (Silva, 2021). In the same year, Twitter removed accounts linked to the Chinese government for inauthentic networks. The Twitter profiles amplify the narratives of the Chinese Communist Party (CCP) about Xinjiang and the minority population, and the government's efforts to fight the COVID-19 (DiResta et al., 2021).

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

Since as early as 2015, Cuba's ruling Communist Party is thought to have coordinated the creation of Twitter bots and fake accounts to campaign for the party and promote political narratives (Torres & Vela, 2018). According to reporting from 2019, so-called

"ciberclarias" or cyber catfishes are Cubans who maintain fake social media accounts on behalf of Cuba's intelligence agency in return for cell phone data or other "privileges" (González, 2019). Some ciberclarias are students recruited from Cuba's University of Informatics Sciences (UCI). These accounts often post in support of Cuba's political elite, attack opposition journalists, and downplay human rights abuses for an international audience (ADNCuba, 2020). In May of 2020, multiple sources reported on apparent instructions distributed to Cubans maintaining fake accounts on how to respond to the broadcast of an "anti-Cuban" interview with American officials (RadioTelevisionMartí, 2020).

In 2020, Twitter removed an additional 526 accounts linked to the Federación Estudiantil Universitaria, a student union tied to the country's Communist Party (Cryst & Perkins, 2020). Accounts relied on hashtags and promoted the Cuban government and policies, particularly Cuba's response to COVID-19. The network also attacked the U.S. and the trade embargo against Cuba (Cryst & Perkins, 2020).

ECU0001. Targeted country **Ecuador**. Political goal **Support Ecuadorian president Rafael Correa and discredit his opponent** :

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

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

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

GEO0001. Targeted country **Georgia**. Political goal **Promote ultra-nationalist political party Georgian March**:

Individuals linked to ultra-nationalist political party Georgian March and pro-government fringe media outlet PosTV used a single inauthentic network to promote their content (Gelava & Buziashvili, 2020). The network camouflaged itself as entertainment and online shopping platforms and included up to 30 Facebook groups, 30 pages, and 10 personal accounts (Gelava & Buziashvili, 2020). Georgian March has strong ties with local pro-Kremlin actors, including the Y. M. Primakov Georgian-Russian Centre and Levan Vasadze, a millionaire and supporter of local conservative and far-right groups (Gelava & Buziashvili, 2020).

Civil society representatives and political experts have long raised concerns about the affiliation of Georgian March with the ruling Georgian Dream party. Until 2016, the

leader of Georgian March, Sandro Bregadze, was the government's Deputy Minister of Diaspora Affairs. *Ifact*, a group of Georgian investigative journalists, reported that Bregadze's relatives donated to Georgian Dream in the pre-election period in 2016 (Gelava & Buziashvili, 2020).

PosTV is a government-affiliated television outlet that started broadcasting in 2018. PosTV has also been involved in organizing disinformation campaigns on Facebook attempting to discredit protests that erupted in June 2019 after the visit of Russian MP Sergey Gavrilov to Georgia (Gelava & Buziashvili, 2020).

Further coordinated disinformation efforts were uncovered by Gigitashvili (2020), who studied two distinct networks of Facebook pages spreading fake news in the run-up to the 2020 parliamentary elections in Georgia. One of the networks spread misinformation against the ruling party Georgian Dream, while the other shared content against opposition parties.

CHN0002. Targeted country **China**. Political goal **Undermine and delegitimize the Hong Kong protests**:

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

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

HND0001. Targeted country **Honduras**. Political goal **Support Honduran President Juan Orlando Hernández**:

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

García-Camargo, 2020).

There is also evidence that the private Israeli firm Archimedes Group financed advertisements and created fake accounts supporting President Hernandez and attacking the opposition in 2019. However, this effort has not been definitively linked to Hernandez or any government officials (Bandeira, 2019).

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

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

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

KOR0001. Targeted country **South Korea**. Political goal **Support Park Geun-hye in 2012 Korean presidential elections**:

Before the domestic influence effort started, the National Intelligence Service (NIS), the intelligence agency of South Korea, leaked a sensitive and secret transcript in late June 2012, targeting the opposition of Park Geun-hye, who ultimately won the presidential elections in 2012. The document revealed a plan of Roh Moo-hyun, the former Korean president and the opposition to Guen-hye, to redefine the sea border with North Korea to help build peace (Cain, 2013).

Keller et al. (2020) detected the disinformation campaign using information from a list of Twitter accounts published in court proceedings against the NIS. The author found that, for the 2012 South Korean presidential election, trolls covered a specific agenda every workday and operated from 9 am to 5 pm. They also found 153,632 instances of account pairs posting the same original tweet within a minute, a very suspicious pattern compared to non-troll accounts in the country.

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

Leading up to the 2017 Mexican gubernatorial elections, the Governor of the State of

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

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

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

MLT0001. Targeted country **Malta**. Political goal **Discredit prominent opponents of the Maltese government**:

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

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

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

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

In one effort to consolidate power, social media operatives created Muslim Facebook pages to warn of imminent anti-Muslim protests organized by Buddhist monks. At the

same time, operatives created Buddhist Facebook pages claiming that "jihad attacks" were being planned by Rohingya Muslims. By distorting reality through the use of social media, this campaign aimed to stoke fear and distrust along ethnic lines (Mozur, 2018).

In 2020, Facebook removed additional networks of inauthentic accounts linked to the Mynamar military, particularly preceding the country's general election in November of 2020 (Gleicher, 2020a). Accounts promoted the military and the "military-backed opposition party the Union Solidarity and Development Party (USDP)" (Nimmo, Ronzaud, et al., 2020). Accounts posed as voters and drove users to off-platform websites. Another Facebook cluster removed in late October 2020 was largely profit-seeking, but some content included pro-military political speech or dangerous speech against Muslim Rohingya people (Ronzaud, Eib, et al., 2020).

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

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

In August 2020, Facebook took down a second, smalled network of accounts, pages and groups originated in Pakistan and operating during 2020 (Facebook, 2020b). The network focused on attacking people that were critical of Pakistan's government or supportive of India (Facebook, 2020b).

PHL0001. Targeted country **Philippine**. Political goal **Discredit critics of President Rodrigo Duterte and support Philippine military**:

Facebook removed inauthentic assets linked to the Philippine military. On September 22, 2020, the social media company took down 31 pages and 77 Facebook and Instagram accounts it linked to individuals affiliated with the Philippine military for engaging in coordinated inauthentic behavior targeting domestic audiences in the Philippines (Cryst, 2020).The earliest post was reported in 2015, attacking the critics of President Rodrigo Duterte (Kharazian & Knight, 2020).

There was also evidence that several military-linked user accounts were coordinating social media campaigns in private Facebook groups, although the exact nature of what they were discussing within those groups could not be determined. Multiple user accounts in the set belonged to individuals who appeared to be serving in the Philippine military, including, notably, Alexandre Cabales, Chief of the Army Social Media Center (Kharazian & Knight, 2020).

Local as well as international human rights organizations have accused the Duterte government of red-tagging, i.e. labeling Duterte critics as communist insurgents, and even accusing them of terrorist recruitment (Kharazian & Knight, 2020).

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

A number of government officials including former Puerto Rican Governor Ricardo Rosselló participated in a Telegram chat which is thought to have coordinated the behavior of a group of pro-government Twitter trolls (Sepúlveda, 2019). The Twitter accounts supported Rosselló and his administration, promoted a hashtag in support of Puerto Rico's police, and targeted political opponents. For example, the network attempted to associate the mayor of San Juan and a Puerto Rican senator with the Nicolás Maduro regime in Venezuela after similar instructions appeared in the Telegram chat (Bandeira & Ponce de León, 2019).

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

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

After the murder of vocal Putin critic and politician Boris Nemtsov on February 26, 2015, for example, an extensive network of bots shared and promoted narratives questioning the circumstances surrounding Nemtsov's death. This effort was coordinated by the Internet Research Agency (IRA) and persisted throughout 2015, peaking from the time of the assassination through early March 2015. Trolls attempted to discredit both Nemtsov and political opposition by claiming that Nemtsov was murdered to attract more people to an anti-government rally planned for March 1, 2015 (Khachatryan, 2015).

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

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

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

protest.

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

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

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

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

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

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

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

THA0001. Targeted country **Thailand**. Political goal **Promote the Thai government and military while silencing political dissent**:

In October of 2020, Twitter removed 926 accounts linked to the Royal Thai Army (RTA)

which promoted pro-RTA and pro-government messaging. Most accounts were created in January of 2020 and targeted candidates from political opposition groups, including the Future Forward Party (FFP) and the Move Forward Party (MFP). The network also praised the Thai government's response to COVID-19. According to an investigation by the Stanford Internet Observatory, this campaign marks "the first time a social media company has suspended a network of accounts linked to the Royal Thai Army," although the government has been accused of social media manipulation in the past (Goldstein et al., 2020). Following the Twitter removal, the Thai army denied responsibility for the disinformation campaign (Tanakasempipat, 2020). In addition to social media interference, Thailand created an "anti-fake news" center in 2019 which censors online political speech, encourages citizens to report anti-government messaging, and distributes harsh prison sentences (Tanakasempipat, 2020).

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

The Tajik government is suspected of maintaining a "troll farm" for amplifying political propaganda and suppressing dissidence online (RFE/RL, 2019). Some fake pro-government accounts are run by unpaid university students and staff, who say that they are threatened into compliance by school administrations and officials from the Education and Science Ministry. Other social media profiles are thought to be maintained by paid operatives from a state-backed network which promotes government narratives, including the notion that Tajikistan is free of COVID-19 (Eurasianet, 2020). Social media trolls are also used to harass political critics such as journalist Humayra Bakhtiyar, who reported on corruption in Tajikistan (CPJ, 2019).

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

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

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

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

For several years, Venezuelan President Nicolás Maduro has used social media to promote political content supportive of his regime. State-linked Twitter account creation first

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

In addition, a Twitter network originating in Venezuela frequently posted in English about such topics as the 2018 U.S. midterm elections, though this could not be definitively attributed to Venezuelan state actors ("Twitter and F]acebook say they removed thousands of troll accounts in run-up to 2018 midterms, author=Collins, Ben, year=2019, publisher=NBC News, url = https://www.nbcnews.com/tech/security/twitter-says-it-removed-troll-accounts-tied-russia-iran-venezuela-n965491, urldate = 2019-01-31", n.d.). According to Twitter, this campaign seems to have been operated by a "commercial entity originating in Venezuela" (Roth, 2019).

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

In 2017, the Vietnam People's Army (VPA) created a cyber military unit called Task Force 47, a 10,000-strong network used to attack the Vietnam Communist Party's political opponents and promote government content on Facebook and other social media platforms (Phuong, 2018). Officially, Task Force 47 is comprised of military personnel trained to combat the "peaceful revolution" of Western political ideology online. In addition, Force 47 suppresses and attacks political dissidents, who often face penalties and prison time for criticizing the government (Hookway, 2017).

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

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

Leading up to Zimbabwe's 2018 presidential election, both the ruling Zanu-PF party and the opposition MDC-Alliance made use of "online warriors," including bots, paid workers, and youth volunteers. These networks promoted doctored images and fake stories to "project the false impression of overwhelming support" and undermine the opposition (Moyo, 2018). The incumbent President Emerson Mnangagwa, who took power after a military coup in 2017, dubbed his online campaigners the "Varakashi", meaning destroyers, and encouraged them to attack enemies of the party online (Mwareya, 2019). Following Mnangawa's election, the Varakashi used fake accounts to disrupt criticism of the administration. In addition, opposition candidate Nelson Chamisa accused Zanu-PF of employing "foreigners" in a fake news campaign, using language suggesting he was referring to Russian assistance (T. Griffin, 2018).

D References for Online appendix (not for publication)

Ackerman, S. (2018). Russia is exploiting american white supremacy over and over again. Retrieved 2019-05-01, from https://www.thedailybeast.com/how-russia-exploits-american-white-supremacy-over-and-over-again

ADNCuba. (2020). ¿cómo detectar a una ciberclaria? Retrieved 2020-02-12, from https://adncuba.com/noticias-de-cuba/como-detectar-una-ciberclaria

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

Alba, D., & Frenkel, S. (2019). Russia tests new disinformation tactics in africa to expand influence. Retrieved 2020-10-30, from https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html

Albayrak, A., & Parkinson, J. (2013). Turkey's government forms 6,000-member social media team. Retrieved 2013-09-16, from https://www.wsj.com/articles/turkeys-government-forms-6000member-social-media-team-1379351399

Aleksejeva, N. (2019). Balticbrief: Sputnik takes aim at a Russian-speaking audience. Retrieved 2019-06-05, from https://medium.com/dfrlab/balticbrief-sputnik-takes-aim-at-a-russian-speaking-audience-6f7668e6cc23

Aleksejeva, N., Karan, K., Barojan, D., & Nimmo, B. (2019). Facebook's sputnik takedown — in depth. Retrieved 2019-01-17, from https://medium.com/dfrlab/facebooks-sputnik-takedown-in-depth-f417bed5b2f8

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

Allyn, B. (2020). Facebook And Twitter Remove Russia-Backed Accounts Targeting Left-Leaning Voters. Retrieved 2021-07-16, from https://www.npr.org/2020/09/01/908386613/facebook-and-twitter-remove-russia-backed-accounts-targeting-left-leaning-voters

Andriukaitis, L. (2019). Kremlin outlets downplay the size of the july 20 protests in moscow. Retrieved 2019-07-29, from https://medium.com/dfrlab/kremlin-outlets-downplay-the-size-of-the-july-20-protests-in-moscow-56a36aa5b9f5

Andrusieczko, P. (2019). Ukraine in the sights of Russian trolls and propagandists - soon presidential and then parliamentary elections. Retrieved 2019-01-20, from http://wyborcza.pl/7,75399,24353939,ukraina-na-celowniku-rosyjskich-trolli-i-propagandzistow-wkrotce.html

Applebaum, A. (2019). Want to build a far-right movement? spain's vox party shows how. Retrieved 2019-05-02, from https://www.washingtonpost.com/graphics/2019/opinions/spains-far-right-vox-party-shot-from-social-media-into-parliament-overnight-how/

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

Assenova, M. (2019). Russia: Non-information as disinformation. Retrieved 2019-08-14, from https://www.polygraph.info/a/russia-non-information-as-disinformation/30110010.html

Auchard, E., & Felix, B. (2017). French candidate macron claims massive hack as emails leaked. Retrieved 2019-06-05, from 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. Retrieved 2019-06-05, from 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. Retrieved 2019-03-21, from https://www.buzzfeed.com/jamesball/a-suspected-network-of-13000-twitter-bots-pumped-out-pro

Bandeira, L. (2019). Archimedes ran politically charged facebook ads in crisis-torn honduras. Retrieved 2019-07-02, from https://medium.com/dfrlab/archimedes-ran-politically-charged-facebook-ads-in-crisis-torn-honduras-1137f355e159

Bandeira, L., & Ponce de León, E. (2019). From telegram to Twitter: Top puerto rican officials plotted possible information operation. Retrieved 2019-07-29, from https://medium.com/dfrlab/from-telegram-to-twitter-top-puerto-rican-officials-plotted-possible-information-operation-a899a00e078e

BangkokPost. (2019). Facebook shows posts of banned accounts in thailand. Retrieved 2019-07-26, from https://www.bangkokpost.com/thailand/politics/1719415/facebook-shows-posts-of-banned-accounts-in-thailand

Bankauskaitė, D. (2019). Kremlin narratives for subversive activity in Lithuania‘s information space. Retrieved 2021-07-17, from https://medium.com/@hitthehybrid/kremlin-narratives-for-subversive-activity-in-lithuania-s-information-space-bd2b93b2cde8

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. Retrieved 2019-04-23, from https://medium.com/dfrlab/questionable-sources-on-syria-36fcabddc950

Barojan, D. (2018a). BalticBrief: NATO not planning to invade Belarus. Retrieved 2019-05-15, from https://medium.com/dfrlab/balticbrief-nato-not-planning-to-invade-belarus-d694d34f04ba

Barojan, D. (2018b). Electionwatch: Down ballot bots in mexico. Retrieved 2018-06-06, from https://medium.com/dfrlab/electionwatch-down-ballot-bots-in-mexico-e1bee023291d

Barojan, D. (2018c). SyriaHoax Part Two: Kremlin Targets White Helmets. Retrieved 2019-05-09, from https://medium.com/dfrlab/syriahoax-part-two-kremlin-targets-white-helmets-c6ab692d4a21

Barojan, D. (2018d). Troll tracker: Pro-kremlin trolls deployed ahead of syria strikes. Retrieved 2019-03-21, from https://medium.com/dfrlab/trolltracker-pro-kremlin-trolls-deployed-ahead-of-syria-strikes-e49acc68c8ff

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

BBC. (2015). Ecuador president rafael correa's troll warfare. Retrieved 2015-01-30, from https://www.bbc.com/news/blogs-trending-31057933

BBC. (2017). Russia turns on morgan freeman over election 'war' video. Retrieved 2019-06-05, from https://www.bbc.com/news/world-europe-41348749

BBC. (2018a). Jessikka aro: Finn jailed over pro-russia hate campaign against journalist. Retrieved 2019-06-05, from https://www.bbc.com/news/world-europe-45902496

BBC. (2018b). Syria war: What we know about douma 'chemical attack'. Retrieved 2019-06-05, from https://www.bbc.com/news/world-middle-east-43697084

BBC. (2019a). Highlights from central asian press, websites 16 aug 19. Retrieved 2019-08-16, from https://advance-lexis-com.ezproxy.princeton.edu/api/document?collection=news&id=urn:contentItem:5WTX-5681-DYRV-33VJ-00000-00&context=1516831

BBC. (2019b). Twitter removes Iranian-backed accounts. Retrieved 2019-06-14, from https://www.bbc.com/news/technology-48635878

Beaton, A., & Simon, S. (2018). Russian trolls tried to influence debate over nfl players kneeling during anthem. Retrieved 2019-05-01, from https://www.npr.org/2018/10/27/661313336/russian-trolls-tried-to-influence-debate-over-nfl-players-kneeling-during-anthem

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

Bell, C. (2018). The people who think 9/11 may have been an 'inside job. Retrieved 2019-06-05, from https://www.bbc.com/news/blogs-trending-42195513

Bellingcat. (2016). Behind the dutch terror threat video: The st. petersburg "troll factory" connection. Retrieved 2019-05-13, from 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. Retrieved 2019-06-05, from https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets/

Belsat. (2018). Top 5 fake stories about belarus spread by Russian media. Retrieved 2019-03-21, from 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. Retrieved 2019-06-05, from https://www1.folha.uol.com.br/internacional/en/world/2018/10/russian-hackers-are-trying-to-interfere-in-brazilian-elections-cybersecurity-firm-says.shtml

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

Bertrand, N. (2016). It looks like Russia hired internet trolls to pose as pro-Trump americans. Retrieved 2019-05-11, from https://www.businessinsider.com/russia-internet-trolls-and-donald-{T}rump-2016-7

Blacktivist. (2016). Republican investigation links Russian trolls to nodapl movement. Retrieved 2019-04-23, from https://www.indianz.com/News/2018/03/01/republican-investigation-links-russian-t.asp

Blanco, P. (2019). Así arruinaron los 'trolls' rusos la vida de jessikka aro. Retrieved 2019-05-08, from https://elpais.com/internacional/2017/12/07/actualidad/1512655209-165226

Boatwright, B. C., Linvill, D. L., & Warren, P. L. (2018). Troll factories: The Internet Research Agency and state-sponsored agenda building. *Resource Centre on Media Freedom in Europe*, 29.

Bogle, A. (2019). Twitter cracking down on political posts ahead of australian election. Retrieved 2019-06-08, from https://www.abc.net.au/radio/programs/am/twitter-cracks-down-on-political-posts-ahead-of-election/10828096

Boylan, D. (2018). Fake news: Iranian propaganda reports of death of saudi crown prince spark conspiracy theories. Retrieved 2019-05-01, from https://www.washingtontimes.com/news/2018/may/29/iran-propaganda-reports-mohammed-bin-salman-death-/

Brattberg, E., & Maurer, T. (2018). How sweden is preparing for Russia to hack its election. Retrieved 2019-05-13, from https://www.bbc.com/news/world-44070469

Brattnerg, E., & Maurer, T. (2018). Russian election interference: Europe's counter to fake news and cyber attacks. Retrieved 2019-03-20, from 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. Retrieved 2019-06-05, from https://www.forbes.com/sites/thomasbrewster/2017/05/08/macron-emails-leaked-and-russia-is-the-chief-suspect/#6ec43ef168f4

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

Burgess, M. (2017). Here's the first evidence Russia used Twitter to influence brexit. Retrieved 2019-03-21, from https://www.wired.co.uk/article/brexit-russia-influence-twitter-bots-internet-research-agency

Burke, J., & Harding, L. (2019). Documents suggest Russian plan to sway south africa election. Retrieved 2019-05-08, from https://www.theguardian.com/world/2019/may/08/documents-suggest-russian-plan-to-sway-south-africa-election

BusinessTech. (2019). Documents show alleged Russian plot to interfere in south african elections: report. Retrieved 2019-05-09, from https://businesstech.co.za/news/government/315678/documents-show-alleged-russian-plot-to-interfere-in-south-african-elections-report/

Cain, G. (2013). If you think the NSA is bad ... Retrieved 2021-07-17, from https://www.cnbc.com/id/100898207

Carvin, A., & Kassab, M. (2019). Libyan hashtag campaign has broader designs: Trolling qatar. Retrieved 2019-07-31, from https://medium.com/dfrlab/libyan-hashtag-campaign-has-broader-designs-trolling-qatar-8b2ba69c7334

Chappelle, A. (2018). Twitter bots, fake news and propaganda in the qatar crisis. Retrieved 2018-06-04, from https://www.aljazeera.com/news/2018/06/twitter-bots-fake-news-propaganda-qatar-crisis-180604134035342.html

Chee, F. Y., & Paul, K. (2019). Twitter suspends saudi royal adviser qahtani, fake gulf accounts. Retrieved 2019-09-20, from https://www.reuters.com/article/us-twitter-saudi/twitter-suspends-saudi-royal-adviser-qahtani-fake-gulf-accounts-idUSKBN1W50O0

Chen, A. (2015). The Agency. Retrieved 2015-06-02, from https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Chizhova, L. (2017). 'living bots': How moscow's mayor uses stealth to shape public opinion. Retrieved 2017-05-23, from https://www.rferl.org/a/moscow-mayor-sobyanin-mobilizing-influencers-stealth-campaign-bots-khrushchyovki/28504056.html

Chulov, M. (2017). Sarin used in april syria attack, chemical weapons watchdog confirms. Retrieved 2019-06-05, from https://www.theguardian.com/world/2017/jun/30/sarin-was-used-in-syria-khan-sheikhun-attack-says-chemical-weapons-watchdog

Clifton, D. (2017). Russian propagandists are pushing for roy moore to win. Retrieved 2019-05-15, from https://www.motherjones.com/politics/2017/12/russian-propagandists-are-pushing-for-roy-moore-to-win/

Cohen, Z., & Herb, J. (2021). Intelligence report contradicts claims by Trump and his team on China election interference. Retrieved 2021-07-17, from https://edition.cnn.com/2021/03/17/politics/us-intel-report-trump-china-election-interference-claims/

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. Retrieved 2019-05-01, from https://sentinel.tw/china-disinformation-tw/

Collins, B., & Wodinsky, S. (2018). Twitter pulls down bot network that pushed pro-saudi talking points about disappeared journalist. Retrieved 2019-05-15, from https://www.nbcnews.com/tech/tech-news/exclusive-twitter-pulls-down-bot-network-pushing-pro-saudi-talking-n921871

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

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

CPJ. (2019). Tajik authorities harass journalist humayra bakhtiyar and family. Retrieved 2019-07-18, from https://cpj.org/2019/07/tajik-authorities-harass-journalist-humayra-bakhti/

Crime and Security Research Institute. (2021). *Hundreds of Fake Twitter Accounts Linked to China Sowed Disinformation Prior to the US Election, With Some Continuing To Amplify Reactions to the Capitol Building Riot* (Tech. Rep.). Retrieved from https://crimeandsecurity.org/feed/china-linked-io-us-2020

Cryst, E. (2020). *Stoking Conflict by Keystroke* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/news/africa-takedown-december-2020

Cryst, E., & García-Camargo, I. (2020). *An analysis of Twitter's takedown of honduran accounts* (Tech. Rep.). Retrieved from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/04022020-hondurastakedown.pdf

Cryst, E., & Perkins, S. (2020). *DeZurdaTeam: A Twitter network promotes pro-Cuba hashtags* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/news/twitter-takedown-october-2020

Daniels, L. (2016). Rise of the peñabots. Retrieved 2016-02-24, from https://points.datasociety.net/rise-of-the-pe%C3%B1abots-d35f9fe12d67

Dave, P., & Bing, C. (2018). Facebook, Twitter dismantle disinformation campaigns tied to iran and Russia. Retrieved 2019-03-22, from https://www.reuters.com/article/us-facebook-russia-usa/facebook-twitter-remove-pages-promoting-iranian-propaganda-idUSKCN1L62FD

de Haldevang, M. (2018). Russian trolls and bots are flooding Twitter with Ford-Kavanaugh disinformation. Retrieved 2020-07-09, from https://qz.com/1409102/russian-trolls-and-bots-are-flooding-twitter-with-ford-kavanaugh-disinformation/

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

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

Dick, S. (2018). Fake pro-independence facebook page that originated in iran is taken down. Retrieved 2019-03-21, from https://www.heraldscotland.com/news/16592877.fake-pro-independence-facebook-page-that-originated-in-iran-is-taken-down/

di Giovanni, J. (2017). Why assad and Russia target the white helmets. Retrieved 2019-06-05, from https://www.nybooks.com/daily/2018/10/16/why-assad-and-russia-target-the-white-helmets/

DiResta, R., Goldstein, J. A., Miller, C., Wang, H., & SY, M. (2021). *One topic, two networks: Evaluating two Chinese influence operations on Twitter related to Xinjiang* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/news/twitter-takedown-december-2021

DiResta, R., & Grossman, S. (2019). *Potemkin Pages Personas: Assessing GRU Online Operations, 2014-2019* (Tech. Rep.). Retrieved from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf

DiResta, R., Grossman, S., K.H., & Miller, C. (2019). *Analysis of Twitter takedown of state-backed operation attributed to saudi arabian digital marketing firm smaat* (Tech. Rep.). Retrieved from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20191223_smaat.pdf

DiResta, R., Shaffer, D., Ruppel, B., Sullivan, D., Matney, R., Fox, R., ... Johnson, B. (2019). The tactics & tropes of the Internet Research Agency.

Di Stefano, M. (2018). Here's the woman behind britain's most divisive Twitter account. Retrieved 2019-06-04, from https://www.buzzfeed.com/markdistefano/heres-the-woman-behind-britains-most-divisive-twitter

Díaz, I. (2017). Venezuela and Russia teamed up to push pro-catalan fake news. Retrieved 2017-11-28, from https://www.thedailybeast.com/why-is-venezuela-waging-cyber-war-in-europe

El Universo. (2014). Compañía ximah creó en facebook cuenta crítica a oposición en ecuador. Retrieved 2015-09-08, from https://www.eluniverso.com/noticias/2014/09/08/nota/3774286/ximah-creo-facebook-cuenta-critica-oposicion

Elliot, H. (2018). Twitter reportedly suspends network of bots pushing pro-Saudi disinformation on suspected Khashoggi murder. Retrieved 2019-05-15, from 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. Retrieved 2019-05-11, from https://www.reuters.com/article/us-spain-politics-catalonia-russia/spain-sees-russian-interference-in-catalonia-separatist-vote-idUSKBN1DD20Y

Eurasianet. (2020). Tajikistan's nonchalance on coronavirus shows cracks. Retrieved 2020-04-06, from https://eurasianet.org/tajikistans-nonchalance-on-coronavirus-shows-cracks

EUvsDisinfo. (2019a). The journalists who exist only on paper. Retrieved 2019-07-15, from https://euvsdisinfo.eu/the-journalists-who-exist-only-on-paper/

EUvsDisinfo. (2019b). Results of 2018 "EU versus disinformation" screening: Ukraine remains under fire through disinformation. Retrieved 2019-05-06, from https://www.euneighbours.eu/en/east/stay-informed/news/results-2018-eu-versus-disinformation-screening-ukraine-remains-under-fire

Evanina, William. (2021). *Statement by NCSC Director William Evanina: Election Threat Update for the American Public* (Tech. Rep.). Retrieved from https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public

Facebook. (2020a). April 2020 Coordinated Inauthentic Behavior Report. Retrieved 2021-07-17, from https://about.fb.com/news/2020/05/april-cib-report/

Facebook. (2020b). August 2020 Coordinated Inauthentic Behavior Report. Retrieved 2021-07-17, from https://about.fb.com/news/2020/09/august-2020-cib-report/

Facebook. (2020c). October 2020 Coordinated Inauthentic Behavior Report. Retrieved 2021-07-17, from https://about.fb.com/news/2020/11/october-2020-cib-report/

Facebook. (2021). May 2021 coordinated inauthentic behavior report. Retrieved from https://about.fb.com/wp-content/uploads/2021/06/May-2021-CIB-Report.pdf

Farchy, J. (2016). Putin names nato among threats in new Russian security strategy. Retrieved 2019-06-05, from 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. Retrieved 2019-03-21, from https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/

Freedom House. (2019). Freedom of the net 2019: Sudan. Retrieved from https://freedomhouse.org/country/sudan/freedom-net/2019

FreedomHouse. (2014). Freedom on the net 2014. Retrieved from https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf

Frenkel, S., & Wakabayashi, D. (2018). After florida school shooting, Russian 'bot' army pounced. Retrieved 2019-05-01, from https://www.nytimes.com/2018/02/19/technology/russian-bots-school-shooting.html

Friedersdorf, C. (2017). Is Russia behind a secession effort in California? Retrieved 2019-04-23, from https://www.theatlantic.com/politics/archive/2017/03/is-russia-behind-a-secession-effort-in-california/517890/

FSI. (2019). Libya: Presidential and parliamentary elections scene setter. Retrieved 2019-10-02, from https://cyber.fsi.stanford.edu/io/news/libya-scene-setter

Fubini, F. (2018). Tweet populisti dalla Russia sulla politica italiana. come negli usa. Retrieved 2019-06-05, from https://www.corriere.it/politica/18_agosto_01/tweet-populisti-russia-voto-italiano-come-usa-f33df26c-95cc-11e8-819d-89f988769835.shtml

Fundación Mil Hojas. (2015). Troll center: derroche y acoso desde las redes sociales. Retrieved 2015-03-24, from http://milhojas.is/cms-front-noticias.php?id=612261

Furlong, A. (2019). Labour: Dossier indicates nhs 'up for sale' in us trade deal. Retrieved 2019-11-27, from https://www.politico.eu/article/labour-dossier-indicates-nhs-up-for-sale-in-us-trade-deal/

Gallagher, E. (2017). Mexican media botnet study. Retrieved 2019-01-04, from https://medium.com/@erin_gallagher/mexican-media-botnet-study-21c78a1664c3

Gallagher, E. (2019). Mexico: Coordinated inauthentic behavior on facebook and Twitter. Retrieved 2019-01-24, from https://medium.com/@erin_gallagher/mexico-coordinated-inauthentic-behavior-on-facebook-twitter-a670280d02fc

Gelava, S., & Buziashvili, E. (2020). Georgian far-right and pro-government actors collaborate in inauthentic facebook network. Retrieved 2021-07-16, from https://medium.com/dfrlab/georgian-far-right-and-pro-government-actors-collaborate-in-inauthentic-facebook-network-730b9593a729

Gigitashvili, G. (2020). Anonymous Facebook pages intensified negative posts ahead of Georgian parliamentary elections. Retrieved 2021-07-16, from https://medium.com/dfrlab/anonymous-facebook-pages-intensified-negative-posts-ahead-of-georgian-parliamentary-elections-f85b0f898a5e

Gleicher, N. (2018a). Coordinated inauthentic behavior explained. Retrieved 2019-06-05, from https://newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

Gleicher, N. (2018b). More information about last week's takedowns. Retrieved 2019-05-15, from https://newsroom.fb.com/news/2018/11/last-weeks-takedowns/

Gleicher, N. (2018c). What we've found so far. Retrieved 2019-06-05, from https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/

Gleicher, N. (2019a). Removing coordinated inauthentic behavior and spam from India and Pakistan. Retrieved 2019-04-01, from https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/

Gleicher, N. (2019b). Removing coordinated inauthentic behavior from Russia. Retrieved 2019-01-17, from https://about.fb.com/news/2019/01/removing-cib-from-russia/

Gleicher, N. (2019c). Removing coordinated inauthentic behavior in thailand, Russia, Ukraine and Honduras. Retrieved 2019-07-25, from https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/

Gleicher, N. (2019d). Removing coordinated inauthentic behavior in UAE, Egypt and Saudi Arabia. Retrieved 2019-08-01, from https://about.fb.com/news/2019/08/cib-uae-egypt-saudi-arabia/

Gleicher, N. (2019e). Removing coordinated inauthentic behavior in UAE, Nigeria, Indonesia and Egypt. Retrieved 2019-10-03, from https://about.fb.com/news/2019/10/removing-coordinated-inauthentic-behavior-in-uae-nigeria-indonesia-and-egypt/

Gleicher, N. (2019f). Removing more coordinated inauthentic behavior from Iran. Retrieved 2019-05-28, from https://about.fb.com/news/2019/05/removing-more-cib-from-iran/

Gleicher, N. (2019g). Taking down more coordinated inauthentic behavior in myanmar. Retrieved 2019-08-21, from https://about.fb.com/news/2019/08/more-cib-myanmar/

Gleicher, N. (2020a). Removing Coordinated Inauthentic Behavior Azerbaijan. Retrieved 2021-07-16, from https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-september-report/

Gleicher, N. (2020b). Removing Coordinated Inauthentic Behavior from Philippines. Retrieved 2021-07-17, from https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-china-philippines/

Gleicher, N. (2020c). *Removing Coordinated Inauthentic Behavior from Russia* (Tech. Rep.). Retrieved 2021-07-17, from https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/

Gleicher, N., & Agranovich, D. (2020). Removing coordinated inauthentic behavior from France and Russia. Retrieved 2021-07-17, from https://about.fb.com/news/2020/12/removing-coordinated-inauthentic-behavior-france-russia/

Goble, P. (2019). Belarus already under Russian troll attack designed to give moscow a base for further aggression. Retrieved 2019-03-21, from http://euromaidanpress.com/2019/01/02/belarus-already-under-russian-troll-attack-designed-to-give-moscow-a-base-for-further-aggression/

Goldstein, J. A., & Hundley, L. (2021). *Viva la #Resistance? Now-Suspended Twitter Accounts from Iran Claim #Resistance Personas in US Politics and Middle Eastern Affairs* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/publication/viva-la-resistance-now-suspended-twitter-accounts-iran-claim-resistance-personas-us

Goldstein, J. A., Sinpeng, A., Bush, D., Ewald, R., John, J., & Thiel, D. (2020). *Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/publication/cheerleading-without-fans-low-impact-domestic-information-operation-royal-thai-army

Gomez, L. (2017). A Russian Twitter bot promoted California secession, or calexit. Retrieved 2019-04-23, from https://www.sandiegouniontribune.com/opinion/the-conversation/sd-russian-bot-pushed-calexit-movement-20171102-htmlstory.html

González, O. (2019). "Ciberclarias", un ejército que invade las redes sociales con cuentas falsas. Retrieved 2019-05-21, from https://www.cubanet.org/destacados/ciberclarias-un-ejercito-que-invade-las-redes-sociales-con-cuentas-falsas/

Gordon, G. (2018). Fake, misleading social media posts exploding globally, oxford study finds. Retrieved 2019-03-19, from https://www.mcclatchydc.com/news/nation-world/national/national-security/article215188910.html

Graphika, & Stanford Internet Observatory. (2020). *More-Troll Kombat* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_stanford_report_more_troll_kombat.pdf

Graphika Team. (2020). *Step into My Parler* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_report_step_into_my_parler.pdf

Greenberg, A. (2020). If Russia Hacked Burisma, Brace for the Leaks to Follow. Retrieved 2021-07-16, from https://www.wired.com/story/russia-burisma-hack-leaks/

Griffin, A. (2015). Angela merkel's instagram bombarded with abuse from Russian troll army. Retrieved 2019-03-20, from https://www.independent.co.uk/life-style/gadgets-and-tech/news/angela-merkels-instagram-bombarded-with-abuse-from-russian-troll-army-10303425.html

Griffin, T. (2018). Zimbabwe's opposition leader accused the ruling party of hiring "fake news mercenaries". Retrieved 2018-07-25, from https://www.buzzfeednews.com/article/tamerragriffin/zimbabwe-fake-news

Grossman, S., Bush, D., & DiResta, R. (2019). *Evidence of Russia-linked influence operations in Africa* (Tech. Rep.).

Grossman, S., H., K., & DiResta, R. (2020). Blurring the lines of media authenticity: Prigozhin-linked group funding Libyan broadcast media. *Stanford Internet Observatory*.

Grossman, S., H., K., DiResta, R., Kheradpir, T., & Miller, C. (2020). Blame it on iran, qatar, and turkey: An analysis of a Twitter and facebook operation linked to egypt, the uae, and saudi arabia. Retrieved 2020-04-02, from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20200402_blame_it_on_iran_qatar_and_turkey_v2_0.pdf

Grossman, S., Jonsson, K., Lyon, N., & Sizer, L. (2020). *Slanted Narratives, Social Media, and Foreign Influence in Libya* (Tech. Rep.). Retrieved from https://cyber.fsi.stanford.edu/io/news/social-media-foreign-influence-libya

Grossman, S., Khadija, H., Ross, E., & Thiel, D. (2020). *Royal Sockpuppets and Handle Switching: How a Saudi Arabia-Linked Twitter Network Stoked Rumors of a Coup in Qatar* (Tech. Rep.). Retrieved from https://fsi.stanford.edu/publication/royal-sockpuppets-and-handle-switching-how-saudi-arabia-linked-twitter-network-stoked

Guynn, J. (2018a). Facebook foils political influence campaigns originating in iran, Russia ahead of u.s. midterms. Retrieved 2019-03-22, from https://www.usatoday.com/story/tech/2018/08/21/facebook-foils-political-influence-campaigns-originating-iran-russia-ahead-u-s-midterms/1058233002/

Guynn, J. (2018b). These are the liberal memes Iran used to target Americans on Facebook. Retrieved 2019-03-21, from https://www.usatoday.com/story/tech/news/2018/08/24/how-iran-targeted-u-s-facebook-youtube-and-twitter-liberal-memes/1079882002/

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

Harris, S., Nakashima, E., Miller, G., & Dawsey, J. (2020). White House was warned Giuliani was target of Russian intelligence operation to feed misinformation to Trump. Retrieved 2021-07-16, from https://www.washingtonpost.com/national-security/giuliani-biden-ukraine-russian-disinformation/2020/10/15/43158900-0ef5-11eb-b1e8-16b59b92b36d_story.html

Henley, J. (2017). Russia waging information war against sweden, study finds. Retrieved 2019-05-13, from 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. Retrieved 2019-03-21, from 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. Retrieved 2019-05-01, from https://www.theguardian.com/technology/2018/oct/17/vast-archive-of-tweets-reveals-work-of-trolls-backed-by-russia-and-iran

Heydarian, R. (2020). Philippines versus Facebook brawl exposes China's sharp power. Retrieved 2021-07-17, from https://asia.nikkei.com/Opinion/Philippines-versus-Facebook-brawl-exposes-China-s-sharp-power

Higgins, A. (2018). Three internet trolls convicted of systematic defamation against journalist in finland. Retrieved 2019-06-05, from 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. Retrieved 2019-05-07, from 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. Retrieved 2019-05-14, from https://assets.documentcloud.org/documents/5011321/Khusyaynova-Complaint.pdf

Hookway, J. (2017). Introducing force 47, vietnam's new weapon against online dissent. Retrieved 2017-12-31, from https://www.wsj.com/articles/introducing-force-47-vietnams-new-weapon-against-online-dissent-1514721606

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2019). *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. Retrieved 2019-03-22, from 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. Retrieved 2019-06-05, from https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html

Jazeera, A. (2017). Syria forces behind khan sheikhoun gas attack: Un probe. Retrieved 2019-06-05, from https://www.aljazeera.com/news/2017/09/syria-forces-khan-sheikhoun-gas-attack-probe-170906115601017.html

Jindia, S., Graphika, & The Syria Campaign. (2017). *Killing the truth: How Russia is fuelling a disinformation campaign to cover up war crimes in Syria* (Tech. Rep.). The Syria Campaign.

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

Jones, M. O. (2020). Anatomy of a disinformation campaign: The coup that never was. Retrieved 2021-07-17, from https://www.aljazeera.com/features/2020/5/19/anatomy-of-a-disinformation-campaign-the-coup-that-never-was

Kann, A., & Buziashvili, E. (2019). Facebook takes down pro-indonesian pages targeting west papua. Retrieved 2019-10-10, from https://medium.com/dfrlab/facebook-takes-down-pro-indonesian-pages-targeting-west-papua-3c8b56449bfd

Kao, J., & Li, M. S. (2020). How china built a Twitter propaganda machine then let it loose on coronavirus. Retrieved 2020-03-26, from https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus

Karan, K. (2019). Royally removed: Facebook takes down pages promoting saudi interests. Retrieved 2019-08-14, from https://medium.com/dfrlab/royally-removed-facebook-takes-down-pages-promoting-saudi-interests-edc0ce8b972a

Karan, K., Barojan, D., Hall, M., & Brookie, G. (2019). Trolltracker: Outward influence operation from iran. Retrieved 2019-05-09, from https://medium.com/dfrlab/trolltracker-outward-influence-operation-from-iran-cc4539684c8d

Karan, K., Kaul, A., & Nimmo, B. (2019). Facebook removes iran-based assets. again. Retrieved 2019-05-30, from https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-f17358ef21f

Karan, K., Osadchuk, R., Gigitashvili, G., Ponce de León, E., & Le Roux, J. (2020). Facebook removes Russian propaganda outlet in Ukraine. Retrieved 2021-07-17, from https://medium.com/dfrlab/facebook-removes-propaganda-outlets-linked-to-russian-security-services-51fbe2f6b841

Karan, K., Peñarredonda, J. L., & Bandeira, L. (2019). Trolltracker: Venezuelan government-linked influence campaign on Twitter. Retrieved 2019-03-13, from https://medium.com/dfrlab/trolltracker-venezuelan-government-linked-influence-campaign-on-twitter-63a8fe7a62e0

Karan, K., Rizzuto, M., & Kann, A. (2019). Uae facebook pages targeted qatar and muslim brotherhood. Retrieved 2019-10-15, from https://medium.com/dfrlab/uae-facebook-pages-targeted-qatar-and-muslim-brotherhood-8aec916fa1f7

Karan, K., & Zhang, P. (2019). Twitter's hong kong archives: Chinese commercial bots at work. Retrieved 2019-09-04, from https://medium.com/dfrlab/twitters-hong-kong-archives-chinese-commercial-bots-at-work-f4c7ae8eea64

Karp, P. (2018). Russian Twitter trolls stoking anti-Islamic sentiment in Australia, experts warn. Retrieved 2019-03-19, from https://www.theguardian.com/australia-news/2018/nov/20/russian-twitter-trolls-stoking-anti-islamic-sentiment-in-australia-experts-warn

Kassab, M., & Carvin, A. (2019). A Twitter hashtag campaign in libya: How jingoism went viral. Retrieved 2019-06-06, from https://medium.com/dfrlab/a-twitter-hashtag-campaign-in-libya-part-1-how-jingoism-went-viral-43d3812e8d3f

Keeley, G. (2018). Russia meddled in catalonia independence referendum, says german intelligence boss. Retrieved 2019-05-11, from https://www.thetimes.co.uk/article/russia-meddled-in-catalonia-vote-p6g5nttpm

Keller, F. B., Schoch, D., Stier, S., & Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, *37*(2), 256-280. doi: 10.1080/10584609.2019.1661888

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

Khana, C. (2017). Bots, blockades and blackouts: how armenia media copes. Retrieved 2019-06-22, from https://oc-media.org/features/bots-blockades-and-blackouts-how-armenia-media-copes/

Kharazian, Z., & Knight, T. (2020). Facebook removes inauthentic assets linked to the Philippine military. Retrieved 2021-07-17, from https://medium.com/dfrlab/facebook-removes-inauthentic-assets-linked-to-the-philippine-military-b61f9a38cb4a

Kist, R. (2018). The fight against the trolls hardens. Retrieved 2019-05-31, from 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. Retrieved 2019-05-31, from 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. Retrieved 2019-05-31, from https://www.thedailybeast.com/mh17-russia-deployed-its-trolls-to-cover-up-the-murder-of-298-people

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

Kroet, C. (2017). Russian fake news campaign targets merkel in german election. Retrieved 2019-03-20, from https://www.politico.eu/article/russian-fake-news-campaign-targets-merkel-in-german-election/

Kuczynski, G. (2019). *Nato-russia relations: The return of the enemy* (Tech. Rep.).

Kurlantzick, J. (2019). How China Is Interfering in Taiwan's Election. Retrieved 2021-07-17, from https://www.cfr.org/in-brief/how-china-interfering-taiwans-election

Lake, E. (2018). Iran's fake news is a fake threat. Retrieved 2019-05-01, from https://www.bloomberg.com/opinion/articles/2018-08-31/iran-s-fake-news-is-not-a-real-threat

Lee, L. M.-C., Tseng, P.-Y., Kao, S.-S. W., Wu, M.-H., & Shen, P. (2020). Deafening Whispers – China's Information Operation and Taiwan's 2020 Election. Retrieved from https://medium.com/doublethinklab/deafening-whispers-f9b1d773f6cd

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

Li, J. (2019). China's Twitter operation focused on this exiled tycoon before hong kong protests. Retrieved 2019-09-02, from https://qz.com/1700575/the-people-china-linked-twitter-accounts-aimed-at-before-hong-kong/

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

Lister, T., & Shukla, S. (2019). Russian mercenaries fight shadowy battle in gas-rich mozambique. Retrieved 2019-11-29, from https://www.cnn.com/2019/11/29/africa/russian-mercenaries-mozambique-intl/index.html

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

Ljubas, Z. (2020). Twitter axes 20,000 government-linked accounts, most from serbia. Retrieved 2020-04-04, from https://www.occrp.org/en/daily/12004-twitter-axes-20-000-government-linked-accounts-most-from-serbia

Lytvynenko, J., & McDonald, L. (2019). Hundreds of propaganda accounts targeting iran and qatar have been removed from facebook. Retrieved 2019-09-03, from https://www.buzzfeednews.com/article/janelytvynenko/uae-propaganda

Mac, R., & Adams, R. (2019). Have you seen these ads about hong kong's protests? China certainly hopes you have. Retrieved 2019-08-19, from https://www.buzzfeednews.com/article/ryanmac/hong-kong-protests-violent-facebook-twitter-ads-china-state

MacFarquhar, N. (2018). Inside the russian troll factory: Zombies and a breakneck pace. Retrieved 2019-03-19, from https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html

Mackinnon, A. (2017). Manipulating elections via Twitter in armenia. Retrieved 2019-04-06, from https://www.codastory.com/disinformation/in-armenia-a-snapshot-of-digital-manipulation-ahead-of-the-election/

Mak, T. (2018). Russia's divisive Twitter campaign took a rare consistent stance: Pro-gun. Retrieved 2019-05-01, from https://www.npr.org/2018/09/21/648803459/russias-2016-twitter-campaign-was-strongly-pro-gun-with-echoes-of-the-nra

Mak, T. (2020). How Russia Is Trying To Boost Bernie Sanders' Campaign. Retrieved 2021-07-16, from https://www.npr.org/2020/03/05/812186614/how-russia-is-trying-to-boost-bernie-sanders-campaign

Marshall, M. G., Gurr, T. R., & Jaggers, K. (2019). Political regime characteristics and transitions, 1800-2018. *Polity IV Project: Home Page*, *17*.

Mason, M. (2018). Intelligence officials plan to repel fake news in australian federal election. Retrieved 2019-06-05, from 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. Retrieved 2019-04-23, from https://www.newsweek.com/brett-kavanaugh-has-huge-opposition-us-russian-state-propaganda-loves-donald-1155046

Mele, C. (2017). Morgan freeman angers Russians over video about 2016 election. Retrieved 2019-06-05, from https://www.nytimes.com/2017/09/22/world/europe/morgan-freeman-russia-video.html

Michel, C. (2018). It turns out Russia is not the only country turning facebook and Twitter against us. Retrieved 2019-05-06, from 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. Retrieved 2019-04-21, from https://www.reuters.com/article/us-france-russia-idUSKBN18P030

Mohan, M. (2017). Macron leaks: the anatomy of a hack. Retrieved 2019-06-05, from https://www.bbc.com/news/blogs-trending-39845105

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

Monaco, N., Smith, M., & Studdart, A. (2020). *Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan* (Tech. Rep.).

Morales, J. . (2020). Perceived popularity and online discourse: Evidence from Twitter in Venezuela. *International Journal of Press/Politics*, *25*(1), 5–27.

Morla, R. (2015). Correa's social-media troll center exposed in quito. Retrieved 2015-03-26, from https://panampost.com/rebeca-morla/2015/03/25/correas-social-media-troll-center-exposed-in-quito/

Moyo, D. (2018). A vicious online propaganda war that includes fake news is being waged in zimbabwe. Retrieved 2018-07-24, from https://theconversation.com/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-99402

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

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

Muller, R. (2018). Conspiracy to commit an offense against the United States. Retrieved from https://www.justice.gov/storage/report.pdf

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

Nassetta, J., & Fecht, E. (2018). *All the world is staged: An analysis of social media influence operations against us counterproliferation efforts in Syria* (Tech. Rep.). Middlebury Institute of International Studies at Monterey.

National Intelligence Council. (2021). *Foreign Threats to the US Federal Elections* (Tech. Rep.). Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

Neuman, S. (2018). Russia's 'fancy bear' reportedly hacks german government network. Retrieved 2019-03-20, from https://www.npr.org/sections/thetwo-way/2018/03/01/589787931/russias-fancy-bear-reportedly-hacks-german-government-networks

News. (2018). Russian 'troll factory' tweets tried to influence italian voters. Retrieved 2019-05-15, from https://www.thelocal.it/20180802/russian-troll-factory-tweets-attempted-influence-italian-elections

Nimmo, B. (2018a). Iran is suspected information operation. assessing the main pages and accounts traced to tehran by fireeye. Retrieved 2019-03-18, from https://medium.com/dfrlab/trolltracker-irans-suspected-information-operation-153fc7b60126

Nimmo, B. (2018b). Putinatwar: Trolls on Twitter. Retrieved 2019-05-014, from https://medium.com/dfrlab/putinatwar-trolls-on-twitter-5d0bb3dc30ae

Nimmo, B. (2018c). Robot wars: How bots joined battle in the gulf. *Journal of International Affairs*, *71*(1.5), 87–96.

Nimmo, B. (2018d). Russia is full spectrum propaganda. Retrieved 2019-03-19, from https://medium.com/dfrlab/russias-full-spectrum-propaganda-9436a246e970

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

Nimmo, B., & Barojan, D. (2017). Fakes, bots, and blockings in armenia. Retrieved 2019-04-01, from https://medium.com/dfrlab/fakes-bots-and-blockings-in-armenia-44a4c87ebc46

Nimmo, B., Barojan, D., Peñarredonda, J. L., & Karan, K. (2018). Electionwatch: Trending beyond borders in mexico. Retrieved 2018-06-28, from https://medium.com/dfrlab/electionwatch-trending-beyond-borders-in-mexico-2a195ecc78f4

Nimmo, B., & Brookie, G. (2018). Trolltracker: Facebook uncovers Iranian influence operation Iranian narratives buried in divisive content target United States and United Kingdom. Retrieved 2019-03-21, from 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. Retrieved 2019-03-22, from 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. Retrieved 2019-03-21, from https://medium.com/dfrlab/trolltracker-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. Retrieved 2019-03-22, from https://medium.com/dfrlab/trolltracker-twitters-troll-farm-archives-8be6dd793eb2

Nimmo, B., Eib, C. S., & Ronzaud, L. (2020). Operation Naval Gazing. *Graphika*.

Nimmo, B., Eib, C. S., & Tamora, L. (2019). Cross-Platform Spam Network Targeted Hong Kong Protests. *Graphika*.

Nimmo, B., & Francois, C. (2018). Trolltracker: Glimpse into a french operation. Retrieved 2019-05-15, from https://medium.com/dfrlab/trolltracker-glimpse-into-a-french-operation-f78dcae78924

Nimmo, B., Francois, C., Eib, C. S., & Ronzaud, L. (2020a). *IRA Again: Unlucky Thirteen* (Tech. Rep.).

Nimmo, B., Francois, C., Eib, C. S., & Ronzaud, L. (2020b). Return of the (spamouflage) dragon. *Graphika*.

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

Nimmo, B., François, C., Eib, C. S., & Ronzaud, L. (2020). Spamouflage Goes to America. *Graphika*. Retrieved from https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf

Nimmo, B., François, C., Eib, C. S., Ronzaud, L., & Carter, J. (2020). *GRU and the Minions* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_report_gru_minions.pdf

Nimmo, B., François, C., Eib, C. S., Ronzaud, L., Smith, M., Lederer, T., ... McAweeney, E. (2020). *IRA in Ghana: Double Deceit* (Tech. Rep.). Retrieved from https://graphika.com/reports/ira-in-ghana-double-deceit/

Nimmo, B., & Karan, K. (2018). Trolltracker: Favorite Russian troll farm sources. measuring the websites and accounts the internet research agency shared most. Retrieved 2019-03-22, from https://medium.com/dfrlab/trolltracker-favorite-russian-troll-farm-sources-48dc00cdeff

Nimmo, B., & Karan, K. (2019). Pakistan army's covert social network. Retrieved 2019-04-01, from https://medium.com/dfrlab/pakistan-armys-covert-social-network-23ce90feb0d0

Nimmo, B., Ronzaud, L., Eib, C. S., & Ferreira, R. (2020). *Myanmar Military Network* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_report_myanmar_military_network.pdf

Nimmo, B., & Toler, A. (2018). The Russians who exposed Russia's trolls. Retrieved 2018-03-07, from https://medium.com/dfrlab/the-russians-who-exposed-russias-trolls-72db132e3cd1

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

NWS. (2018). Russian trolls active in belgium and the netherlands. Retrieved 2019-05-13, from 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. Retrieved 2019-05-13, from 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. Retrieved 2019-05-01, from https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/

Owens, J. (2018). Twitter cracking down on political posts ahead of australian election. Retrieved 2019-06-08, from https://www.theaustralian.com.au/national-affairs/foreign-affairs/russias-tweet-troll-factory-meddled-in-australian-politics/news-story/24674946dab18d03ec6055a675b66856

Pearce, K. (2014). Two can play at that game: Social media opportunities in Azerbaijan for government and opposition. *Demokratizatsiya*, *22*, 39-66.

Peinado, F. (2019). Una red de cuentas falsas de Twitter promueve a vox en campaña. Retrieved 2019-04-26, from https://elpais.com/politica/2019/04/25/actualidad/1556203502_359349.html

Peisakhin, L., & Rozenas, A. (2018). When does Russian propaganda work — and when does it backfire? Retrieved 2019-05-06, from 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. Retrieved 2019-05-01, from https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/

Perlroth, N., & Rosenberg, M. (2020). Russians Hacked Ukrainian Gas Company at Center of Impeachment. Retrieved 2021-07-16, from https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

Pertsev, A. (2018). Russian political consultants discover africa. Retrieved 2019-05-15, from https://www.kommersant.ru/doc/3607961

Petreski, V. (2018). Electionwatch: Fascist falsification ahead of macedonian referendum. Retrieved 2018-09-28, from https://medium.com/dfrlab/electionwatch-fascist-falsification-ahead-of-macedonian-referendum-77e9c15acdb7

Petreski, V., & Karan, K. (2019). Election watch: Macedonian memes, American midterms. Retrieved 2019-05-13, from https://medium.com/dfrlab/electionwatch-macedonian-memes-american-midterms-b1f35f9df2ee

Peñarredonda, J. L., & Karan, K. (2019). influenceforsale: Venezuela's Twitter propaganda mill. Retrieved 2019-02-03, from https://medium.com/dfrlab/influenceforsale-venezuelas-twitter-propaganda-mill-cd20ee4b33d8

Phuong, N. T. (2018). The truth about vietnam's new military cyber unit. Retrieved 2018-01-10, from https://thediplomat.com/2018/01/the-truth-about-vietnams-new-military-cyber-unit/

Pinnell, O. (2018). The online war between qatar and saudi arabia. Retrieved 2018-06-03, from https://www.bbc.com/news/blogs-trending-44294826

Ponce de León, E., & Pérez, D. S. (2020). Network of pro-maduro Twitter accounts pushed anti-guaidó hashtags. Retrieved 2020-01-14, from https://medium.com/dfrlab/network-of-pro-maduro-twitter-accounts-pushed-anti-guaid%C3%B3-hashtags-530f034f3628

Poulsen, K. (2018). Mueller finally solves mysteries about Russia's 'fancy bear' hackers. Retrieved 2019-05-15, from https://www.thedailybeast.com/mueller-finally-solves-mysteries-about-russias-fancy-bear-hackers

Poulsen, K. (2019). Accused Russian troll uses a novel argument to fire back at facebook. Retrieved 2019-07-30, from https://www.thedailybeast.com/accused-russian-troll-uses-a-novel-argument-to-fire-back-at-facebook

Poulsen, K., & Ackerman, S. (2018). The most shocking moments of the new Russia complaint, from 'Civil War' to 'Fake' Rubio to 'Colored LGBT'. Retrieved 2019-05-03, from 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. Retrieved 2019-05-11, from https://www.thedailybeast.com/russians-appear-to-use-facebook-to-push-pro-{T}rump-flash-mobs-in-florida

Prentis, J. (2018). Facebook and Twitter say iran propaganda pages deleted. Retrieved 2019-05-01, from https://www.thenational.ae/world/mena/facebook-and-twitter-say-iran-propaganda-pages-deleted-1.762801

Price, R. (2018). Facebook says iran-backed accounts pretended to be news organizations to spread information and to launch cyber attacks. Retrieved 2019-06-05, from https://www.businessinsider.sg/facebook-detects-information-campaigns-russia-iran-2018-8/

Radio, S. (2016). Russia's propaganda efforts underscored in sapo report. Retrieved 2019-05-13, from https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6391875

RadioTelevisionMartí. (2020). "me enfurece" y "contenidos emocionales": las presuntas instrucciones a las "ciberclarias". Retrieved 2020-05-07, from https://www.radiotelevisionmarti.com/a/me-enfurece-y-contenidos-emocionales-las-presuntas-instrucciones-a-las-ciberclarias-/264779.html

Reuters. (2021). Taiwan says china is spreading fake news during COVID spike. Retrieved 2021-07-17, from https://www.voanews.com/east-asia-pacific/taiwan-says-china-spreading-fake-news-during-covid-spike

Revelli, A., & Foster, L. (2019). Network of social media accounts impersonates u.s. political candidates, leverages u.s. and israeli media in support of iranian interests. Retrieved 2019-05-28, from https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html

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

RFE. (2018). Russian trolls found amplifying u.s. republican charge against fbi. Retrieved 2019-05-14, from https://www.rferl.org/a/russian-trolls-amplify-us-republican-charge-anti-{T}rump-bias-at-fbi-/28986362.html

RFE/RL. (2019). Tajik students, educators claim they're pressured to 'troll' government critics. Retrieved 2019-05-12, from https://www.rferl.org/a/tajik-students-educators-claim-they-re-pressured-to-troll-government-critics/29936072.html

Robertson, I., Karan, K., & Kaul, A. (2019). Facebook takes down inauthentic pages with connections to thailand. Retrieved 2019-07-25, from https://medium.com/dfrlab/facebook-takes-down-inauthentic-pages-with-connections-to-thailand-7dbf331f5ba5

Rocha, R. (2018). Data sheds light on how Russian Twitter trolls targeted canadians. Retrieved 2019-05-15, from 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. Retrieved 2019-05-15, from https://www.washingtonpost.com/technology/2018/12/22/facebook-suspends-five-accounts-including-social-media-researcher-misleading-tactics-alabama-election/

Ronzaud, L., Eib, C. S., François, C., Chandra, A., Rio, V., & Thu, M. (2020). *Myanmar Inauthentic Behavior Takedown* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_report_myanmar_inauthentic_behavior_takedown.pdf

Ronzaud, L., Hubert, I., & Nimmo, B. (2020). *Capture the Flag* (Tech. Rep.). Retrieved from https://public-assets.graphika.com/reports/graphika_report_capture_the_flag.pdf

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

Rosendahl, J., & Forsell, T. (2016). Finland sees propaganda attack from former master Russia. Retrieved 2019-03-22, from https://www.reuters.com/article/us-finland-russia-informationattacks/finland-sees-propaganda-attack-from-former-master-russia-idUSKCN12J197

Ross, A. (2019). How Russia moved into central africa. Retrieved 2019-10-17, from https://www.reuters.com/article/us-africa-russia-insight/how-russia-moved-into-central-africa-idUSKCN1MR0KA

Roth, Y. (2019). Information operations on Twitter: principles, process, and disclosure. Retrieved 2019-06-13, from https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

RSF. (2020). Rsf unveils 20/2020 list of press freedom's digital predators. Retrieved 2020-03-12, from https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators

RT. (2018). Russians view us, ukraine and eu as country's main enemies – survey. Retrieved 2019-06-05, from https://www.rt.com/russia/415487-russians-us-ukraine-eu-enemies/

Ruediger, M. (2018). Electionwatch: FGV DAPP uncovers foreign Twitter influence in Brazil. Retrieved 2019-05-15, from https://medium.com/dfrlab/electionwatch-fgv-dapp-uncovers-foreign-twitter-influence-in-brazil-7ab24e34223

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

Sanger, D. E. (2018). Mystery of the midterm elections: Where are the Russians? Retrieved 2019-05-16, from 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. Retrieved 2019-05-14, from https://www.nytimes.com/2018/08/21/us/politics/russia-cyber-hack.html

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

Satariano, A. (2019). Facebook identifies Russia-linked misinformation campaign. Retrieved 2019-01-17, from https://www.nytimes.com/2019/01/17/business/facebook-misinformation-russia.html

Satter, R., Donn, J., & Vasilyeva, N. (2017). Russian hackers hunted journalists in years-long campaign. Retrieved 2019-05-08, from https://apnews.com/c3b26c647e794073b7626befa146caad

Savytskyi, Y. (2016). Kremlin trolls are engaged in massive anti-Ukrainian propaganda in Poland. Retrieved 2019-03-19, from http://euromaidanpress.com/2016/06/21/kremlin-trolls-are-engaged-in-massive-anti-ukrainian-propaganda-in-poland/

Sazonov, V., Müür, K., & Mölder, H. (2016). Russian information campaign against the ukrainian state and defence forces. *NATO Strategic Communications Centre of Excellence*.

SBSNews. (2018). Macedonia to hold name-change referendum on september 30. Retrieved 2018-09-31, from https://www.sbs.com.au/news/macedonia-to-hold-name-change-referendum-on-september-30

Schafer, B. (2017). Dashboards hamilton 68 and artikel 38. Retrieved 2019-05-15, from https://securingdemocracy.gmfus.org/securing-democracy-dispatch-10/

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

Sear, T., & Jensen, M. (2018). Russian trolls targeted australian voters on Twitter via auspol and mh17. Retrieved 2019-03-21, from https://theconversation.com/russian-trolls-targeted-australian-voters-on-twitter-via-auspol-and-mh17-101386

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

Sepúlveda, A. (2019). Detallan movilización de 'trolls tuiteros' por los 'brothers' de fortaleza. Retrieved 2019-07-30, from https://www.noticel.com/article/20190730/detallan-movilizacion-de-trolls-tuiteros-por-los-brothers-de-fortaleza/

Shane, S., & Blinder, A. (2018). Secret experiment in Alabama senate race imitated Russian tactics. Retrieved 2019-05-15, from https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html

Silva, S. (2021). Wikipedia in Chinese editing war of words. Retrieved 2021-12-03, from https://www.bbc.com/news/technology-59081611

Silverman, C., & Lawrence, A. (2016). How teens in the balkans are duping Trump supporters with fake news. Retrieved 2019-05-13, from https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-{T}rump-misinfo

Silverman, C., Lester, F. J., Cvetkovska, S., & Belford, A. (2018). Macedonia's pro-Trump fake news industry had american links, and is under investigation for possible Russia ties. Retrieved 2019-05-13, from https://www.buzzfeednews.com/article/craigsilverman/american-conservatives-fake-news-macedonia-paris-wade-libert

Silverman, C., & Mac, R. (2020). It Took Facebook More Than A Year — And A Whistleblower — To Remove A Troll Farm Connected To Azerbaijan's Ruling Party. Retrieved 2021-07-16, from https://www.buzzfeednews.com/article/craigsilverman/facebook-azerbaijan-troll-farm

Smith, R. (2019). Venezuelan bots, whatsapp and disinformation in spain. Retrieved 2019-05-21, from https://firstdraftnews.org/latest/venezuelan-bots-whatsapp-and-disinformation-in-spain/

Snegovaya, M. (2017). Russian propaganda in germany: More effective than you think. Retrieved 2019-03-20, from https://www.the-american-interest.com/2017/10/17/russian-propaganda-germany-effective-think/

Solon, O. (2017). How syria's white helmets became victims of an online propaganda machine. Retrieved 2019-06-05, from https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories

Soshnikov, A. (2017). Inside a pro-russia propaganda machine in ukraine. Retrieved 2019-03-25, from https://www.bbc.com/news/blogs-trending-41915295

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

St. Clair, J., & Frank, J. (2018). Ghosts in the Propaganda Machine. Retrieved 2021-07-17, from https://www.counterpunch.org/2018/01/05/ghosts-in-the-propaganda-machine/

Staff, M. (2018). Russia driving huge online 'disinformation' campaign on syria gas attack, says uk. Retrieved 2019-06-04, from https://www.middleeasteye.net/news/russia-driving-huge-online-disinformation-campaign-syria-gas-attack-says-uk

Stein, J. (2018). Tammy baldwin seeks hearing after Russians pushed image of obama in noose at badgers game. Retrieved 2019-03-22, from https://www.jsonline.com/story/news/politics/2018/03/21/tammy-baldwin-calls-twitter-troll-hearing-russians-pushed-wisconsin-image-obama-noose/446618002/

Stewart, E. (2019). How China used facebook, Twitter, and youtube to spread disinformation about the hong kong protests. Retrieved 2019-08-23, from https://www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media

Stewart, L. G., Arif, A., & Starbird, K. (2018). Examining trolls and polarization with a retweet network. In *Proc. acm wsdm, workshop on misinformation and misbehavior mining on the web.*

Stojanovski, F. (2017). Fake news tries to link austria's chancellor-to-be and philanthropist george soros. Retrieved 2019-05-13, from https://www.stopfake.org/en/fake-news-tries-to-link-austria-s-chancellor-to-be-and-philanthropist-george-soros/

Strick, B., & Syavira, F. (2019). Papua unrest: Social media bots 'skewing the narrative'. Retrieved 2019-10-11, from https://www.bbc.com/news/world-asia-49983667

Stubbs, J. (2020). Exclusive: Russian operation masqueraded as right-wing news site to target U.S. voters - sources. Retrieved 2021-07-17, from https://www.reuters.com/article/us-usa-election-russia-disinformation-ex-idUSKBN26M5ND

Stubbs, J., & Bing, C. (2018). Special report: How iran spreads disinformation around the world. Retrieved 2019-05-14, from 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. Retrieved 2019-05-13, from https://www.wired.com/2017/02/veles-macedonia-fake-news/

Suliman, M. (2021). Why russia is using facebook to launch disinformation campaigns in sudan. Retrieved from https://restofworld.org/2021/russia-sudan-facebook-disinformation

Summers, J. (2017). Countering disinformation: Russia's infowar in ukraine. Retrieved 2019-05-06, from https://jsis.washington.edu/news/russia-disinformation-ukraine/

Superlinear. (2018). Social media disinformation: parallels between the us and south african experiences. Retrieved 2019-05-15, from 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. Retrieved 2015-06-03, from https://www.manufacturing.net/news/2015/06/report-russian-internet-trolls-behind-louisiana-chemical-explosion-hoax

Szymański, P. (2018). Finland: the fight against disinformation. Retrieved 2019-03-22, from 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? Retrieved 2019-05-06, from https://www.lawfareblog.com/macron-leaks-are-they-real-and-it-russia

Tanakasempipat, P. (2020). Thai army denies Twitter disinformation campaign after takedowns. Retrieved 2021-07-17, from https://www.reuters.com/article/us-thailand-cyber/thai-army-denies-twitter-disinformation-campaign-after-takedowns-idUSKBN26U0W2

The Shift. (2018). Investigating joseph muscat's online hate machine. Retrieved from https://theshiftnews.com/2018/05/14/investigating-joseph-muscats-online-hate-machine/

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

Thomas, J. (2019). Cyber warfare in vietnam. Retrieved 2017-10-04, from https://theaseanpost.com/article/cyber-warfare-vietnam

Timberg, C., & Romm, T. (2018). These provocative images show Russian trolls sought to inflame debate over climate change, fracking and dakota pipeline. Retrieved 2019-04-23, from https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/congress-russians-trolls-sought-to-inflame-u-s-debate-on-climate-change-fracking-and-dakota-pipeline/

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

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

Twitter and F]acebook say they removed thousands of troll accounts in run-up to 2018 midterms, author=Collins, Ben, year=2019, publisher=NBC News, url = https://www.nbcnews.com/tech/security/twitter-says-it-removed-troll-accounts-tied-russia-iran-venezuela-n965491, urldate = 2019-01-31. (n.d.).

Uren, T., Thomas, E., & Wallis, J. (2019). Tweeting through the great firewall. Retrieved 2019-09-03, from https://www.aspi.org.au/report/tweeting-through-great-firewall

van der Noordaa, R., & van de Ven, C. (2019). The mh17 plot. Retrieved 2019-05-31, from https://www.groene.nl/artikel/het-mh17-complot

Volz, D. (2017). U.s. far-right activists, wikileaks and bots help amplify macron leaks: researchers. Retrieved 2019-05-15, from https://www.reuters.com/article/us-france-election-cyber/u-s-far-right-activists-wikileaks-and-bots-help-amplify-macron-leaks-researchers-idUSKBN1820QO

Wallis, J., Uren, T., Thomas, E., Zhang, A., Hoffman, S., Li, L., ... Cave, D. (2020). *Evidence of Russia-linked influence operations in Africa* (Tech. Rep.).

Weixel, N. (2018). Nearly 600 Russian troll accounts tweeted about obamacare: report. Retrieved 2019-05-01, from https://thehill.com/policy/healthcare/406309-nearly-600-russian-troll-accounts-tweeted-about-obamacare-report

Wendling, M. (2017). Russian trolls promoted California independence. Retrieved 2019-04-23, from https://www.bbc.com/news/blogs-trending-41853131

Wendling, M. (2019). General election 2019: Reddit says uk-us trade talks document leak 'linked to Russia'. Retrieved 2019-12-07, from https://www.bbc.com/news/blogs-trending-50695558

Winger, G. (2020). China's Disinformation Campaign in the Philippines. Retrieved 2021-07-17, from https://thediplomat.com/2020/10/chinas-disinformation-campaign-in-the-philippines/

Withnall, A. (2018). Finland: Russian propaganda questioning our validity risks destabilising country. Retrieved 2019-03-22, from https://www.independent.co.uk/news/world/europe/russia-finland-putin-propaganda-destabilising-effect-a7371126.html

Wong, J. C., & Harding, L. (2021). 'Facebook isn't interested in countries like ours': Azerbaijan troll network returns months after ban. Retrieved 2021-07-16, from https://www.theguardian.com/technology/2021/apr/13/facebook-azerbaijan-ilham-aliyev

Wong, Q., & Hautala, L. (2018). Facebook removes iranian influence campaign as midterms near. Retrieved 2019-06-05, from https://www.cnet.com/news/facebook-announces-removal-of-iranian-influence-campaign-as-midterms-near/

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

Yaron, O. (2018). Tel-aviv times? iran created fake hebrew news sites in major 'influence campaign'. Retrieved 2019-03-22, from https://www.haaretz.com/israel-news/.premium-israeli-cyber-security-company-iran-created-fake-hebrew-news-sites-1.6463020

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

Yong, C. (2018). Select committee on fake news: Russian trolls divided societies and turned countries against one another. Retrieved 2019-05-13, from https://www.straitstimes.com/politics/select-committee-on-fake-news-russian-trolls-divided-societies-and-turned-countries-against