THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY of WASHINGTON

TASK FORCE REPORT

Hacking Democracy: Cybersecurity and Global Election Interference

2018

Henry M. Jackson School of International Studies
University of Washington, Seattle
Task Force Report Winter 2018

Hacking Democracy:

Cybersecurity and Global Election Interference

Faculty Advisor
Dr. Jessica Beyer

Evaluator
Paul Nicholas
Senior Director, Global Security and Diplomacy, Microsoft

Editors
Alexander Wirth
Julia Summers

Coordinator
Heidi Samford

Authors
Qi Cheng
Conor Cunningham
Fabian Gacayan
Anni Gu
Alex Hall
Olivia Lee
Ashley Sawyer
Safy Sayoud
Vriti Wadhwa
Jion Yi

Table of Contents

Executive Summary

As the global community enters a new digital era, the increase of social connectivity, the proliferation of online hostile actors, and the deliberate obfuscation of media pose new challenges to democratic processes around the world. In this project, we examine the global impact of Internet-based election interference on democratic processes through a survey of 12 democratic countries with elections within the past five years. We use this information to derive policy recommendations for the US government based on successful government policies in states surveyed and an in-depth understanding of the US case.

Our research illustrates that election interference has become an important factor of the democratic process in many states around the world. In nearly every country we examined, external governments and/or domestic politicians used disinformation and cyberwarfare tools to influence the public and attack democratic institutions. While election interference is not a new phenomenon, the technologies used today reach a larger and more diverse group than ever before.

Our case studies include one country in North America (United States), one in South America (Brazil), six in Europe (Bulgaria, France, Italy, Spain, Ukraine, United Kingdom), two in Africa (Senegal, Kenya), and three in Asia (Japan, India, South Korea). We also examine a history of election meddling during the Cold War to understand the history of such interference and to look for solutions from before the digital age.

Each case study covers an election or several elections that have occurred recently or will be held soon after the publication of this project. For some countries, these elections are presidential contests, while others are parliamentary or other legislative elections. We also examined the 2016 United Kingdom European Union membership referendum and the 2017 Catalán independence referendum in Spain.

Case Studies

Each country case study is divided into sections detailing the types of election manipulation that occurred, as well as the actors that perpetrated any attempted interference. Case studies also include information that contextualizes election meddling within each country's unique political and social circumstances. The election meddling portions of the case studies are divided into two types. First, we examine *election infrastructure meddling*, which we define as attacks on government systems integral to elections and any related infrastructure with

the intention of manipulating the outcome of an election. Second, we focus on *social media meddling*, which we define as attempts to artificially influence public discourse online with the intention of manipulating the outcome of an election.

Election Infrastructure Meddling

Election infrastructure meddling was found in 7 of our 13 case studies. Election infrastructure meddling includes attempts to gain access or manipulate vote-tallying systems, other election systems, such as voter registration systems, and systems that are not associated with the government but are important to elections, such as political parties.

For example, in Kenya the country's supreme court suspended the 2017 general elections after finding unspecified evidence that the vote-tallying system had been manipulated. In the 2016 United States presidential election, at least two state voter registration systems were compromised following a barrage of spear-phishing and other hacking attempts. In 2017, damaging information about one of the candidates in the French presidential elections was taken from the online systems of their campaign through hacking and leaked to the press. In addition, several case studies revealed weaknesses in current electronic voting systems, such as easily hacked devices in use during United States' and Indian elections.

Social Media Meddling

Social media meddling was found in 12 of our 13 case studies. Social media meddling includes the use of "fake news" – deliberately spreading false or misleading information – something we found in nearly every case. It also includes armies of politically motivated "troll" accounts, automated social media accounts, and online communities functioning as meme factories.

For instance, in Brazil, fake news was used to turn public opinion against the embattled President Dilma Rousseff, shifting the political landscape of Brazil ahead of this year's general election. In Ukraine, legions of "troll" accounts have been used to harass political activists, media, and politicians, sowing discord during the 2014 presidential and parliamentary elections. In Spain, automated accounts churned out fake news and propaganda in Catalonia during the region's controversial independence referendum. In Japan, online communities with ties to political parties promote memes online and act as informal promoters of Japanese nationalism.

Our research revealed that attempts to influence electorates are widespread; in Bulgaria, for example, nearly three quarters of citizens reported seeing a form of fake news. The concept

of election interference itself has also become heavily politicized. In Senegal, the "fake news" moniker is being used as a tool to delegitimize opposition media, and in the United States, right-wing media sources have worked to cast doubt on the existence of election manipulation.

Actors

We identified two major perpetrators of election interference; domestic political partisans and foreign states. In the cases we examined, the only foreign state involved in election manipulation was the Russian Federation.

Domestic political partisans tended to be nationalist, but included both incumbents and opposition actors. For example, in Kenya, social media meddling stood to benefit the campaign of incumbent Uhuru Kenyatta, while in Italy and the United Kingdom, social media meddling fueled or is fueling the cause of right-wing, populist ideologies in opposition to the existing government.

We found the Russian Federation to be the only state actor that has acted to manipulate elections abroad in our case studies. This manipulation took a variety of forms, from covert support of favored candidates in places such as Bulgaria, Italy and France, to extreme destabilization campaigns such as the cyberattacks in Ukraine. Election interference was carried out with varying intentions, sometimes with the intention of supporting a given candidate, sometimes with the intention of blocking a candidate, and sometimes with the apparent goal of creating social discord.

Policy Recommendations

During the project, we identified seven recommendations intended to better mitigate the threat of online-election interference in the US. The recommendations include suggestions for actions within the US Federal Government, as well as its engagement with outside election infrastructure, such as the US public, US states, and the international community.

1. Engage civil society in debunking fake news by promoting information literacy among the public and providing grants to organizations working to disprove misinformation

2. Make social media platforms accountable for countering the spread of fake news on their platforms and removing fake profiles and bots from their networks

3. Involve state officials more deeply in Department of Homeland Security (DHS) investigations

4. Engender the sharing of best practices among states

5. Offer resources to non-government organizations, such as the Democratic and Republican National Committees, to make them less vulnerable to future cyberattacks

6. Compel voting machine hardware and software vendors to make their products secure

7. Propose a resolution to the United Nations General Assembly that establishes an internationally accepted definition of information warfare

Recommendation 1 – Engaging Civil Society in Debunking Fake News

Based on the proliferation of fake news and its influence in elections, we recommend that the US government engage civil society in debunking fake news by promoting information literacy among the public and providing resources to organizations working to disprove misinformation. Both Ukraine and Bulgaria have created programs that draw on civil society to combat disinformation campaigns. Federal and state institutions should support civic groups similar to those in Ukraine and elsewhere financially. Expanding these organizations will help to educate civil society on how to better understand and target fake news and propaganda and also provide databases about fake news.

In response to Russia's computational propaganda, Ukraine's government initiated the "Internet Army" project, which invited volunteers to participate in combatting Russian disinformation campaigns. At the same time, media projects such as StopFake (stopfake.org) and Euromaidan Press were launched to debunk fake news and provide fact based news resources. StopFake debunks fake news and propaganda, verifies information, trains media stakeholders to better identify fake-news, and gives seminars on journalistic integrity and fact checking. Additionally, HromadskeTV, an independent media channel that is funded by public donations and grants, was started in 2014.

Bulgaria also has several civil society media organizations actively working to debunk fake news and propaganda. Stopfake.org is one such organization that volunteers run and fund - having spread from Ukraine to Bulgaria.

In Japan and Senegal there are also efforts to counter disinformation online and, in Senegal, there is active government support for civil society working in this space.

Recommendation 2 – Make Social Media Platforms More Accountable

In the digital era, public security and private social media platforms are deeply connected. The US Government should create legislation compelling social networking services to meet standards on the prevention of disinformation on their platforms. Social media platforms should create teams responsible for addressing bots, trolls, fake news and illegal ads. These teams should also serve as liaisons between law enforcement and social media platforms.

Several countries have implemented similar measures. For example, Germany requires websites to remove content deemed illegal, such as hate speech, fake news and illegal materials. Failure to comply with the law within 24 hours can result in a fine of up to 50 million Euros ("Germany Starts Enforcing Hate", 2018). Additionally, French president Emmanuel Macron has announced legislation to fight "fake news" on social media. Transparency regarding the source of advertisement funding on popular social media platforms will be required, as well as limits on the amount of advertisements ("Macron Plans Law to Fight", 2018). In Italy, Facebook has launched a new fact-checking tool that debunks false information with the Italian Segment of Facebook (Serhan, 2018).

Recommendation 3 – Involve State Officials More Deeply in DHS Investigations

We also recommend that the DHS involve state officials more deeply its investigations. Following the DHS announcement that 21 states had been targeted by Russian state-sponsored hackers prior to the 2016 Presidential Elections, states expressed frustration that the DHS had been inadequately forthcoming in providing information for states to identify and mitigate threats on their systems (Mulvihill & Pearson, 2017). For example, state elections officials were denied access to information because of inadequate federal security clearances, and many of these clearances had not been granted more than a year after the 2016 elections (Lee, 2018). The DHS has announced that it is has prioritized 37 security clearance requests for state and local officials tasked with election management, including employees involved with election cybersecurity. The DHS should further prioritize its security-clearance processing to grant clearances to state officials who have elections in the near future. For example, Texas will hold midterm elections for the 2018 midterm elections in March 2018. The DHS should also expand the number of security clearances given to include at least several employees in every state elections office.

States have complained that prior to the 2016 Presidential Elections, they were not given information that could have been used to help them understand the threat of hacking. The DHS should not only examine the process with which it makes documents available to states, which it has announced it will do (Johnson, 2018), but also work to be more proactive in sharing relevant information with states prior to elections. The DHS should strive to continue to work with Secretaries of State to ensure mutual understanding of all cybersecurity related issues that arise.

The DHS should be more active in giving resources to states to help develop systems adequately protected from cyberattacks. While the DHS has announced that it will be able to fill requests from states that have requested analysis of their systems to determine cyberattack readiness (Johnson, 2018), many states will not be fully examined until September 2018 (Starks 2018). The DHS should continue prioritizing the examination of state election infrastructure for vulnerability to cyberattacks, and should make sure that all 50 states and the District of Columbia are examined with time allotted to allow states to upgrade infrastructure before the next major elections. Federal government examinations should include recommendations for states to upgrade their systems.

Recommendation 4 – State Election Security Best Practice Sharing

The US government and state governments should work to make sure that states share best practices for election protection. States should work to more proactively involve themselves in organizations designed to maintain secure election systems across the US. For example, states should closely work with the National Election System Information Sharing & Analysis Organization (NES-ISAO) to identify upcoming threats and best practices.

Additionally, states should work to integrate their government and the private sector more closely in cybersecurity preparedness. For example, Oregon has established a Cybersecurity Center of Excellence and the Oregon Cybersecurity Advisory Council to promote public-private collaboration in cybersecurity. Such organizations can engender an environment of partnership and encourage states and private entities to collaborate around election security.

States should take the example of other countries in pursuing initiatives undertaken at the provincial/state level that increase election security. For example, the South Korean province of Gyeonggi-do has established a blockchain supported voting system, using the technology to create a digital voting trail that is extremely difficult to manipulate.

While voting procedures that vary across state jurisdictions have made it difficult for a large scale cyberattack on US election infrastructure, states should work to share best-practices to increase the security of their peer governments. For example, governments that mandate post-election audits that test election results can advocate for the implementation of similar policies elsewhere.

Recommendation 5 – Offer Resources to Election-related NGOs

We recommend that the US federal government offer resources to non-government organizations, such as the Democratic and Republican National Committees, to make them less vulnerable to future cyberattacks. The US Government should offer assistance to election institutions, including candidate campaigns and their corresponding parties, to ensure that their cybersecurity is adequately protected against the possibility of a cyberattack. When the US government receives credible information of attacks against election institutions, they should be proactive in communicating with the institution and offering appropriate assistance to mitigate the impact of the attack.

Recommendation 6 – Compel Secure Voting Hardware and Software

Our research shows that voting machines and election related software creates election vulnerabilities anywhere they are used. In many of our cases, governments are sticking to paper ballots because of security concerns. The US government should legally compel voting hardware and software vendors to create secure systems—including creating more transparency around their products.

The federal government should use the Information Sharing Analysis Centers (ISACs) mechanism to create greater industry-wide security. ISACs are entities created by critical industries and operators to share information on potential threats to the operation of given industries (About ISACs, 2017). While ISACs exist as tools to assist the federal and state government in a variety of critical industries, such the automotive industry, oil and gas industry, public transit industry, and others, no ISAC exists to promote security between election firms. While the designation of election infrastructure as critical infrastructure under the Government Facilities critical infrastructure designation suggests the creation of an ISAC to correspond to the election industry, this has not been organized publicly. The federal government should encourage the formation of an election infrastructure ISAC immediately.

Additionally, the US government should require vendors that provide hardware and software for elections to maintain more stringent standards for cybersecurity, such as those modeled in the National Defense Authorization Act, which mandates strong cybersecurity regulations for contractors working with the Department of Defense, allowing their removal from the military supply-chain for noncompliance to cybersecurity regulations (Charney & Werner, 2011). For example, authorities in France have mandated security requirements for electronic voting devices on the local level, while entirely electronic voting countries such as India and Brazil have faced increasing scrutiny of their elections systems.

Further, Election Poll Books, which are used to access voter registration systems at polling stations in certain states, should be required to be tested before election day, and should only be used with paper backup systems present to account for possible database discrepancies or system outages.

Also, while many states use electronic vote recording systems either in general elections or as disability accessible devices, only some states use the systems with verified-voting paper audit trails (VVPAT), which produce a physical record of voting simultaneous to the electronic vote. In cases around the world, unverified electronic voting has led to concerns of election tampering, and even lead to the annulment of a presidential election in Kenya. The US government should pursue the possibility of requiring electronic voting devices to use VVPAT. Many countries surveyed in this project, such as the United Kingdom, Ukraine, and

The US Government should pass the Amendment to the National Defense Authorization Act for 2018, which would require that grant money provided by the federal government to states for election purposes cannot be spent on electronic voting devices without VVPAT, but allow states to spend grant money on post-election audits as well as cybersecurity improvements ("Brennan Center Summary", n.d.).

Finally, the US Government should use the proposed Internet of Things Improvement Act of 2017 as a model. This Act would require that Internet equipped devices installed in US government networks have no known cybersecurity vulnerabilities, are readily patchable, and that government agencies must seek permission from the Office of Management and Budget before purchasing any non-compliant devices (Sterling 2017). The same type of requirements should be put on any election security mechanisms.

Recommendation 7 – Become a Leader in Creating International Norms

The US should introduce a resolution to the General Assembly of the United Nations (UNGA) to establish an internationally accepted definition of "information warfare" and "election interference" efforts. The UNGA contains the legal framework to establish a set of norms regarding acts of information warfare that could set a foundation for further international dialogue regulating international cyber conduct. By increasing communication, the international community can simultaneously enhance tactics to counter information warfare.

Following patterns of information exploitation throughout the Cold War, defamation, propaganda, and "fake news" campaigns will be utilized in continued election interference attempts unless there are international safeguards creating repercussions for violators.
The international community needs to reach a consensus for common terminology and define information warfare to eliminate legal ambiguity. Current international protections for election manipulation consist of adaptions of more general international sovereignty statutes. These international statutes leaves the connection between cybersecurity and information warfare unaddressed and allows election manipulation attempts to go unchecked without repercussions.

While the task of creating any shared standards in the UNGA is daunting and haunted by the failed efforts of previous attempts to define contentious terms, as well as continued controversy around offensive cyberwarfare, there appears to be rough agreement that something must be done. For instance, in 2017, after the UN Group of Governmental Experts failed to come up with any agreement around cyberwarfare, US representative Michele Markoff argued, "I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions." (Markoff, 2017) and, in 2015, the countries that make up the Shanghai Cooperation Organization (which includes Russian and China) wrote a letter to the UN arguing that, among other things, states must not, "Use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability." The two perspectives are embedded in very different views of Internet Governance – Internet sovereignty versus multi-stakeholderism – but both reflect an underlying desire to take action.

Our research illustrated that the major lesson to be learned from Cold War election interference is that without a major power backing efforts to end election manipulation, nothing will happen. The major actors in this space – the US, China, and Russia – must set aside the useful tool of cyber-manipulation. The US should step forward and lead.

Other Lessons Learned

In this section, we include several policies found in our survey of global Internet-based election interference. While these examples did not fit into larger recommendations, we felt they deserved highlighting as examples lessons learned to address the wide-reaching problem of election interference.

Brazil

Você Fiscal (You Inspector), an app created by cybersecurity expert Diego Aranha, allows voters to match election results with the number of votes registered on the voting machine by matching a photo taken of the immediate results to the final tally. Following each election, the results from every machine are printed and posted in a public place such as a town hall. Then, the voter is able to photograph the results and submit them to an online database monitored by Aranha and his colleagues at the University of Campinas. This helps prevent interference in the transmission process for ballot results from polling stations to the central system.

Japan and France

In Japan, strict legal restrictions have decreased the ability of fake news and disinformation to spread in the period immediately prior to an election. For example, the ban on media discussion of election news slowed the distribution of leaks tied to the campaign of French presidential candidate Emmanuel Macron in the 2017 French Election.

Kenya

Kenya offers an example of the dangers of not paying attention to the commercialization of disinformation campaigns on social media during campaigns. Harris Media LLC, a US based advertising agency that uses social media and data analytics to target audiences during political campaigns, was operating during the last Kenyan election (Privacy International, 2017). It was working against the candidate Raila Odinga, creating content that had the potential to destabilize the election and cause violence—including claims Odinga would implement martial law and relocate tribes other than his own from Kenya.

United States of America 2016 Presidential Election

By Alexander Wirth

Internet-based election interference played a prominent role in the 2016 United States presidential election. Interference included attempts to influence social discourse through fake news, social media bots, troll armies, and online communities as well as direct cyberattacks against election infrastructure, political parties, and private companies associated with elections. Interference operations were likely sourced from the Russian Federation, as well as domestic political partisans. Election meddling has played a prominent role in American politics following the 2017 election, and is currently the subject of government investigation.

Table 1: Election Interference in the United States	
Election Infrastructure	
Government Hacking	N
Political Hacking	Y
Election Infrastructure Hacking	Y
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	Y
Online Communities	Y
Election Manipulation Actors	
Russian Federation	
Alt-Right Political Communities	

Recent Election

This case study focuses on the most recent United States presidential election, which occurred on November 6, 2016. During this election, Former Secretary of State Hillary Clinton, the presidential nominee of the Democratic Party, ran against businessman Donald Trump, the nominee of the Republican Party. Donald Trump won the election, carrying 304 electoral votes of the necessary 270 but receiving only 46.1 percent of the popular vote to Clinton's 48.2 percent (Federal Elections Commission, 2017). The election also led to victories in the federal Senate and House for the Democratic Party (although the Republicans retained majorities in both chambers), while the Republican Party gained net two additional gubernatorial offices.

Background Context

The US is one of the oldest modern democracies, as well as the second largest democracy by population. In the 2016 election, 55.8 percent of Americans eligible to vote turned out, an increase from the 2012 election (Federal Elections Commission, 2017). Two parties, the Democrats and the Republicans, dominate the US political system. The US is rated "Free" by Freedom House (Freedom House, 2018) and ranks 18th on Transparency International's Corruption Perception Index (Transparency International, 2018).

Because it is one of the world's superpowers, many actors have large stakes in the policy outcomes of US presidential elections. The executive branch of the US, headed by the president, has broad discretion to determine foreign policy, spend the national budget, and determine policy outcomes, creating strong incentives to work to install friendly actors in the position and block actors who might threaten interests.

Election Infrastructure and Policy Background

The US conducts elections through state governments, mostly through the offices of elected Secretaries of State. While the federal government has some laws governing election conduct, most election policy is determined at the state level. Because of the broad discretion given to states, elections can look different depending on the state in which you vote. 22 states allow ballots to be cast early, while in 26 states voters must go to a voting place on Election Day (Verified Voting, 2016).

Eligibility to vote can change depending on state. States have discretion over whether convicted felons are eligible to vote, the method with which citizens register to vote, and other requirements for voting, such as types of identification presented at polling places. Voter identification laws vary by state, with some states requiring identification (including driver's licenses, government identification, utility bills, and other forms) while others will hand out provisional ballots to voters without IDs (Underhill, 2018). States also decide the eligibility requirements for absentee ballot voting and whether or not voters must register a party affiliation to take part in political party primary elections.

Election Infrastructure Meddling

While not as visible as social media influence, the United States election infrastructure was subject to multiple cyberattacks with mixed success. In 2016, the DHS classified election infrastructure as critical under the Government Facilities designation, freeing federal resources unavailable before to assist the protection of election mechanisms. However, as the relationships

between the federal and state governments becomes increasingly politicized, and state level secretaries of state diverge from the federal government in level and strength of cybersecurity management, the ability of the US voting system to protect itself from cyberattacks is not clear.

Leaks through Hacking

The hacking and release of files associated with candidate Clinton and the Democratic National Committee during the presidential campaign played a large role in attempts to sway public discourse before voting.

Throughout the 2016 election process, Democratic, Republican, and non-partisan systems were broken into by Fancy Bear (also known as Advanced Persistent Threat (APT) 28), Cozy Bear (APT29) a parallel apparatus to Fancy Bear, and other hackers (Meyer, 2016). These leaks, which included communications between DNC and Clinton campaign staffers, were subsequently linked by Guccifer 2.0, believed to be another pseudonym for Russian intelligence agents, and WikiLeaks, a website that publishes leaks of secret or classified information (Rutenburg, 2017). The leaks were released gradually, apparently to insert them in several news cycles, and were taken up by right-leaning mainstream media outlets as well as fake news websites, bots, and far-right online communities. While the hack was covered extensively by right wing media such as Breitbart and the Daily Caller, it was also picked up and reported on by center or center-left leaning media such as the New York Times, Politico, and the Washington Post (Hamburger and Tumulty, 2016).

Additionally, conservative media has continually challenged the notion that the leaks were caused by Russian hacking (Klein, 2017). Because of the steady release of the leaks, the impact of the releases on the outcome of the presidential campaign is not clear – however, the leaks occurred at the same time the opinion polls of the two campaigns began to tighten, turning against the Clinton Campaign (Enten, 2016). Much like with other fake and junk news, the DNC leaks were spread most voraciously in swing states - in Michigan for example, more than half of Twitter news was fake or junk coverage (Kwong, 2017).

Voting Machine Tampering

States use a variety of equipment to tally votes, varying on the state, county, and local level, as well as in providing accessibility accommodations or tallying early votes. States use mail in and paper balloting, as well as Direct Recording Electronic Voting Systems (DRE). DRE can be equipped with voter-verified paper audit trails (VVPAT), which record electronic votes

on paper to create a verifiable record; VVPAT is implemented in slightly more than half of states where DREs are used (Verified Voting).

No Secretaries of State reported that their election systems were hacked during the 2016 elections (Perlroth, et al., 2017). However, the potential for hacking voting machines could be a threat in the future. During the DEFCON 25 conference in 2017, every digital voting machine tested by a group of hackers was breached. Devices were found to have universal default passwords that could be found with a Google search, or easily reachable USB ports from which software could be inserted and run. One device had an exploitable system weakness that had been in the system since 2003. Many devices included physical or digital parts that were manufactured in other countries, specifically China (Blaze, et al., 2017).

Voting Registration Tampering

During the presidential campaign, repeated cyberattacks were directed at secretaries of states and others connected to voter registration (Satter, 2017). Reports of hacking against state election infrastructure appeared in the fall of 2016, when the US Government announced that hackers had targeted at least 20 state election websites (Mulvihill & Pearson, 2017).

Eventually, the DHS announced that four state election systems had been compromised – the two that have been made public, Arizona and Illinois, both had their voter registration systems compromised by hackers, one of them likely associated with the Russian Federation (Fessler, 2017). In Illinois, hackers accessed voter records through a security flaw in an online voter registration form, through which they were able to view voter registration information (there is no evidence that information was edited) (Berkowitz, 2017). In Arizona, the US Government found that an employee's password was compromised and available online; it is not clear how the password was stolen and there is no evidence the credentials were used to access the system (Vicens, 2016). The other breaches have not been made public. In addition to the four state systems, hackers successfully breached and used the election software company VR systems to send spear phishing emails to 122 state and local election administrators; it is unclear if these hacking attempts were successful (Perlroth, et al., 2017).

In the US, voter registration systems are separate from voting tabulation, and compromised voter registration systems do not directly impact voting results (Berkowitz, 2017). While there is no evidence that voter registration systems were edited, changes to registration records, such as deleted names or changed addresses, could lead to interruptions during voting

(Harris, 2016). Additionally, much information around voting discrepancies during the 2016 election remains sealed – many states have not carried out extensive examinations of their voting systems to determine if breaches or hacking occurred (Perlroth, et al., 2017). In many states, information on the nature of hacking attempts on their system were not given to them by the federal government because of the information's classification – in late 2017, a year after the election, the DHS began offering security clearances to state election officials (Syeed, 2017).

Social Media Meddling

During the 2016 elections, a variety of methods were used to sway public discourse, including fake news, troll armies, online communities working as meme factories, bots, hacking, and other tools (Marwick & Lewis, 2017). These tools were pervasive; in one study of fake news access in 2016, it is suggested that the average American adult saw and remembered more than one story published through a fake news outlet (Allcott and Gentzkow, 2017).

Facebook has testified to the US Congress that approximately 126 million Americans were served Russian sponsored advertising in 2016 (Byers, 2017). Attempts to influence American election discourse were carried out by political actors in the United States, such as "alt-right" social media figures and partisan online communities, as well as one state actor, the Russian Federation. These methods were used largely against Democrat Hillary Clinton and for Republican Donald Trump (Marwick & Lewis, 2017).

Internet Use Profile

The most popular social media site in the United States is Facebook, although Twitter, WhatsApp, Instagram and Snapchat are also popular (Alexa, n.d.). Facebook, the largest US social network, is used by 79 percent of Americans (Greenwood, Perrin & Duggan, 2016).

Fake News and Rumors

In the 2016 election, Fake News was distributed en masse to Americans via social media, likely reaching more Americans than its analogs in the mainstream media. According to a Buzzfeed study, the five most shared Fake News articles all outperformed their counterparts from more mainstream sources. "Pope Francis Shocks the World, Endorses Donald Trump for President, Releases Statement" outpaced the most shared mainstream news article "Trump's History of Corruption is Mind-Boggling. So Why is Clinton Supposedly the Corrupt One?" by 100,000 social media engagements (Silverman, 2016). Well-established US media outlets, such as the Washington Post (which published the corruption article) were regularly outperformed by websites with no clear offices, employees or contact information (Silverman, 2016).

While fake news stories from individual outlets often did not receive much attention, stories that were picked up by other outlets, fringe political blogs, and social media figures quickly reached exponentially larger audiences (Bounegro et al., 2017). The content of fake news tended to be right leaning, often endorsing conspiracy theories around the Clinton Campaign. Some fake news was also geared towards left-leaning audiences in an attempt to pull supporters from center-left Clinton, including ads supporting political movements such as Black Lives Matter or left-wing competitors such as Bernie Sanders (Shane, 2017b). Fake news was folded into already existing American conspiracy theorist networks – hosted on websites that already held a suite of popularly held conspiracy theories (Starbird, 2017).

While fake news was often written with a political motive in mind, many articles also were created because of the profitable web page traffic they promised – in fact, some places built industries out of American fake news. In the Macedonian town of Veles, an entire industry came to be constructed around the generation of right-wing fake news; this was not because of the area's political affiliation, but because conservative articles were more likely to be clicked and thus higher revenue producers (Subranian, 2017).

Bots

According to a study by the Universities of Southern California and Indiana, roughly nine to 15 percent of Twitter accounts are bots (Varol et al.,2017). During the 2016 elections, bots were leveraged to influence American opinion on a variety of levels, interacting with individual users, promoting posts that served their interests, and using large scale posting to generate artificial trends. Bots played an important role in propagating misinformation and obfuscating reality in online political media. According to an Indiana University survey, while bots made up eight percent of a given sample of Twitter users, they represented 33 percent of shares of fake news (Shao et al., 2017).

On Twitter, bots targeted real users identified as susceptible to fake news, and would tag users with large amounts of followers in tweets to direct their followers' attention to fake news. Bots also tagged geographic locations in an apparent attempt to influence certain geographic areas over others, peaking in political swing states such as Michigan in the days before the election (Clifton, 2017). While the ownership of many bots remains unknown, a large amount of them appeared to be controlled by parties related to the Russian Government; the cybersecurity firm FireEye told the New York Times that it had identified multiple fake account originating in

Russia (Shane, 2017) and Varol et al. found that many of the same accounts used in the US presidential election began to promote misinformation in the following French and German elections, in line with Russian geopolitical interests (Varol et al., 2017).

Troll Armies

Troll armies were very active during the 2016 US Elections, and were significant in their role of spreading fake news and misinformation. Originally, trolls referred to Internet users who carried out mischief or activities online intended to engender a humorous response, however in the 2016 election trolls took on the role of far-right provocateurs, transitioning over time from parodying far-right beliefs rooted in racial and gender prejudice to seriously promoting those ideas (Marwick & Lewis, 2017). While many trolls were likely political partisans within the United States, groups sponsored by the Russian Federation, notably the Internet Research Agency, were likely also involved in the promotion of "trolling" and fake news (Bradshaw & Howard, 2017).

Online Communities and Meme Factories

The 2016 presidential election was marked by the rise of online communities playing a significant role in amplifying and shifting certain discourses throughout the election cycle. Congregating on message boards such as 4Chan, 8Chan, and Reddit, far-right posters created image-macros, commentary, memes, and social media strategy to promote far-right media and the Donald Trump campaign. Posters made up a variety of subsets of Internet culture – conspiracy theorists, men's rights activists, and white supremacists (Marwick & Lewis, 2017).

Conclusion

The 2016 elections showed the power of Internet-based communication and infrastructure in impacting the political discourse of the United States. The ability of the United States to prescribe solutions before it is tested again, in 2020, is much less clear. As the world continues to faces the consequence of increased interconnectivity and the rise of fake news dissemination through social media, the United States serves as an example of the sheer dynamic shifting power cybersecurity and social engineering can have on national paradigms.

Election Interference during the Cold War

By Heidi Samford

Throughout the Cold War, election manipulation operations served as a foreign policy instrument to achieve policy goals and oppose policy threats in foreign elections. As a result, state-sponsored propaganda, misinformation campaigns, and covert funding of political movements became a frequent and prevailing feature of Cold War democracies. These election manipulation methods provided the framework for Internet-based election manipulation efforts and information warfare.

Political Background

Election manipulation offers a unique ability to influence political rhetoric while avoiding high military expenses or escalating conflict. It also provides plausible deniability to states attempting to influence rivals' domestic politics (Goldman, 2015). After the onset of the Cold War, election interference became a surrogate for hard conflict and a crucial tool in American foreign policy and strategy to combat the expanding Soviet Union. (Del Pero, 2001). Covert funding of political campaigns, candidate training, document forgery, defamation campaigns, and the spread of propaganda were the most utilized interference tactics. Successful election interference depended on the covert nature of the attempt. Therefore, for the purposes of this overview, military coup d'états are not included as election manipulation. When tracking elections throughout the Cold War, Levin found covert manipulation efforts in 64.1 percent of national elections (Levin, 2016). However, even the "overt" influencing attempts contained covert elements. This accounted for 23.8 percent of election influencing attempts (Levin, 2016).

Nations who engaged in election influence operations had the opportunity to elect officials inclined to act in accordance to the nation's political agenda, providing beneficial diplomatic relations. The US maintained a political interest in promoting democratic ideology within foreign elections in order to limit the spread of communist influence. Alternatively, the Soviet Union aimed to establish a communist model in Eastern Europe and spark a global socialist movement while increasing their regime security. The US and Soviet Union are connected to 117 instances of election manipulation between 1946-2000; this translates to 11.3 percent of national elections (Levin, 2016). 59 percent of campaigns that received election aid from the US or Soviet Union achieved their designed election outcome (Agrawal, 2016).

Covert Funding

Covert funding of ideologically aligned political organizations became a prominent form of election manipulation. The US founded the Central Intelligence Agency's Office of Policy Coordination (OPC) to influence election outcomes by channeling money into the campaigns of centrist coalitions (Warner, 1998). The US deployed dozens of covert funding operations throughout the 1960s and 1970s around the world (Border, 1997).

Italy's 1948 Parliamentary election illustrates the effectiveness of covert funding. Both Cold War superpowers engaged in covert operations to influence the outcome of the election. The Italian election occurred during a critical period, following a communist coup in the Czech Republic earlier in 1948 (Luconi, 2011), increasing concern over communist influence. The creation of the Italian Communist Party and the Italian Socialist Party further signaled the growing influence of communism in Italy. The US implemented covert funding operations to ensure Soviet-leaning parties would never reach leadership positions.

Anti-communist political parties received covert aid from the US in an attempt to counter the leftist coalitions (Del Pero 2001). The communist left suffered a large defeat at the polls while the Christian Democrat party gained an absolute majority, drawing 48.7 percent of votes and gaining a majority in the Italian Parliament (Einaudi 1948). As a result, the election helped establish foreign election manipulation as a viable foreign policy tool and instilled US confidence in the method (Miller, 2006). The expansion of Communism motivated the US to establish a more aggressive foreign policy, ultimately leading to an increased frequency of election manipulation.

The US spent an estimated total of over $1 million on campaign funding in the 1948 Italian election (Agrawal, 2016). Moreover, covert funding and manipulation efforts did not end with the conclusion of the 1948 election. Approximately 44.4 percent of election manipulation cases are repeat interventions 71 percent of which take place in consecutive elections (Levin, 2016). Repeated intervention attempts in Italian elections would occur for the next 24 years (Kapur & Saradzhyan, 2017). If we include all US election influence attempts on Italian elections, the total amount of funding increases to $75 million (Goldman, 2015).

Defamation Campaigns and "Fake News"

In contrast to the US, the Soviet Union primarily employed propaganda and defamation campaigns designed to create public scandals and influence public sentiment during elections. The Soviet Committee for State Security (KGB) created a special division, Service A, whose

duties consisted of producing false documents, creating propaganda, spreading misinformation, and interfering in Western public diplomacy efforts (Kramer, 2017). It is estimated that Service A employed over 15,000 officers to perpetrate misinformation campaigns during peak Cold War tensions (The Economist, 2016). Service A was heavily tied to interference efforts within the US during the Cold War. In 1982, the KGB employed "active measures" against Ronald Reagan's reelection campaign and began promoting the slogan "Reagan means war!" (Osnos, 2017). Service A also deployed efforts to validate US conspiracy theories and undermine citizen trust in the US government. These efforts included promoting and funding publication of conspiracy theories suggesting CIA involvement in the Martin Luther King Jr. and John F. Kennedy assassinations, or that the Pentagon developed the HIV/AIDS virus (Osnos, 2017).

Throughout the Cold War, one of the Soviet Union's most strategically important targets was West Germany. The Soviets viewed West Germany as a critical "door to the West" and central in the debate over US military bases and missile deployment (Daniels, 2017). The Soviet Union deployed covert interference attempts to sway public opinion concentrated on the stationing of US-operated nuclear weapons in Europe. The Soviet Union did not initiate the European anti-nuclear movement, but its onset provided the Soviets with an opportunity to exercise its own agenda on a public platform. Soviet efforts to aid the anti-nuclear movement consisted of formulating "front organizations" to spread their messages (such as the World Peace Council) and targeting European grassroots peace movements that opposed the placement of nuclear weapons in Europe (Daniels, 2017). The Soviet Union's propaganda displayed NATO and the US as the primary perpetrators of world tensions and simultaneously deemphasized the impending security threat of the Soviet Union. The propaganda campaign consisted of misinformation strategically published in the press, and construction of forgeries of NATO and US documents. The US attempted to counter the effect by exposing its covert nature and circulating declassified documents to the public and allied governments (Weiss, 2017).

The US also utilized misinformation propaganda in an effort to influence an election outcome. Both the US and Soviet governments engaged in propaganda efforts during the Indonesian elections of 1955. Indonesia occupied a critical geographic location in the Pacific region, making its election of interest to both superpowers (Cavanough 2016). The US deployed misinformation tactics to alter public perception and ultimately discredit Indonesia's first democratically elected president, Sukarno (Gup, 2000). In addition to covertly funding rebel

paramilitary factions, The US circulated fabricated compromising photos and pornographic videos with a man wearing a mask with Sukarno's features, exploiting Sukarno's womanizing reputation (Gup, 2000). The video was designed to portray Sukarno in a compromising position with a female KGB officer and illustrate to the public that the Soviet Union exercised control and influence over the president. The Soviet Union struggled to counter the fabricated material and attempted to blackmail Sukarno with a legitimate sex tape (Lister, 2012). While neither influence attempt was successful, the US ultimately discarded the propaganda campaign and diverted efforts into a coup that resulted in the placement of the Suharto regime. (Cavanough, 2016)

Agreements Related to Election Interference

The only international accords that directly address, or can be interpreted to address, the regulation of election manipulation are the Charter of the United Nations (UN Charter) and The International Covenant on Civil and Political Rights (ICCPR). The ICCPR acts as a multilateral human rights treaty within the International Bill of Human Rights (UN Resolution 217), alongside the Universal Declaration of Human Rights.

The UN Charter establishes restrictions on actions designed "to intervene in matters that are essentially within the domestic jurisdiction of any state." (UN Charter Art. II) Furthermore, in 1965, the UN adopted Resolution 2131, stating that, "No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal […] affairs of any other State." It also establishes a state's "inalienable right to choose its political, economic, social and cultural systems without interference in any form by another State." Signatory states of the ICCPR are committed to "genuine, periodic elections" without "unreasonable restrictions." Additionally, Article 20 of the ICCPR specifically prohibits the use of propaganda for wartime purposes, as a violation of human rights (Van De Velde, 2017). However, these statutes lack oversight and enforcement mechanisms to hold nations accountable for violations.

The International Court of Justice (ICJ) case of "Military and Paramilitary Activities in and Against Nicaragua" (Nicaragua v. United States) is a unique instance in which a nation has sought action against election interference through international law enforcement mechanisms. Nicaragua charged the US with violating international conventional laws through attempts to manipulate presidential elections by financing, training, and arming the Contras. Additionally, Nicaragua accused the US of employing direct attacks on shipping ports and oil installations, resulting in damage to the Nicaraguan economy (Briggs 1987). Nicaragua contended these

actions violated The Treaty of Friendship, Commerce and Navigation, which regulates trade between Nicaragua and the US (Desierto, 2017). The US rebutted these charges and stated their actions were to ensure "collective self-defense" of El Salvador against leftist guerrillas backed by the Nicaraguan government (Lewis, 1986). Ultimately, the ICJ upheld the charges and ruled the US "violated the sovereignty" of another state through intervention in its affairs. This treaty ensured that its signatories would not "interrupt peaceful maritime commerce". As a result, the ICJ required the US to pay Nicaragua reparations of $17 billion for damages caused by US supported military attacks (Lewis, 1986). However, the US contested the ICJ's jurisdiction and failed to reach a settlement with Nicaragua (Castillo, 2011).

Conclusion

While the US and the Soviet Union were responsible for the majority of election manipulation activity, they were not exclusive in carrying out election interference. It is important to note that election interference is not exclusive to the two superpowers. In several instances, election manipulation has been used as a tool in regional conflicts in order to secure national security, gain geopolitical advantages and expand a nation-state's scope of influence. For example, Iran interfered with the 2010 Iraq election through convert funding of political campaigns (Ignatius, 2010) while China attempted to influence the Taiwanese elections of 2012 through defamation efforts (Chou 2011).

Election manipulation operations have been used by nations through covert funding, disinformation and propaganda since the Cold War. State-sponsored election interference has merely evolved its tactics to operate on social media platforms, as well as develop their individual cyber capabilities (Van De Velde, 2017). In theory, there are international protections against election interference and manipulation. However, the severe lack of oversight and absence of specific classifications for election interference leads to weak enforcement. The incorporation of cyber capabilities and Internet-based interference methods acts to exacerbate this issue.

Case Study: Brazil

By Alexander Hall

Brazil is a country where Internet-based election interference has altered election results on a municipal scale and has manipulated online political discourse on a national level. Meddling observed in Brazil includes the spread of misinformation, the use of computational propaganda, online communities, and the alteration of municipal election results in Rio de Janeiro. Interference operations come mostly from domestic sources such as private media companies and politically motivated volunteers. With the October 2018 general election approaching, the security of Brazil's electronic voting system remains in question and the country's active online community is expected to play a major role in determining the outcome of the election.

Table 2: Election Interference in Brazil	
Election Infrastructure	
Government Hacking	Y
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	Y
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	Y
Online Communities	Y
Election Manipulation Actors	
Brazil's manipulation actors include both paid trolls and bot operators as well as politically motivated volunteer activists.	

Recent Election

Brazil holds presidential elections every fourth year with the last one occurring in 2014 and the next scheduled for October 2018. Brazil's presidential election in 2014 was polarizing and exacerbated existing public distrust of the government (Matoso, 2015)[1]. Prior to the 2018 election, four parties hold significant power. The center-right Brazilian Social Democratic Party (PSDB) currently leads the governing coalition while the center-right Brazilian Democratic Movement (MDB) and the leftist Workers' Party (PT) also possess significant representation (Arnaudo, 2017).

[1] All material in Portuguese covered in this section was translated by Alexander Hall.

Background Context

While President Dilma Rousseff's successes in promoting economic growth helped her maintain a 71 percent approval rating following her reelection in 2014 (Matoso, 2015), PT and its two former presidents, Luiz Inácio da Silva (Lula) and Rousseff, have been vilified by the Brazilian middle and upper classes for corruption, while defended by the working and impoverished classes. President Rousseff was impeached in 2016 for transferring money between government accounts without congressional approval (Weisbrot, 2018). However, since these actions were commonplace under her predecessors and not illegal, the impeachment can be viewed as a political power play, rather than a crackdown on corruption.

Lula has experienced a similar treatment by Brazil's judiciary. A frontrunner in the upcoming 2018 presidential elections, Lula was convicted of using public money to fund a beachside apartment complex in the state of São Paulo. Lula, once a widely revered figure in Brazil, has become a major representative of the country's corrupt political climate. He was sentenced to nine and a half years in prison in a special hearing as part of an anti-corruption campaign called Operation Lava Jato. Many of Lula's supporters claim the judge's bias was a major reason for his conviction. (Weisbrot, 2018). The verdict bars Lula from running and gives momentum to rivals such as far-right candidate Jair Bolsonaro. Despite accusations of bias, Moro's Lava Jato has also convicted conservative politicians as well as others from across the political spectrum (Wroclavsky, 2015).

For all the controversy surrounding Brazil's politicians, the country's electronic voting system attracts less criticism. Brazilian elections are largely carried out smoothly with few appeals of results (Avgerou, 2013). According to a 2017 poll, only eight percent of Brazilians approved of the current government, while 81.5 percent of the population trust the nation's electronic voting systems (Avgerou, 2013). Additionally, 52 percent had positive views of the nation's military police and 83 percent of the poll's respondents believed that corruption has worsened since Rousseff's impeachment in 2016 (Holmes, 2017). Lack of faith in the government, widespread perception of increasing public corruption, and comparatively high approval rating of the nation's military police makes for a 2018 election environment that could support a drastic change in several directions, including one towards increased military power (Bergamasco et al, 2018).

Pre-election polling for the October 2018 election shows the emergence of right-wing military sentiment. According to a recent poll conducted by Datafolha, the leading eligible contender following former president Lula's conviction is pro-military candidate Jair Bolsonaro of the Social Christian Party (PSC), who is polling at 20 percent (Boghossian, 2018). Bolsonaro has the most significant presence on social media among the candidates and possesses an extremely active online following (de Lara, 2018).

Election Infrastructure and Policy Background

Brazilian presidential elections feature a two-round system, where the second round is a run-off. The upper house of Congress is elected through a winner-takes-all system, where a candidate is only required to obtain a plurality of the votes rather than a majority. The lower house is elected through an open list system where seats are allocated in accordance with their party's vote counts (Avgerou, 2013).

Brazil adopted electronic voting systems in 1996 as a solution to reduce voter fraud and election corruption. The systems were first tested during the 1996 municipal elections in state capitals and during the 1998 general elections in cities with more than 40,000 inhabitants (Avgerou, 2013). In the 2000 municipal elections, electronic voting became the universal election method. The Superior Electoral Tribunal (TSE) is in charge of running the electronic systems. Regionally, Regional Election Tribunals (TRE) oversee elections. The TSE and state-run TREs are responsible for governing the electronic election infrastructure (Avgerou, 2013).

The systems however, are vulnerable in several areas. The TSE tries to hide these weaknesses (Mari, 2014). The voting machines' susceptibility to tampering has frustrated many in the Brazilian Cybersecurity community. Professor Diego Aranha, for example, claims that since the Brazilian machines do not produce a physical receipt of the vote, they are susceptible to manipulation (Mari, 2014). TSE banned public testing of their voting machines after Aranha's findings in 2012. Aranha claims this ban is because Brazil likes to portray itself as a global power and electronic voting is something they can lead the world in (Mari, 2014).

The government, however, lifted the ban on public testing of the machines in 2017 and invited Aranha back to test the integrity of the machines (Alessi, 2018). The cryptology expert found many of the same problems that he discovered during his last test in 2012 (Alessi, 2018). These findings included the fact that a potential hacker had full control upon hacking the system and that the only thing stopping them would be time and the hacker's dedication to the task

(Alessi, 2018). Following the tests, Aranha stated that physical receipts of voting are more necessary than ever (Alessi, 2018).

Election Infrastructure Meddling

While Brazil has taken steps to protect its systems from cyberattacks, its electronic voting machines have been accessed and tampered with at least once, and fears of tampering in the upcoming elections persist.

Government Hacking

Although Brazil's electronic voting machines have proven to be vulnerable, there has only been one successful case of hacking into the voting network. During the 2012 municipal elections in Rio de Janeiro, a group of independent hackers was able to infiltrate the TSE's voting system and alter results (Carolina, 2016). The leader of the group says that he and his colleagues possessed privileged access to the Internet service provider company *Oi* (Silva, 2013). Oi was in charge of providing infrastructure for Rio's electoral committee (Silva, 2013). There has been no public investigation carried out on the issue (Carolina, 2016).

Brazil's election networks, run by TSE, were estimated to receive 200,000 cyberattacks per second in the run-up to the 2014 elections ("Brazil Court Dismisses Hacker", 2014). Then TSE president José Dias Toffoli claimed that in 2014, the TSE's Internet security mechanisms were well equipped to handle election hacking through the Internet ("Brazil Court Dismisses Hacker", 2014). Still, several candidates in the presidential election including current frontrunner, Jair Bolsonaro, are pushing for voting receipts in fear of election fraud (Alessi, 2018). In 2015, the Brazilian Congress approved a measure mandating the production of a physical receipt from voting machines. Despite its approval, the prosecutor general overruled the bill on the grounds that it would cost over five billion reais and violate the anonymity of the voter (Alessi, 2018). The use of voting receipts in the upcoming election is still being debated (Alessi, 2018).

Social Media Meddling

Brazil's size gives the country major influence over the Internet in Latin America. 66 percent of Brazilians have Internet access, and 87.7 percent of Brazil's Internet-connected population is social media users, the second highest percentage in the world (Kemp, 2017). Brazil possesses the third highest number of Facebook users as well as the sixth highest number of users of Twitter worldwide, numbering around 18 million (Kemp, 2017).

Fake News and Rumors

Fake news is rampant in Brazil and the Brazilian government has taken measures to prevent its dissemination. Around 92 percent of Brazilians believe that the spread of fake news could have a serious effect on their country, a rate higher than countries such as the United States, Germany, and France (Cakebread, 2017). Misinformation was commonplace during the impeachment of Dilma Rousseff and is expected to play a major role in the 2018 elections (Gragnani, 2017). Throughout President Rousseff's impeachment process, Brazilians took to social media to voice their opinions. This online discourse, however, was greatly influenced by lies and false information. During the week leading up to the impeachment decision, three of the top five articles about Dilma Rousseff on Facebook were false (Cakebread, 2017). When Rousseff was reelected in 2014, she was extremely popular with a 71 percent approval rating. However, at the time of her impeachment, her approval rating was a mere nine percent (Matoso, 2015). Although Rousseff made mistakes and played into her own downfall, her impeachment and the discourse surrounding the process was owed in part to the spread of fake news.

Fake news about Rousseff was also spread through WhatsApp, a messaging application owned by Facebook (Kulwin, 2018). As the messages from WhatsApp are encrypted, it is extremely difficult to track the spread of fake news and determine how many people it reaches (Funke, 2017). It is common to share political articles on WhatsApp through large family groups, sometimes containing as many as 100 people.

Brazil has started to take action to combat fake news in the lead up to the 2018 election. In January, the Brazilian congress passed a bill that legalized the removal of posts and accounts that contain or propagate fake news (Downie, 2018), mirroring similar actions taken in Germany. However, the law passed in Brazil is unlike that of its European counterparts in that it delegates the power to determine what is fake news to the military police (Downie, 2018). Further, the precedent providing grounds for the bill was a law used in the 1960's and 1970's by the military dictatorship to suppress dissent (Downie, 2018).

As the 2018 election approaches, there is likely to be a heated online discourse that includes fake news (Arnaudo, 2017). On February 28th, the TSE entered into negotiations with Facebook, Twitter, WhatsApp, and Google with hopes of turning them into effective partners in the fight against online fake news (Londoño, 2018).

Bots

In the 2014 general election, both Rousseff and her opposition's campaigns employed social media campaigns that included automated social media accounts (Arnaudo, 2017). These bot-driven accounts are known as computational propaganda, and were used to both amplify the views of candidates and disseminate "fake news" (Arnaudo, 2017).

Although Brazil has laws against using computational propaganda as a method of campaigning, they are rarely enforced. The law is also ambiguous on whether campaigns are permitted to hire proxies to make the bots for them.

Rousseff's main opponent in 2014, Aécio Neves, had a significantly greater number of bots (Arnaudo, 2017). Neves' campaign spent more than 300 million reais to a Rio de Janeiro-based company named FaceMedia to develop their social media brand (Gragnani, 2017). The Neves campaign and FaceMedia maintain that the payment was solely for improving their social media brand (Gragnani, 2017). However, several ex-employees of FaceMedia have recently come forward to confirm the creation of fake Facebook and Twitter profiles (Gragnani, 2017).

Neves' computational propaganda connections were able to continue to work after the election, while they were illegal for a sitting president to have them (Arnaudo, 2017). This continued propagation of hostility towards Rousseff continued to highlight existing animosity and exacerbate the negative perception towards her future impeachment proceedings.

Troll Armies

Troll armies are poised to have a large impact in the 2018 election. Organized troll armies have increased in number and have offered their social media services to assist candidates online, suggesting a drastically more significant impact on the outcome of the 2018 elections compared to 2014 (Gragnani, 2017). University of São Paulo public policy professor Pablo Ortellado, believes that the role of computational propaganda and troll armies will rise and that Brazilian political figures will exploit the polarization and volatility of the partisan atmosphere in the country (Gragnani, 2017).

Online Communities and Meme Factories

Online communities are expected to play a major role in online discourse surrounding the 2018 presidential election. Facebook groups such as *Jair Bolsonaro Presidente 2018,* which has nearly 850 thousand likes, curates Bolsonaro's stances and speeches, making them seem mainstream (Fagundez, 2017). This group has been extremely active in combating criticism of Bolsonaro on Facebook and WhatsApp by arguing with critics online. Bolsonaro's followers

operate by propagating memes, giving him the moniker, “Bolsomito” (Bolso-myth) for his relative lack of corruption compared to other Brazilian politicians (Bergamasco et al, 2018). On January 9, 2018, Bolsonaro’s online army swarmed SBT journalist Rachel Sheherazade online after she wrote a highly critical article about Bolsonaro (de Lara, 2018). She received more than 3,800 tweets attacking her (de Lara, 2018).

Conclusion

Understanding Brazil’s election process and political discourse is vital to grasp how that discourse can be altered in a highly connected society where social media is deeply ingrained. The lack of definite laws regarding the use of computational propaganda and the intervention of the military police to weed out fake news could alter the landscape of political discourse on the Brazilian Internet. Additionally, the vulnerabilities in the electronic voting machines also show us the necessity of maintaining the integrity of those machines through advocating for voting receipts and creating redundancies in public election results. Although these issues are not unique to Brazil, by studying election interference in South America’s largest nation, we can gain a perspective on how to better preserve democratic discourse and election methods elsewhere.

Case Study: Bulgaria

By Conor Cunningham

Internet based election interference in Bulgaria had an unknown effect on the 2016 Bulgarian presidential elections and the 2017 Bulgarian parliamentary elections. Interference included attempts to influence social discourse through fake news and troll armies. Interference operations were likely sourced from Russia, pro-Russian domestic actors in Bulgaria and, to a lesser degree, Turkey**.** Extensive misinformation and disinformation campaigns are evident throughout Bulgaria, but to what extent they affect the way Bulgarians vote is difficult to infer.

Table 3: Election Interference in Bulgaria	
Election Infrastructure	
Government Hacking	No
Political Hacking	Yes
Government Website Hacking	No
Election Systems Hacking	No
Social Influence Operations	
Fake News	Yes
Bots/Computational Propaganda	Yes
Troll Armies	Yes
Online Communities	No
Election Manipulation Actors	
Russian Federation Bulgarian citizens Turkey	

Recent Election

Bulgaria held a presidential election in 2016 and a parliamentary election in 2017. The major actors in the 2016 presidential elections were the Bulgarian Socialist Party (BSP), who supported Rumen Radev, and the Citizens for European Development of Bulgaria (GERB), represented by Tsetska Tsacheva. The BSP is a left-wing socialist party that is pro-Russian. The GERB is a center-right party that is pro-EU (Hill, 2017).

In the 2016 election, Radev won by a large margin, acquiring 59 percent of the vote to defeat the Tsacheva, who had just over 35 percent of the vote ("Bulgaria PM Borisov Quits", 2016). The election led to the resignation of Prime Minister, Boyko Borisov. Following the BSP's victory in the 2016 election, the 2017 parliamentary elections, in contrast, resulted in a plurality for the GERB with the BSP coming in second place. After the BSP's large victory in

the presidential elections, the parliamentary elections showed a transition back towards pro-EU policies (Toshkov, 2017). Borisov, again with the GERB, won the 2017 election. Rumen Radev was a political novice whose support came from dissatisfied Bulgarians and whose platform revolved included building closer ties to Russia and a promise to push the EU to lift sanctions on Russia, policies that resonate with Bulgarians because of cultural, historical, and economic ties to the country. The BSP also gained support because of the failure of the GERB's previous administration to overhaul the judicial system and weed out corruption (Bechev, 2016).

Following Radev's failure to form a governing coalition, early parliamentary elections were scheduled in 2017. The 2017 parliamentary election marked a win for the GERB party who won 33.54 percent of the vote, while the BSP received 27.93 percent. Following the election, GERB formed a governing coalition with the United Patriots, a right-wing political coalition (Barzachka, 2017). This coalition marks the first time in Bulgaria's post-communist history that a right-wing party was included in the government (Barzachka, 2017).

The plurality gained by the GERB signified the intention of Bulgaria to maintain a commitment to the EU in 2017. The GERB success was also seen as a loss for Russia because it challenged Russian influence in Bulgaria and the Balkan region (Dzhambazova, 2017).

Background Context

Bulgaria's close historic ties with Russia play an important role in Russia's interest in the region. Unlike many post-communist states that maintain resentment towards Russia, Bulgaria has a more positive opinion of Russia partly due to its role in Bulgaria's independence from the Ottoman Empire (Sofia, 2017). As the poorest and most corrupt member of the EU and a state that has failed to be fully integrated into the EU system, high levels of nostalgia for the People's Republic of Bulgaria are present (Biray, 2015). For Russia, Bulgaria is a valuable strategic player. Between 2005 and 2014 Russia's economic presence in Bulgaria averaged 22 percent of Bulgarian GDP (Walcott, 2016). Bulgaria also allows Russia a place to promote a pro-Russian agenda within the EU. In 2006, a permanent representative to the EU from Russia called Bulgaria the Russian "Trojan Horse in the EU" (Naydenov, 2017).

Significant minorities of Bulgarians are of Turkish descent, amounting to about eight percent of the population. Many Turkish Bulgarians live abroad in Turkey or elsewhere in the EU but remain voting citizens.

Election Infrastructure and Policy Background

Bulgaria has a democratic system of government with a prime minister, who is the head of the government, and a president, who is the head of state. Every citizen is allowed to vote in Bulgarian elections except for prisoners and those deprived of legal capacity by a court decision. The European Court of Human Rights found that voting restriction to be a violation of the European Convention on Human rights (ODIHR, 2017).

The Central Election Commission implements election law, and administers elections with the District Election Commission and the Precinct Electoral Commission (ODIHR, 2016).

Voting in Bulgaria remains strictly by paper ballot. Prior to the 2017 parliamentary election, the Central Election Commission planned to use 500 voting machines throughout Bulgaria. However, this did not come to fruition (ODIHR, 2017).

Election Infrastructure Meddling

Since Bulgarian elections are all done by paper ballot, the possibilities for election infrastructure hacking are lower in Bulgaria than countries using electronic voting. Nevertheless, Russia and Turkey do try to influence electoral procedures.

Leaks through Hacking

The BSP is the successor of the Bulgarian Communist Party and many members still hold close ties to Russia (Parkinson, 2017). Russian Intelligence gave a 30-page dossier that outlined the potential path to victory for the BSP in the upcoming presidential elections in 2016 to the BSP. The dossier included methods such as; releasing false weekly reports exaggerating BSP support and how to buff up the candidate's image through pro-Russian news outlets. In the following election, BSP candidate Rumen Radev won by a large margin (Parkinson, 2017).

Government Hacking

Although there were no reports of direct election infrastructure hacking in Bulgaria's 2016 and 2017 national elections, there were reports of infrastructure hacking in the 2015 municipal elections (The Sofia News Agency, 2016). The content on websites of state agencies and institutions were hacked and sensitive information about individuals and businesses were stolen. Several government websites were replaced with anti-democratic and racial propaganda (The Sofia Globe, 2016).

Social Media Meddling

One of the biggest problems in Bulgaria is the spread of fake news. In 2017, a survey found that 71.5 percent of Bulgarians come across fake news at least a couple times a year

(Tanev, 2017). A quarter of the respondents on the survey indicated that they encountered fake news on a daily basis.

Internet Use Profile

Bulgaria is highly active on social media, especially among younger Bulgarians, even if many Bulgarians continue to use traditional media sources as the most common source of news. In 2017, 67.3 percent of households had Internet access, with 66.9 percent of those households having a fast broadband connection (Leviev-Sawyer, 2017). The five most popular websites in Bulgaria are Google Bulgaria, Facebook, YouTube, Google, and Abv.bg (SimilarWeb, 2018). As of June 2017, there were 3.4 million Facebook users, or 48 percent of the population of Bulgaria (Statista, 2017a). 12 percent of the population also uses Instagram (Statista, 2017b).

Fake News and Rumors

The spread of misinformation is a major problem for Bulgaria. For instance, a story found on the Russian portal Topwar.ru detailed how Bulgarian troops had refused to shoot targets in the colors of the Russian flag when they were expected to do so during a military exercise conducted by NATO (Penev, 2017). The story was picked up by other outlets, crossing to the English version of the Crimean-based website News Front, then also appearing on the Czech news cite Ac24.cz and an independent research organization from Canada known as Global Research Canada (Penev, 2017).

In February 2017, several websites reported that Johannes Hahn, the European Commissioner for European neighborhood policy and enlargement negotiations, had made secret suggestions that the EU would claim Bulgarian territory within 40 years and that Bulgaria would no longer be a country. This story had actually been created in 2013 as a satirical piece by a Bulgarian portal (Penev, 2017). In this case, an article that was clearly written with the intention of not being taken seriously was picked up and spread as something real. The proliferation of fake news has led to civil society projects and independent media such as NOVA television and Mediapool attempting to monitor fake news. Political action targeting fake news has been brought up by several politicians but has yet to come to fruition (Mejdini, 2017).

Fake news appears to play a role in the Russian plan to cripple and divide the EU and exploit areas where Euroscepticism already exists, such as Bulgaria. For younger, educated Bulgarians, fake news and propaganda are easier to spot. However, for uneducated, rural, and older populations, fake news poses a threat because of difficulty discerning the veracity of a

source. Fake news preys on sentiments felt by many Bulgarians who see Russia as a key partner in the present and future (Tanev, 2017).

Troll Armies

Online communities in Bulgaria play a key part in producing and disseminating misinformation. The Bulgarian "Clean Internet" initiative has identified key actors producing and spreading information on Facebook. According to "Clean Internet" a man named Stefan Proynov manages hundreds of sites and Facebook accounts that, together with his associate Adrian Dimitrov, have produced 90,000 posts on social media in the last two years (Bivol 2017b). In an interview, Stefan claimed that they had actually spread closer to 200,000. Proynov argues that his trolling campaign is completely personal, claiming that the GERB ruined his business and life. Besides anti-GERB rhetoric on his accounts and websites, he also promotes pro-Putin, anti-Roma, anti-immigrant, nationalistic slogans, and pro-BSP messages (Bivol, 2017a).

Other: Ethnic Turkish Citizens Voting Abroad

Besides Russia, Bulgarian officials believe that Turkey attempts to influence elections in Bulgaria. Nearly half a million Bulgarian citizens, mainly of Turkish descent, live abroad in Turkey. Most of these citizens support the ethnic-Turkish party Democrats for Responsibility, Solidarity and Tolerance, a party often referred to as Turkey's Trojan horse in Bulgaria (Theresheva, 2017). Turkish officials have openly supported candidates from the Democrats for Responsibility, Solidarity, and Tolerance.

Conclusion

The presidential elections in 2016 and parliamentary elections in 2017 show contrasting political outcomes, however both elections were surrounded by large and increasing amounts of fake news. Misinformation spread during the election proved to be largely pro-Russian, anti-democratic, anti-EU, and anti-immigrant. This information did not only come from Russian websites, but was also created by Bulgarians who supported the message being spread. The degree to which misinformation impacted the election is unclear, however BSP was unable to succeed in the latter elections.

Bulgaria must make moves to combat fake news being spread around the country. The extensive use of misinformation is likely to continue to generate dissatisfaction among Bulgarians. Furthermore, the introduction of electronic voting machines in the near future will add another tool for political actors to influence elections.

Case Study: France

By Ashley Sawyer

Internet based election interference did not have a significant effect on the 2017 French Presidential Elections. Interference included attempts to influence social discourse through fake news, social media bots, troll armies, online communities, and direct cyberattacks against election infrastructure and political parties. Interference operations were likely sourced from the Russian Federation, as well as international and domestic partisan communities. Election meddling has led to an investigation and increased public discourse on national security.

Table 4: Election Interference in France	
Election Infrastructure	
Government Hacking	N
Political Hacking	Y
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	Y
Online Communities	Y
Election Manipulation Actors	
Russian Federation Domestic Partisan Communities International Partisan Online Communities	

Recent Election

The most recent French Presidential election was held in May 2017. In that election, La République En Marche! (En Marche!) Candidate Emmanuel Macron won with 66.1 percent of the vote against his opponent, National Front Candidate Marine Le Pen (Aisch et al., 2017). While Macron won the majority vote, he became the leader of a deeply divided nation. Le Pen's anti-European Union (EU) and anti-immigrant platform gained support in the Northern and Southern regions of France. Major issues in the election included unemployment, economics, workers' rights, globalization, immigration, the refugee crisis, secularism and France's participation in the EU (El Amraoui & Safdar, 2017). Le Pen did particularly well where the unemployment rate was above 12 percent. Macron, however, won across multiple demographic

groups, including urban, rural, highly employed and highly unemployed areas (Aisch et al., 2017).

Dissatisfied with the political landscape in France, Macron founded the political party En Marche! in 2016. En Marche! has been regarded as an overall centrist party, but with leftist social policies and a liberal approach to economic policies (Gillett, 2017). On the contrary, the National Front (in French, Le Front Nationale), is considered to be a far-right party with conservative policies and ideologies (Branford & Nowak, 2017). The distinct differences between the two candidates led to controversy on the campaign trail.

Major controversies during the election included claims by Le Pen that Macron was harboring money in offshore accounts; Le Pen eventually used this claim, which originated within online communities, against Macron during a presidential debate (Rumeur sur en prétendu, 2017).[2] The sources of Le Pen's campaign funds also came into question; specifically, financial ties have linked Le Pen to Russian lending sources. French banks refused to lend the National Front funds for Le Pen's campaign; therefore, Le Pen sought to gain a loan from a Russian bank, which gave her €9 million (Vinocur, 2017). Russian media outlets have frequently praised Le Pen while continuously spreading rumors of Macron's sexuality and other unsupported claims (McAuley, 2017).

Background Context

A 2017 poll found that 80 percent of French citizens do not have satisfactory trust their government (Wike et al., 2017). 65 percent of the French population is not satisfied with the way that democracy is working in their country (Wike et al., 2017). Among those surveyed that support the National Front, 71 percent said that they did not trust their government at all. Among those surveyed that *did not* support the National Front, 35 percent said that they did not trust their government at all (Wike et al., 2017).

Election Infrastructure and Policy Background

Elections in France are structured around a two-round election system, which uses paper ballots. When someone turns 18, they are automatically registered to vote. Criminals are allowed to vote in prison by using a proxy, except for certain types of sentences (Législatives Assemblée Nationale, n.d.). When voting, French citizens go to their assigned voting districts and vote using paper ballots, which are counted manually. At a voting station, the voter enters a booth, marks

[2] All French content in this case study was translated by Ashley Sawyer

their ballot and inserts it into an envelope. After casting their ballot, the voter signs the "voters list," and their voter registration card is stamped, signifying that they have voted (Code Électoral, Art. L58).

Election Infrastructure Meddling

The 2017 French Presidential Election was the victim of election infrastructure meddling in the form of leaks through hacking. Furthermore, significant concerns of voting machine tampering emerged. These tactics had little to no effect on the outcome of the vote, but instilled fear in the integrity of the election in many French voters ("France Drops Electronic Voting", 2017).

Leaks through Hacking

In the 2017 French Presidential election, leaks of political documents were used to attempt to meddle with the outcome of the vote. En Marche! was hacked in 2017, after which a large cache of files was posted on Pastebin, an anonymous file sharing website, under the title EMLEAKS (Mohan, 2017). The post occurred hours before voting stations in France were set to open (Willsher & Henley, 2017). Within the leaked information were tens of thousands of campaign emails and documents, some of which were falsified (Willsher & Henley, 2017). The falsified documents were included with legitimate ones in an effort to cast the Macron campaign as involved in questionable campaign activities, such as fraud (Willsher & Henley, 2017). Although it has not been proven, this hack is thought to have come from the Russian Government (Hosenball, 2017).

Attempts were made to hack into Macron's campaign through Facebook (Sharkov, 2017). Russian operatives attempted to pose as "common acquaintances" of Macron and En Marche! workers in hopes of obtaining information about Macron's personal life and phishing for En Marche! campaign materials (Sharkov, 2017). Attempts to have Macron's associates download tainted software were unsuccessful (Sharkov, 2017).

Evidence suggests that hackers, with potential links to the Russian Government, orchestrated the attacks (Hosenball, 2017). Following 2014 sanctions on Russia by the EU, Russia has held an anti-EU stance (Hosenball, 2017). Le Pen, who is known for her anti-EU rhetoric, would be favorable leader of France for Russia (Hosenball, 2017).

Voting Machine Tampering

During the 2017 French Presidential election, there was no evidence of voting machine tampering. Voting machines were introduced to the French public for the 2007 Presidential

Election; to test the public's response, the machines were placed in 86 of France's 36,000 voting districts (Crampton, 2007). The implementation of these machines, however, was met with fierce backlash. Many citizens thought that the machines inhibited the democratic principles of the vote, which had historically been done through paper ballots (Crampton, 2007). Critics argued that voting machines did not promote an open and transparent election; therefore, the machines did not instill public confidence (Crampton, 2007). As a result, France's Minister of the Interior decreed a moratorium on the buying and implementation of new voting machines in the same year they were introduced (Tanneau, 2017). Consequently, the 2012 Presidential Election saw a decrease of voting districts utilizing voting machines (Tanneau, 2017). The practice continued into the 2017 Presidential Election, in which 64 of 36,000 utilized the voting machines; these 64 districts contain approximately five percent of French voters (Tanneau, 2017). The remaining voting districts use only paper ballots.

Social Media Meddling

The 2017 French Presidential Election was the center of multiple social media meddling operations, particularly on Twitter. The French public, which almost entirely has access to the Internet, was targeted by large amounts of fake news stories, Twitter bots and online troll armies. Discussions fostered in online communities, such as 4chan, often targeted the candidates and attempted to slander their reputation (Broderick, 2017).

Internet Use Profile

The Internet is used widely across France; 83.8 percent of French citizens use the Internet regularly (UNdata, n.d.). In France, the most popular social media site is Facebook, used by 37.89 percent of Internet users. YouTube, Twitter, Google+, and LinkedIn follow Facebook, respectively (Statista, n.d.).

Fake News and Rumors

The 2017 French Presidential Election was plagued by continuous fake news stories. These stories, many of which originated from within online communities, gained attention leading up to the both rounds of voting. With the help of social media sites as a platform, particularly Twitter and Facebook, fake news stories spread quickly and efficiently.

One popular fake news story suggested Macron was harboring funds in an offshore account in the Bahamas. Two fake documents, alleged to be Macron's tax statements, were posted to 4chan message board /pol/, which stands for "politically incorrect" hours before a televised presidential debate (Rumeur sur en préntendu, 2017). Twitter accounts, heavily

suspected to be bots, tweeted in English throughout the debate; the accounts urged Twitter users to use #MacronCacheCash in an effort to discourage voters from voting for Macron (Rumeur sur en préntendu, 2017). The falsified documents eventually caught the attention of Le Pen's campaign; Le Pen then included the information against Macron in the debate.

Following the attack, Macron issued a complaint, which prompted the Paris Prosecutor's Office to open "…a preliminary investigation for 'false news with a view to divert the votes, false, use of forgery and concealment of false'" (Rumeur sur en préntendu, 2017).

Bots

During the 2017 French Presidential Election, bots quickly spread fake news and information regarding the En Marche! hack, particularly on Twitter. The news of this document leak was spread quickly through the use of bots. Within an hour of the Pastebin release, the hack was recirculated through /pol/ (Mohan, 2017). From /pol/ it was picked up by Jack Posobiec, an American far-right journalist who writes for Canadian outlet *Rebel Media* (Mohan, 2017). On his twitter page, Posobiec advertised the document dump on /pol/, and labeled the tweet #MacronLeaks. Posobiec's tweet received attention immediately; "[The tweet] was reportedly retweeted 87 times in the first five minutes, suggesting… that the message was being boosted with the help of bots" (Mohan, 2017). Posobiec's post went viral, and EMLEAKS gained significant momentum. Several alt-right Twitter accounts, mostly in the US, began to notice Posobiec's tweet, and it was spread quickly through the use of bots.

The attention on 4chan and Twitter caused WikiLeaks to take notice of EMLEAKS. WikiLeaks tweeted, stating "Alleged multi-GB team Macron email archives. Could be a 4chan practical joke. We are examining" (Mohan, 2017). Prior to WikiLeaks' tweet, #MacronLeaks was being spread mainly among English-speakers not located in France. However, following WikiLeaks' tweet, #MacronLeaks began to spread in French twitter accounts. By Midnight Saturday May 6, #MacronLeaks garnered more than 47,000 tweets and had begun to trend in France. By late Saturday morning, the day voting began to take place, #MacronLeaks was trending worldwide (Mohan, 2017).

Macron and his campaign, however, were unable to fight back. French election code is strict on strategies candidates can use while campaigning, and requires a complete halt of campaigning before voting begins; due to the timing of the leak, Macron and his campaign didn't have adequate time to respond to the leak before the campaigning deadline. However, there also

wasn't a lot of media coverage of the leak from within France itself. France's Electoral Commission warned media outlets not to cover the leak, stating "…that journalists could face criminal charges for publishing or republishing the material, under laws that came into effect at midnight forbidding any commentary liable to affect the presidential race" (Deardon, 2017).

Troll Armies

Throughout the election, the Russian Federation was alleged to have supported troll armies assigned to promote anti-Macron and pro-Le Pen rhetoric online (Nougayrède, 2017). Evidence of personal connections between Le Pen and Konstantin Rykov, a Russian that was formerly employed by the Russian Government for propaganda purposes, has emerged (Vinocur, 2017). Rykov is considered to be a very prominent social media activist in Russia, and during the campaign, he ran a pro-Le Pen, pro-Russia and anti-Macron Twitter account that posted in both French and Russian (Vinocur, 2017).

However, most trolling was run by Le Pen's campaign. Groups gathered on Twitter to spread coordinated messages and hashtags; Twitter users that interact and sympathize with the troll accounts were often contacted individually (Vinocur, 2017). Gaëtan Bertrand, Le Pen's online campaign coordinator, stated that the Le Pen campaign often interacted with trolls and helped supply information they could promote on social media (Vinocur, 2017).

Online Communities and Meme Factories

Throughout the 2017 French Presidential Election, multiple rumors about candidates, fake news and memes emerged from 4chan. An anonymous 4chan user called on the alt-right users to engage in a "Total Meme War" in support of Le Pen; following this call to action, multiple memes, including Pepe the Frog, a character that has been tied to anti-Semitic values, began to circulate on the Internet (Scott, 2017). These memes would often come with anti-Macron messages.

Fake quotes attributed to Macron were created to make him look soft and indifferent on terrorism; 4Chan users attempted to use the news of the 2016 Paris terrorist attack against Macron (Broderick, 2017). However, while most stories attacked Macron directly, many rumors focused on his wife and stepdaughter; one popular story was that Macron was having an affair with his stepdaughter (Broderick, 2017).

Conclusion

Election meddling plagued the 2017 French Presidential Election, appearing in the form of campaign hacking, document leaks, fake news, twitter bots, troll armies, and the spread of

information within online communities. However, there is no evidence to suggest that there was any meddling in regards to registration tampering or government hacking. Attempts to influence the election affected the functioning of both the Macron and Le Pen campaigns. However, the meddling had no discernible effect on the outcome of the election. Polling numbers for Macron and Le Pen stayed the same; in some cases, Macron did even better than predicted ("French Election: Macron Takes", 2017). While it is apparent that there were no effects on the election outcome, the attempts to sway the turnout of the election have resulted in an investigation and rising concerns over national security.

Case Study: India

By Vriti Wadhwa

Internet based election interference in India had an unknown effect on the 2014 parliamentary elections. Interference included attempts to influence social discourse through fake news, social media bots, troll armies, and online communities. While there is no evidence of direct cyberattacks against election infrastructure, it has still been proven vulnerable. Interference operations were likely sourced from domestic political candidates and media companies. With the 2014 elections considered as experimental for many methods of election meddling, India's consistent growth in digital populations and online communities leaves room for people to question whether Internet based interference took place. Election interference is a major concern in the upcoming 2019 elections.

Table 5: Election Interference in India	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	N
Troll Armies	Y
Online Communities	Y
Election Manipulation Actors	
Political candidates and Their Followers Paid trolls	

Recent Election

India most recently held elections in 2014 to choose the country's lower house parliament (Baru, 2014). Participating parties included; the Indian National Congress (INC), a secular party led by Rahul Gandhi; the Hindu Nationalist urban-middle class Bharitya Janata Party (BJP) led by Narendra Modi and; the anti-corruption Aam Aadmi Party (AAP), led by Arvind Kejriwal (Burke, 2014a). The elections ended with a victory for BJP's Modi, winning a total of 282 seats out of 543. The Indian National Congress received a historically low 44 seats.

The INC for most of its 54-year democratic history has ruled India, but they have lost much of their reputation due to poor economic performance, corruption, and inflation (Burke,

2014c). In addition, the election saw one of the highest voter turnouts, at 66.4 percent of the population (Mitra & Schottli, 2016). The elections comprised a total estimated 814.5 million eligible voters, with 1.4 million electronic voting machines and 930,000 polling booths (Battacharaya, 2014).

Despite the Modi administration's economic success, his Hindu nationalism has caused controversy between Hindu-Muslim communities. In 2002, when Modi led the state of Gujrat, riots occurred between Hindus and Muslims, killing approximately 1,200 people (Fisher, 2014). During the 2014 elections, Hindu nationalist organization Rashtriya Swayamsevak Sangh (RSS) endorsed Modi, an organization that has been banned multiple times due to political and religious acts of violence.

Background Context

Modi's victory began a new political era in India, a change after the generational rule of the INC since the post-Indira Gandhi years ("Everything you need to know," 2014). Modi's use of social media and campaigning techniques was a fresh paradigm for Indian voters, taking advantage of all media platforms such as television, radio, newspapers, and social media (Palshikar, Kumar, & Lodha, 2017). The 2014 election involved high social media use, with candidates incorporating online strategies into campaigns to win the votes of both rural and urban populations. The change in tactic indicated a transformation in election strategies, boosting digital advertising and an increase in overall Internet use.

The 2014 elections in India had an unexpectedly large increase in turn out because of an increase in young voters, women voters, and rural voters (Mitra & Schöttli, 2016)**.** Roughly 150 million voters were between the ages of 18-23 and particularly focused on more involvement and participation in the government, greater protection for women after sexual violence cases, gay rights, and rising inflation (Bhowmick, 2014).

Election Infrastructure and Policy Background

India is the largest democracy in the world and holds a parliamentary system of government. The Indian voting system is divided into two entities, the Lokh Sabha (House of the People or- lower parliament) and Rajya Sabha (Council of States or- high parliament). India elects members to the Lokh Sabha in five-year intervals. The prime minister is chosen by the Lokh Sabha (Panda, 2014), while the Lokh Sabha and Rajya Sabha, choose the president (Desikan, 2012).

The Election Committee of India (ECI) takes responsibility for the monitoring of electoral processes enumerated in the constitution of India ("Election Commission of India", n.d.). The Election Committee of India allows anyone to vote if they are listed on the electoral roll- a list of people with names that are added to vote after turning 18. These rolls are also computerized, and include photo identity number cards for cross check purposes ("Election Commission of India" n.d.). The Election Committee of India implemented electronic voting machines (EVMs) to help improve voting reliability ("Election Commission of India", n.d.), time management, eliminate bogus voting, make voting accessible for illiterate people, and improve India's environment ("Impact of Electronic Voting in India," 2017). Prior to this, only paper ballots were allowed, introducing the possibility of ballot box stuffing (Anumoom, 2017). In May 2000, the ECI created Electors' Photo Identity Cards, to be given to voters, in order to improve accuracy of the electoral roll and legitimacy of voting machines, which are currently being distributed ("Election Commission of India," n.d.).

Any elector or candidate is allowed to file an election petition regarding forms of election malpractice. The High Court of the State is involved, and outcomes could possibly lead to second elections ("Election Commission of India," n.d.).

Election Infrastructure Meddling

In Indian elections, potential instances of voting machine tampering have occurred, but no cases of election manipulation through the Internet have been found. However, while there is still no evidence of machine manipulation on public record, concerns exist around machine meddling. While rumored events and tests have taken place, the Election Commission of India has dismissed all allegations.

Voting Machine Tampering

Despite no hard case evidence of electronic voting machine tampering during the 2014 election process, there are a significant amount of rumors about potential vulnerability. BJP's opposing candidate, the anti-corruption Aam Aadmi Party, held a live demonstration to the public on May 2014 where a computer engineer illustrated electronic machine vulnerability (Bhatnagar, 2017). The engineer suggested that secret codes can be entered in the machine and completely change the outcome of the vote (Bhatnagar, 2017). During the live event, Bhardwaj demonstrated how pressing on the button for the Aam Admi Party actually made the vote go to

BJP (Bhatnagar, 2017). However, the Election Commission of India said that Bhardwaj tampered with a lookalike machine.

Similarly, University of Michigan professor Alex Halderman led a research experiment to show how connecting a homemade electronic device to an electronic voting machine used in Indian elections allowed him to change votes (Siddle, 2010). Halderman replaced the machine's display board with a lookalike that was attached to a microprocessor and Bluetooth radio, which allowed him to manipulate votes wirelessly (Zetter, 2010).

There have also been cases of machines favoring the BJP in Uttar Pradesh, Kanpur, and Assam state (Pandey, 2017). When voters chose a candidate, the machine would always vote for BJP. However, it is still unclear whether the machines malfunctioned or were intentionally tampered with (Pandey, 2017).

One state elections commission, after studying and testing the machines, suggested it was almost impossible to manipulate the actual manufacturing of voting machines. After doing a Trojan Horse test, the Committee concluded that in order to manipulate a machine a specific key press sequence was needed. Without this, they argued, it is impossible to hack the machine. The committee stated that physically tampering the machine is only possible if the machine's electronic card is physically replaced, but they said this too was unlikely (Election Committee of India, 2007).

To refute allegations of machine tampering, the Election Commission of India announced the use of electronic voting machines with VVPAT. This process has already been initiated in several state elections (Express News Service, 2017).

Social Media Meddling

During the 2014 elections, disinformation operations using social media were common. These methods included fake news, trolls, and meme factories.

Internet Use Profile

India has the second largest number of Internet subscribers globally, after China (Freedom House, 2017). In 2016, there were 460 million Internet users, equivalent to roughly 30 percent of the population, compared to 10 percent of the population in 2011 (Statistica, n.d.). The most popular social networks in India include Facebook (and Messenger), YouTube, WhatsApp, and Instagram (Statistica, n.d.). There were around 195 million Facebook users in India in 2016, the most Facebook users worldwide in an individual country, as of 2018 (Statistica, n.d.).

Even though Internet usage was only 15 percent during in 2014 (Daniyal, 2017), the elections that year demonstrated how social media platforms such as Facebook, Twitter, and WhatsApp have been extensively used as a social space for public discourse (Thorsen and Sreedharan, 2015). Because of an overwhelming presence of media, the Election Committee of India established rules of its usage in campaigns, requesting parties list out social media accounts and declare funds acquired by social media (Thorsen and Sreedharan, 2015).

Fake News and Rumors

Modi's victory in the 2014 elections not only increased social media use, but also accompanied a proliferation of fake news. Almost 700 cases of "paid news" stories were found during the 2014 elections (Indo-Asian News Service, 2014). The Indian media refers to "paid news," as incorrect opinion polls, interviews of political candidates, or press releases (Vyawahare, 2014). Beyond paid news, fake news included allegations that the INC sought Pakistan's help to defeat the BJP.

After the election, fake news circulation increased. Fake news stories have led to acts of violence and even death, including the beating of a man due to a fake WhatsApp message in 2017 (Kumar, 2017). With the rise of Indian Internet connectivity, the rate of fake news circulation is getting worse. Because there is more awareness of the existence of fake news, independent websites like SM Hoax Slayer, Alt News, and BOOM Live have been created to try keep track of fake news posts (Lal, 2017).

Troll Armies

Modi's digital campaign tactics and prominent media presence has led to the rise of troll armies, which help spread BJP ideology. Facebook's global government and politics lead, Katie Harbath, has helped develop Modi's online presence for his political campaigns. During the 2014 elections, Modi heavily relied on Facebook and Whatsapp to gain followers who would help promote him through social media (Etter, Silver, & Frier, 2017). This also meant sending aggressive and harassing messages to Modi's political rivals, journalists, and Muslims. Gauri Lankesh, a journalist critic of Modi who was targeted by trolls on Facebook and other media platforms, was killed in September 2017 - no arrests have been made (Etter et al., 2017).

Modi's Twitter account is known for suspicious activity. Modi's followers are referred to as his "troll army". Modi followers attack minorities, women, journalists, and others opposed to the BJP agenda (Hume, 2018). "Recruiters" have approached Indian Twitter users to promote a party's message and political agenda. The INC has denied allegations that they employ

"Recruiters" and has blamed the BJP instead. Indian journalist Swati Chaturvedi has accused Modi of directing his followers to insult people on digital platforms. Chaturvedi argues that trolls are a significant component to Modi's political agenda, and that Modi's team has a list of targeted people who receive death or rape threats if they don't agree with his viewpoint (Hume, 2018). The BJP has said that their party has never encouraged trolling (Hume, 2018).

Online Communities and Meme Factories

Modi strategically digitized is campaign to the public, especially regarding his speeches and famous phrases that stuck to audiences. This includes the tagline "Abki baar, Modi *sarkar,*" which translates to "This turn, Modi's Government." Soon enough this phrase erupted on the Internet and become a prominent addition to meme culture. Other memes named him as "modern Mahathma" (Thorsen & Sreedharan, 2015)

Conclusion

While there is positive progress in electoral system growth and voter turnout, drastic change in technological advancement could potentially be a platform for new forms of election tampering. Since the 2014 elections, there has been an increase in violence and death threats due to misinformation and the spread of fake news. The Election Commission of India is aware of people doubting India's election credibility, and is trying to implement improved security measures for the 2019 elections. Regardless, significant discussion in India of the potential for election meddling should serve as a signal that election security in India is an issue that should be better addressed.

Case Study: Italy

By Anni Gu

Internet based election interference played a small role in the 2013 Italian General Elections. Interference included attempts to influence social discourse through fake news, social media bots and direct cyberattacks against political parties and the Italian government. Interference operations were likely sourced from the Russian government as well as domestic political parties. Election meddling is playing a small role in Italian politics in the upcoming 2018 general election, which generally instead focuses on the role of politicians on social media.

Table 6: Election Interference in Italy	
Election Infrastructure	
Government Hacking	Y
Political Hacking	Y
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	N
Online Communities	N
Election Manipulation Actors	
Russian government Political parties	

Recent Election

This case study will focus on the 2013 Italian general elections and the upcoming 2018 elections. In that election, the Centre-left coalition lead by the Democratic Party (DP)'s Secretary Pier Luigi Bersani won 29.55 percent of the vote, while the People of Liberty (PdL) received 29.18 percent, and Beppe Grillo's Five Star Movement received 25.55 percent.

Background Context

In 2011, Prime Minister Silvio Berlusconi resigned; his successor, Mario Monti, oversaw a major tax reform and spending reduction. After these austerity measures contributed to financial market failures, public trust in the Italian Government and the EU decreased.("World Heritage Encyclopedia," n.d.). As a result, public trust in democracy dropped significantly, as well as confidence in the EU (Traynor, 2013). In this environment, Beppe Grillo's populist Five

Star Movement (M5S) arose in the 2013 election. By webcasting his criticism of political elites, Beppe Grillo, the founder of the party, gained support from right-wing populists.

Italians' trust in media is consistently low, at 50 percent in 2012 (Traynor, 2013) and 45 percent in 2018. Italian trust in government, is consistently below 30 percent (Edelman, 2018).

The Russian Government has invested in Eurosceptic parties in the 2018 election (Corker, et al., 2018). Compared to the Democratic Party, which support involvement in the EU and was a supporter of EU sanctions on Russia, the M5S is markedly more Eurosceptic. Salvini's Northern League, a member of Berlusconi's coalition, might also propose an Italian-EU exit referendum (Binnie, 2018).

The rise of M5S is connected to its leader's prolific use of Internet media, as a prominent blogger. M5S shares parallels with Berlusconi, a media mogul who owns the three largest commercial television stations in Italy (Faris, 2010).

Election Infrastructure and Policy Background

Italy holds general elections for Parliament every five years. It uses paper ballots for its general election. In order to vote, voters must present ID cards and a voting certificate, which they receive when they are registered to vote. Ballots indicate the name of each party instead of the names of candidates.

Officials hand-counted ballots on the second day of the 2013 election (Donadio, 2013).

Election Infrastructure Meddling

The use of paper ballots makes cyberattacks against voting infrastructure difficult. However, several sectors of the Italian government are still vulnerable to cyberattacks.

Leaks through Hacking

Potential high profile hacking of political parties has fueled fake news in the run up to the 2018 elections. In August 2017, hackers were rumored to have obtained information on M5S members and a list of the party's donors but nothing has been released (Jones & Cinelli, 2017).

Government Hacking

The Italian Foreign Ministry was hacked in the Spring of 2017. According to a government official, a hacking group "used a malware to spy on [the field office] systems and exfiltrate sensitive information," (Paganini, 2017). Although the official refused to explain how the hacking was detected, the official claimed that the encrypted system was not invaded and only email systems were compromised.

According to a report by The Guardian, several people with knowledge of the case suspect Russian hackers accessed the system to monitor government decision-making (Kirchgaessner, 2017). This action might be a signal of Russia's interest in the next Italian general election. Russian officials have denied the accusation (Kirchgaessner, 2017).

Social Media Meddling

Fake news is a prominent problem in modern Italian politics. Fake news is posted by anonymous accounts, claiming to release information leaked through hackings; posts are then spread on blogs and social media. Bots are also prominent on Italian social media.

Internet Use Profile

81 percent of Italian households have Internet access via a personal computer (Organization for Economic Cooperation and Development [OECD], 2018). According to data from *We are Social* and *Hootsuite*, YouTube and Facebook are the most used social media in Italy, following by WhatsApp. 52 percent of Italians use Facebook, most through mobile applications (Hootsuite, n.d.).

Fake News and Rumors

Fake news is a common disinformation tactic in Italy. It does not require a high cost and is easy to produce, often only requiring a misleading title or a photo-shopped picture. Fake news is popular social media, and online Italian newspapers frequently repost news onto other sites, giving the stories a veneer of legitimacy (Nardelli & Silverman, 2016). Often, links and reposts from multiple sites appear to have popular support, but the reposting sites actually belong to the same owner (Pellegatta, 2018). People who control one or more popular sites, such as Beppe Grillo, can create a popular news story by reposting between sources (Nardelli & Silverman, 2016). Grillo's blog and Facebook account, which have nearly 2 million followers, have been described as the center of a network that promotes fake news (Taylor, 2017). The account's prominence can be compared to Italy's largest newspapers, and Grillo also controls *TzeTze* and La Cosa, two supposedly independent newspaper sites which hold a combined following of nearly 1.2 million people on Facebook (Nardelli & Silverman, 2016).

M5S has aimed to promote a narrative of corruption in the Democratic Party and their other popular opposition (Nardelli & Silverman, 2016). In 2016, Grillo uploaded a post to his blog with a picture of a large crowd of people and the caption, "[a] sea of humanity in the square, the people can't take it anymore," (Horowitz, 2017). His caption implied that the crowd was people who came to protest his opposition; in fact, the picture was from a speech given by Pope

Francis (Nardelli & Silverman, 2016). In another instance, an M5S video mistranslated a conversation between Matteo Renzi and Vladimir Putin (Horowitz, 2017). Renzi believed that M5S's fake news and rumors were partially responsible for failure of a 2016 referendum that resulted in his resignation (Horowitz, 2016). M5S propaganda is also viewed as partially responsible for falling public support in the DP since 2014 (Edwards, 2017). By December 2017, M5S's popularity had surpassed the DP in opinion polls, becoming the most popular party (Edwards, 2017).

On November 21, 2017, Matteo Salvini, a conservative politician, shared a fake story about an underage Muslim girl being sexually assaulted by her "husband" of age 35, posted by an unidentified source. Several major news sites also shared the story (Pellegatta, 2018). The story, which was fake, was also shared by several right-wing figures besides Salvini (Pellegatta, 2018).

BuzzFeed also found that *TzeTze*, one of the main pro-M5S news sites, frequently posted news from *Sputnik*, a pro-Russian state owned media outlet (Nardelli & Silverman, 2016).

Bots

Bots are widely used by Italian political parties to spread fake news through comments and reposts, or to spread political rhetoric (Nimmo & Pellegatta, 2018).

On January 23, 2018, during an appearance by Salvini on Italian television, a "suspicious number" of accounts tweeted identical text praising Salvini's appearance (Nimmo & Pellegatta, 2018). More than 150 accounts posted the same text in a 74 second timeframe. Those accounts were linked to an automator called "LegaNordIllustrator," which is connected to the official Lega Party Twitter feed and to the URL SalviniPremier.it. The fake accounts included corporate accounts without profiles or details of personal activities, while others were accounts of human users (Nimmo & Pellegatta, 2018).

Troll Armies

There is no specific evidence of troll armies involved in Italian social media. However, a report by the US Government mentioned that Russia "invested a lot" in controlling Italian public opinion (Corker, et al., 2018). Italy has launched programs to allow online reports of provocative posts and fake news (Noack, 2018). The government has also asked help from Facebook, the most popular social network service in Italy, to hire fact checkers the veracity of some posts (Giuffrida, 2018).

Conclusion

Italy is vulnerable to cyberattack but its traditional election infrastructure has limited actor's ability to directly manipulate voting systems. Instead, meddling happens more frequently on social media, which can be used to affect public opinion in the lead up to an election. While the Italian government has taken steps to mitigate the impact of fake news on their elections, its presence will almost certainly be felt more than ever before in the 2018 elections.

Case Study: Japan

By Olivia Lee

Internet based election interference was common through online communities in the 2014 and 2017 Japanese general elections, but did not necessarily affect the outcomes of the elections. Interference included attempts to influence social discourse through fake news, online communities and social media bots, but did not include cyberattacks. Interference operations were likely sourced from online groups and troll armies that have ties to political parties. While Internet based election meddling has not had a large effect in Japan's recent elections, the Japanese case gives basis to strong election law and enforcement, paper ballots, and also probes further research on the ties between politicians and online communities.

Table 7: Election Interference in Japan	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	Y
Online Communities	Y
Election Manipulation Actors	
Liberal Democratic Party (indirectly) LDP Net Supporters Club Online Right-Wing Communities	

Recent Election

Japan held its 47th General Election in 2017, a snap election called by Prime Minister, Shinzo Abe following the 2014 election. In both elections, The Liberal Democratic Party (LDP) took the majority. In addition, two new parties ran and secured the next largest number of seats: the Party of Hope, led by Yuriko Koike, and the Constitutional Democratic Party of Japan, led by, Yukio Edano (Solís & Mason, 2017). In both 2014 and 2017, the general election had a voter turnout of 53 percent (Yoshida, 2014). In the 2014 general election, the LDP won 238 seats and the Komeito (it's partnered coalition party) won 87 seats. The top other minority parties included the Democratic Party with 73 seats and the Japan Innovation Party with 41 seats (Asahi, 2014).

Prior to the 2017 election, these two parties merged into one Democratic Party (Osaki & Yoshida, 2016). This shows fraction and change within the opposition parties.

Background Context

The fundamental structure of the Japanese government consists of the Emperor, Judiciary branch, the National Diet, and the Cabinet, where the conservative LDP has been in control for most of Japan's democratic history.

The 2017 Edelman Trust Barometer ranks Japan as distrustful of both government and media (at scores 37 and 31 respectively). Trust in various forms of media, particularly newspapers, television, and Nippon Hoso Kyokai - Japan's only public broadcaster, have all been on the decline since 2001 (Yamamoto et al., 2014). According to Pew Research, "trust in the national government to do what is right for the country" is also low, with 40 percent answering "not at all" or "not much" and 51 percent answering "somewhat" (Stokes, 2017).

Election Infrastructure and Policy Background

Japan has a parliamentary political system where the National Legislature (Diet) is made up of an upper house (the House of Councilors) and a lower house (the House of Representatives). The prime minister has the power to dissolve the lower house and call a snap election at any time.

Japanese citizens can vote after registering at age 18 (Umeda, 2015). In 2002, legislation allowed electronic voting machine use in local parliamentary elections, but these machines still are not used for general elections (Ministry of Internal Affairs and Communications [MIC). Furthermore, only ten prefectures (out of 43) have used this technology in elections (MIC). In national Japanese elections, the voter writes down the name of the candidate for a House of the Councilors election, or writes a party affiliation for general elections when electing the House of Representatives (Local Governance Policy Making and Civil Society, 2007). The voters write the ballot out in a booth by themselves where candidate names and parties are listed (Local Governance Policy Making and Civil Society, 2007)

In 2013, the Public Office Election Law was amended to allow Internet usage for campaigning for candidates, which had previously been banned (Williams, 2017). This has allowed politicians to campaign online, although the effect on voters' is still uncertain.

Election Infrastructure Meddling

While there has been numerous cases and arrests over election violations, the rate of election fraud has vastly decreased in general elections since 1986 (Bright Election Promotion

Foundation Incorporated, 2013). The bulk of recent offenses have been from buying out voters (referring to paying or purchasing items for voters), at around 50 cases in recent elections (Bright Election Promotion Foundation Incorporated, 2015).

While cyberattacks have not been documented targeting Japanese election infrastructure, Japan has faced cyberattacks in the private sector, particularly from foreign actors. In January 2018, hackers stole $530 million worth of virtual currency from Coincheck, a large cryptocurrency exchange in Japan (Barron, 2018). Although the attackers behind the theft are still unknown, the South Korea National Intelligence Service told Japanese lawmakers that the attack might have been from North Korea.

Social Media Meddling

Japanese elections have featured the use of social media to influence the electorate, particularly with the proliferation of domestic troll armies associated with political parties.

Internet Use Profile

92 percent of the Japanese population used the Internet (World Bank, n.d.). The most popular social networks in October 2017, ranked by audience reach include Line (a messaging application), Twitter, Facebook, Instagram, Google+, and Skype (Statistica, 2017).Fake News and Rumors

Fake news has been an increasingly prominent topic in recent elections. Examples include left leaning news outlets such as Asahi making false claims that Shinzo Abe had doubted the outcome of his election (Tanaka, 2017). Politically and racially charged fake news has caught on in Japan, such as a fake claim in 2017 that Japanese girls were raped by a Korean (Hatachi et al., 2017). In response to fake news surrounding candidates in the 2017 general election, voluntary groups such as FactCheck Initiative Japan, which Buzzfeed Japan supports, followed how fake news stories were posted (Furuta, 2017). Buzzfeed News reported that several stories published during the election were not true, including several around Koike and her intention to run, and an article on the Democratic Party purchasing Twitter followers (Furuta, 2017).

FactCheck Initiative Japan highlights that media in Japan needs to improve its use of credible information (Furuta, 2017). In the Japanese girls example, the original writer confessed to paying a company to spread the story on Twitter using bots, making the post go viral on Twitter as well as Facebook (Hatachi et al., 2017), showing how fake news can spread in Japanese media. Fake news is present across the political spectrum. Some fake news finds its

basis in rumors, rather than made-up stories, such as a claim that the Constitutional Democratic Party bought Twitter followers, based on an actual sudden increase in Twitter followers (Odo & Stapczynski, 2017).

Political rumors and conspiracy theories are also widespread on the Japanese Internet. The Jimintou (LDP) Net Supporters Club, for instance, is often accused of working for the LDP, who are paying them to influence opinion online. Similarly, the LDP's Net Countermeasure Team has also been accused of pushing right-wing propaganda online (Misukiru, 2017). While these rumors are widespread, they have yet to make their way into mainstream media. Commenters and writers of this rumor express that although the online right's views are easy to find on Japanese Internet, these views may not accurately represent the Japanese population.

Bots

Along with Twitter's popularity in Japan, the platform has also been used as a tool to spread politically charged propaganda. During the 2014 general election, large amounts of Twitter bots tweeted in relation to the election (Schäfer et al., 2017). In a sample of 542,584 Tweets, filtered for content relating to the election, and searched for duplicates using an algorithm (discluding retweets), 431,050 Tweets (79.4 percent) were identified as produced by bots (Schäfer et al., 2017). Although there is uncertainty around who created the bots, they expressed views of the "netto uyo", or online right—a term used to describe Japanese right wing online communities.

Online right groups and online LDP supporters are not only prominent but also have certain political backing. The LDP officially endorsed the Jimintou (LDP) Net Supporters Club (J-NSC) in 2012 (Schäfer et al., 2017). Based off the J-NSC's views and the online right's views, there is overlap in themes of support for the LDP.

During the 2014 election, Abe strategized by portraying his economic plans in the public sphere, and by letting the online right, including the J-NSC and other groups, spread his nationalist agenda online (Schäfer et al. & Kingston, 2017). This worked in Abe's favor, because he was able to support online groups that agreed with his nationalistic policies, while focusing on campaigning for issues that resonated with the public more closely in mass media.

Online Communities and Meme Factories

The online right refers to Japanese Internet users who express far right views. Internet users who hold right-wing views can be found in high numbers on Twitter, 5channel (anonymous forums) and Niconico Douga (a video website). The online right often expresses

nationalist views, and many express anti-Korean views, explicitly or tacitly. On Twitter, for instance, there are thousands of accounts, many of which are likely bots, which state in their profile descriptions, “I love Japan” and “I hate things anti-Japanese”. These accounts tend to retweet right-wing news stories. Politically, the online right tends to support the right-wing LDP and Prime Minister Abe.

Other: Social media use by politicians

With the revision of the Public Office Election Law in 2013, Japanese politicians are now able to use the Internet for their campaigning period. Despite increased Tweeting, there is not evidence for a direct tie between candidates’ actions on Twitter and the election’s outcomes (Williams, 2017; Schäfer et al., 2017). Williams argues that for there to be a connection between politician’s Internet use and voters’ there needs to be greater institutional change so that citizens gain more interest in not only candidates’ social media but also politics in general (Williams, 2017).

Conclusion

Although Japan has an array of political movements online, including bots on Twitter, active online communities and new involvement by politicians, the potential effects of these actors depends on the Japanese population. On the other hand, there are also online groups with real ties to parties, such as the J-NSC and its ties to the LDP. This represents a strategy for politicians, in order to indirectly support more extreme views online while appearing more moderate in mainstream media (Schäfer et al. 2017). Endorsement of online supporters can also work to encourage the use of bots to influence others politically. Furthermore, rumors and fake news’ ability to reach mainstream media has the potential to influence voters. Although Japan is yet to face large-scale government hacking, hacking in the private sector should serve as a warning to other forms of cyber areas. The Japanese case shows the pros of paper ballots and strong law enforcement of election law. Further, although carrying limited influence in the case of Japan and its voter turnout, there is a possibility for politicians to mobilize online politics through communities, as an indirect way to influence elections.

Case Study: Republic of Kenya

By Fabian Gacayan

Internet based election interference played a minor role in the 2017 Kenyan Presidential Elections. Interference included attempts to influence social discourse through fake news and online communities, as well as direct cyberattacks against election infrastructure. Interference operations were likely sourced from domestic political partisans and foreign data-mining companies. Election meddling has played a minor role in Kenya's politics, whose political parties generally divide themselves along ethnic identities.

Table 8: Election Interference in The Republic of Kenya	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	Y
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	N
Troll Armies	N
Online Communities	Y
Election Manipulation Actors	
External Data-Mining Companies Unidentified Election Infrastructure Hackers	

Recent Election

The 2017 Kenyan Presidential elections resulted in incumbent President Uhuru Kenyatta's re-election with 54 percent of the vote, defeating challenger Raila Odinga. Nearly 1.6 million votes separated Kenyatta's 8.2 million votes (54 percent) and Odinga's 6.7 million votes (44 percent) ("Kenya Results Hacked, Opposition Says," 2017). Odinga refused to accept the results and petitioned the Kenyan Supreme Court on the grounds that the regulatory agency responsible for tallying votes - the IEBC - had failed to properly verify the ballots (Okumu, 2017). Following orders from the Supreme Court, the IEBC allowed the Court and political parties access to its servers for investigation. On September 1, 2017, the Supreme Court nullified the election results due to suspicions that the election may have been hacked, specifically during the transmission of votes, and that the IEBC had failed to initially verify the results before announcing them (Sieff, 2017).

The Court initially set a second election date for October 17, 2017 but then changed the date to October 26, 2017 to allow the IEBC to reform voting processes. Odinga, despite being included on the ballot, refused to participate in the second election due to a lack of "legal and constitutional guarantees" against potential electoral fraud (Ombuor, 2017). Kenyatta garnered 98.27 percent of the vote in the second election: 7,483,895 votes; voter turnout was 38.84 percent, a significant drop from the annulled election's 79.61 percent turnout (Lang'at & Ngirachu, 2018; Independent Electoral and Boundaries Commission, 2017).

Background Context

During the 2007 Presidential elections, over 1,000 Kenyans were killed and over 500,000 Kenyans were displaced in post-election violence (Masters, 2017). In the aftermath, the Kenyan government approved the formation of an Independent Review Committee to investigate potential causes for post-election violence. In their findings, the committee concluded that irregularities in previous elections, in the form of implausibly high voter turnouts, bribery, ballot stuffing, and impersonation of absent voters, contributed to public outrage over perceived rigged elections, resulting in the post-election violence (Kriegler & Aboud, 2008). Following these findings, the Kenyan government moved to replace the Electoral Committee with a new independent regulatory body responsible for ensuring a transparent election: the IEBC. The IEBC was meant to prevent future violence resulting from political outrage. Raila Odinga, who ran and lost during the 2007 general elections, blamed his loss on voter fraud and tampering (Gettleman, 2007). Despite filing a petition, the Supreme Court deemed the elections valid and without enough irregularities to warrant a new election (Karimi, Elbagir, & Smith-Spark, 2013).

The Kenyan population holds general mistrust for their national government, instead preferring regional county officials who share their ethnic identities. Kenya has both a national government and a devolved government, the latter of which has an elected county governor who both administers and implements laws to meet the demands of their respective county. When asked about attitudes towards the national government and politicians, 35 percent of Kenyans held some form of trust in the national government and politicians, whereas 64 percent held a general distrust. In contrast, about 53 percent of Kenyans have trust towards their county governor with 47 percent holding distrust (Sauti za Wananchi, 2017). Kenyans affiliate themselves with political parties who share the same ethnic identity as their own (Lynch, 2011). County governors are elected officials who likely share the same ethnic identities as their

constituents and are, as a result, more likely to trust the governors, as opposed to a national politician who may not share their ethnic identity (Sauti za Wananchi, 2017).

Kenyans largely vote along ethnic lines and candidates appeal to voters who share their ethnic backgrounds (Lynch, 2011). There are over 70 different ethnic groups in Kenya, with the five largest making up 70 percent of the population (African Studies Center, n.d.). The International Commission of Inquiry on Post-Election Violence reported that much of 2007 election violence could be attributed to false voter perceptions during the election. At the time, many voters believed that access to state resources would only be guaranteed if the candidate representing their ethnic group had won the presidency (Waki, McFadyen, & Pascal, 2008). Part of the reason for creating the IEBC was to provide Kenya with a regulatory agency independent of ethnic preferential treatment during election processes that the Electoral Committee of Kenya had been susceptible to (Mutahi, 2016).

Election Infrastructure and Policy Background

Kenya's presidential election uses a modified two-round system. The IEBC employs Biometric Voter Registration (BVR), Electronic Voter Identification (EVID), and a Results Transmission System (RTS), with the RTS sending results from polling stations to tally centers via text message. The BVR is used by the IEBC to confirm the identities of voters using fingerprints and photos (Mutung'u, 2017). An additional benefit to the BVR and EVID is the prevention of voter fraud. The IEBC opened 40,833 polling stations in the country for both the election and re-election (Dahir & Kuo, 2017).

At polling centers, voters are identified using the BVR, then given six stamped and colored ballot papers for various elections at the county and national level, including the presidential ballot. After voting on the ballots, the voter places their six ballots in their respective ballot boxes. At each polling center is a Presiding Officer who, after all votes are counted, fills in Form 34A, which gathers the results of the presidential election. On Form 34A, the Presiding Officer indicates the total number of accepted votes, rejected votes, disputed votes, and valid votes at the polling station (Hussein, 2017). Each completed Form 34A is then scanned and sent to a tallying center where a Constituency Returning Officer uses the information to fill out Form 34B, which is used to gather the number of votes each presidential candidate received from each polling station (KTN News Kenya, 2017). After the votes are tallied, they are sent to a national

tallying center where the chairman of the IEBC uses the tallied numbers to announce the winner of the election.

Individuals who are at least 18 years old, hold Kenyan citizenship, have a Kenyan passport or ID card, and have registered to vote at a registration center four months before an election are eligible to vote. Individuals who are already registered in the electoral system simply verify that they are registered to vote at the registration station before they are permitted to vote; this is to ensure that voters don't use false identities and that Kenyan citizens make all votes. In the event of an annulled election, voters do not have to reregister for the vote. The month-long process to register to vote, long lines at registration centers, and distances from registration centers are some factors that impede eligible Kenyans from registering and voting (Benjamin, 2017).

According to the Kenyan Constitution, a candidate may file a petition to the Kenyan Supreme Court to challenge the results of the election up to a week after the vote. The Supreme Court then has two weeks to hear and determine the petition and to make a final decision. The Supreme Court's decision is final. In the event that the Supreme Court determines an election is invalid, a new election is to be held within 60 days.

Election Infrastructure Meddling

Throughout the election process, candidate Odinga repeatedly claimed that candidate Kenyatta, his Jubilee party, and those loyal to the Jubilee party had attempted to rig the presidential election in their favor (Dahir & Kuo, 2017). According to Odinga, various attempts included hacking into IEBC servers and manipulating voter numbers. While Odinga made numerous claims of election infrastructure meddling, Kenyatta's party was largely quiet.

Leaks through Hacking

The first instance of infrastructure meddling revolved around the murder of Christopher Msando, a senior manager for the IEBC information technologies division. On July 31, 2017, Kenyan police found Msando after he had been missing for three days; his body showed signs of torture (Said-Moorhouse & van Heerden, 2017). Police arrested murder suspects but then released them (Odhiambo, 2017). During the election, Candidate Odinga claimed that hackers had used Msando's credentials to gain access to IEBC servers and activate an algorithm to inflate Kenyatta's votes (AFP, 2017). Specifically, Odinga claimed that hackers had introduced an algorithm into IEBC servers to widen the percentage gap between him and Kenyatta by 11

percent. He also claimed that hackers had manipulated the IEBC servers to not detect dates and times of submitted changes to the voting numbers and to hide from official detection (Odinga, 2017a). Despite refusing to reveal the source of his information, Odinga produced on his Facebook page 46 photos of computer logs that allegedly tampered the IEBC servers to favor Kenyatta (Odinga, 2017b). The IEBC has confirmed that there was an attempted hack on their systems, but that the hack was unsuccessful (Owino, 2017). In responding to Odinga's computer log images, the IEBC said they had looked at the logs and had determined them to not be authentic and that they had not originated from IEBC servers (Ndonga, 2017). The IEBC also stated that Msando's passwords for their servers had been deactivated shortly after his death (Menya, Mwere, Githae, Ngirachu, & Langat, 2017).

Voting Machine Tampering

Odinga claimed that the IEBC proclaimed Kenyatta as the winner prematurely, as 10,438 Form 34A forms, out of a total 41,451, were unaccounted for at the time of IEBC's declaration that Kenyatta had won the presidency (Ogemba & Muthoni, 2017). Furthermore, there were irregularities with the Form 34B forms. 56 lacked a security watermark, officers had not signed ten, 66 bore no stamps, ten were illegible, 31 had no serial numbers, and party agents had not signed 32 for confirmation (Ogemba & Muthoni, 2017). According to Odinga, this translated into seven million votes not accounted for (Ogemba & Muthoni, 2017).

Following the August 2017 elections, at the request of the Kenyan Supreme Court, the IEBC allowed both political alliances access to their voter servers on a "read-only" basis. On September 1, the Supreme Court decided to nullify the elections and continue with a re-election citing initial interference from the IEBC with regards to allowing access and the possibility that an outside party had infiltrated and compromised the IEBC's systems (Duggan & Said-Moorhouse, 2017). However, the Court stopped short of concluding that the compromise had affected the outcome of the presidential elections. The Court also did not identify the party responsible for compromising IEBC systems (Freytas-Tamura, 2017).

Outside of these claims, the IEBC worked quickly to try and mitigate any problems at voting stations. For instance, the IEBC fired a clerk at a polling station where ballot papers had been pre-marked as "rejected". At another polling station, police arrested a clerk for issuing double ballot papers to specific voters (Elkana, 2017).

The results of the October 2017 re-election served to show how loyal Kenyans are to their political party. For the second election, Odinga vowed to not rerun in protest of what he perceived as failure to reform the IEBC and urged supporters to not take part in the second election. Out of 19.6 million registered voters, only 7.6 million voted, roughly 38.86 percent of registered voters. In contrast, nearly 79 percent of registered voters took part in the previous election (Hussein, 2017). According to the IEBC, Kenyatta collected 7,483,895 votes for the second election, 98.26 percent of the total votes. Odinga collected 73,228 votes (Lang'at & Ngirachu, 2017). In the initial election, Kenyatta had gathered 8,203,290 votes out of a total 15,593,050 votes. With a lack of votes for Odinga, and similar numbers for Kenyatta, it is apparent that Kenyan voters remain largely loyal to their political party, and tampering claims and hacking accusations do little effect on their party preference.

Social Media Meddling

In Kenya, affiliates of both presidential campaigns used social media as a tool for communicating with voters, spreading misinformation, and influencing public opinion. The Internet in Kenya has experienced rapid growth in the past decade and Kenya lacks legislation for regulating the spread of misinformation.

Internet Use Profile

89.7 percent of the Kenyan population has access to the Internet, either through a desktop computer or a smartphone (Communications Authority of Kenya, 2017). This translates into 43,329,434 Internet users in Kenya, out of a population of 48,466,928. In comparison, the Internet user population was 200,000 in 2000, which translates into 21,564.7 percent growth in Internet usage (Communications Authority of Kenya, 2017). The most popular apps for sharing information and communication are (Facebook) Messenger, WhatsApp Messenger, and Twitter (Wangari, 2016; Chacha, 2018).

Fake News and Rumors

Fake news directed at both presidential candidates was present throughout the elections. Throughout the course of the election, fake news bulletins, under the guise of news outlets such as CNN or the BBC, displayed false claims that either one of the two leading candidates, Kenyatta and Odinga, were in the lead (Sevenzo, 2017). These claims appeared to have no impact on the elections, as the IEBC was consistent in updating the public on the presidential race via Twitter up to the declaration of the winner.

US-based Harris Media LLC, an advertising agency that uses data analytics to create political campaigns that target audiences based on their social media account, was involved in a major public relations campaign against candidate Raila Odinga (Privacy International, 2017). Leading up to the August 2017 elections, two major sites were created: 'The Real Raila' and 'Uhuru for Us'; both of which are now inaccessible (Privacy International, 2017). 'The Real Raila' made incendiary claims against candidate Odinga, including that he would relocate tribes not associated to his own from Kenya, implement martial law, reduce funds for clean water production, and proclaim himself as president for life. Meanwhile, 'Uhuru for Us' made claims that candidate Kenyatta would lower food prices and not induce police violence. Nowhere in Kenya's electoral laws and regulations does it state that political candidates are required to endorse campaigns or ads they have funded (Privacy International, 2017). As a result, it is unconfirmed whether Kenyatta or his party funded these websites.

Additionally, it is illegal under Kenyan law for political parties and candidates to endorse and distribute hate speech. However, the IEBC has admitted that it is exceptionally difficult to track hate speech (Chege, 2017). 'The Real Raila' and 'Uhuru for Us' share an IP address with Harris Media's own website and both sites shared the same Google Analytics tag as other conservative sites connected to Harris Media (Privacy International, 2017). When reached out for comment, Harris Media refuses to confirm collaboration with the Kenyatta political campaign and the Secretary-General of Jubilee has denied knowledge of the sites connected to Harris Media (Chege, 2017).

Both presidential candidates were linked to data mining companies during their campaigns. Kenyatta had reportedly paid six million US dollars to British-based Cambridge Analytica to gather survey data on Kenyans and to manage Kenyatta's public image. A spokesperson from the British firm has denied involvement in 'The Real Raila' and 'Uhuru for Us' campaigns but has neither denied nor confirmed involvement in Kenyatta's re-election campaign (Kelley, 2017). Meanwhile, Odinga reportedly signed a contract with US-based campaign data mining company Aristotle International Inc. (Star Team, 2017). The company's tasks included streamlining Odinga's campaign organization, improving Odinga's public image, managing press operations, polling public opinion, and analyzing Odinga's chances of winning the election (Star Team, 2017). While both campaigns utilized data mining companies, the impact of those companies work on the outcome of the election is indeterminate.

Conclusion

Following the violence of the 2007 elections, Kenya has taken precautions to prevent a recurrence of violence. This has taken the form the IEBC, an independent regulatory agency designed to be free from political allegiance and to monitor and carry out transparent elections. The 2017 elections were the IEBC's second time monitoring and carrying out elections. The system still has flaws, but irregularities are not commonplace.

Odinga's allegations that the IEBC had been hacked to favor Kenyatta notwithstanding, multiple sources outside of Kenya have stated their belief that the elections were fair with minimal tampering. *The Economist* completed a study, based off of a small sample of Kenyan paper ballots, which showed their results mirrored those of the actual electronic voting systems ("Kenya's election may turn nasty," 2017). The rise of the Internet and social media in Kenya appears to have exacerbated ethnic divisions, which already existed in Kenya and had come to define political parties. The presence of fake news and potential hacking may have influenced some voter opinions, but the vast majority of Kenyans have remained loyal to their political parties and ethnic background regardless of accusations and misinformation.

Case Study: Republic of Korea

By Jion Yi

Internet based election interference played a significant role in the 2012 and 2017 South Korean Presidential Elections. Interference included attempts to influence social discourse through fake news. Interference operations were likely sourced from domestic political actors such as government agencies and online communities. South Korea's misguided use of social media during the elections, combined with its recent government corruption scandals, has manipulated public opinion and intensified political polarization to a dangerous degree.

Table 9: Election Interference in The Republic of Korea	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	N
Troll Armies	N
Online Communities	Y
Election Manipulation Actors	
Government agencies Voters active on social media	

Recent Election

This case study focuses on two elections in South Korea: the 2012 and 2017 presidential elections. In the 2012 election, the most prominent candidates were Park Geun-Hye from the Liberty Korea Party and Moon Jae-In from the Democratic United Party (Kim, 2012). Park was elected in 2012, surpassing Moon by 2.6 percent of the vote (Kim, 2012). Park was a candidate from the same party as Lee Myung-Bak, her presidential predecessor, and the Liberty Korea Party had been the majority party since Lee's election in 2007 (Hwang & Son, 2007).

Park was impeached before the end of her term in 2017, following accusations of abuse of authority, bribery, extortion, and leaking government secrets (McCurry, 2017). The same year, Moon Jae-In from the Democratic Party was elected as the next president with 41.1 percent of the vote (Kyung-Hyang Newspapers, 2017). The runner-ups won 24.0 percent, 21.4 percent, 6.8 percent, and 6.2 percent of the vote, respectively (Kyung-Hyang Newspapers, 2017), a

significantly wider distribution of votes compared to 2012 and a sign that public trust in the major political parties, especially the Liberty Korea Party, has declined significantly since the 2012 election. The election of a Democratic Party member threatened the influence of Liberty Korea Party, arousing the fear in conservatives (Boykoff, Griffiths, & Kwon, 2017).

Background Context

South Korea is a democratic country where the Constitution guarantees the freedom of speech and press and the right to assembly and vote (National Law Information Center, n.d.). According to Freedom House, the Freedom Status of South Korea is "free," with an aggregate score of 84 out of 100 (Freedom House, 2018). The Press Freedom status is "partly free." (Freedom House, 2018)

Election Infrastructure and Policy Background

In South Korea, a president has a term of five years and cannot run for a second term. The legislative branch, the National Assembly, has 300 members, 253 of which are elected in local constituencies and the rest by political parties. The most recent National Assembly election took place in April 2016.

The country runs on a plural party system. Currently, the three most prominent parties are the liberal Democratic Party, the conservative Liberty Korea Party, and the progressive socialist People's Party (Korean Culture and Information Service, n.d.). Following Moon's election, the Democratic Party came to dominance.

South Korea has a seven-chapter long section of election policies in its Constitution. Its eighth, ninth, and the tenth clauses are the most applicable to Internet-based election meddling. The eighth clause states that journalists and broadcasting services organizations, if they produce fake or defamatory news, are obliged to produce corrected news afterward. In cases where individuals and organizations violate these laws, they can be charged for libel or slander according to the Electronic Communication Fundamental Law (National Law Information Center, n.d.). The ninth clause of the section states that government agents must stay politically neutral and not engage in any activity that could affect election results (National Law Information Center, n.d.). The tenth clause warrants the establishment of the Internet-based election defilement oversight committee to prevent election meddling attempts online (National Law Center, n.d.).

South Korean citizens, age 19 or older, can vote for national elections (KOCIS, n.d). While paper ballots are the most common voting means, the National Elections Committee and a telecommunication company called KT developed an electronic voting system called K-Voting in 2013 (Jeong, 2017). Distributed for public use, it allows electronic votes through PCs, mobile phones, or tablets after the users pay a service fee (National Election Commission, n.d.). K-Voting has not been used for a presidential election, although political parties such as the Justice Party and Bareun Party have used it for electing their party chairs and presidential candidates (Jeong, 2017).

K-voting has allowed voters to use their electronic devices at voting sites as well. Voters are given unique voting codes on a piece of paper, which they use to vote on an electronic device. The piece of paper has a short list of guidelines, which include a warning that the voters must not show their voting paper to anyone (National Election Commission, n.d.). This means of voting may be susceptible to social engineering, as another voter may try to steal this piece of paper and spoof the voter's identity.

Election Infrastructure Meddling

There have been several examples of state-sponsored cyberattacks from the Democratic People's Republic of Korea (North Korea) targeting South Korean infrastructure sectors, such as financial services, nuclear and hydropower facilities, as well as broadcasting companies (Beyer & Park, 2017). However, the electoral system has not been publicly attacked.

Voting Machine Tampering

A 2015 investigation revealed that Immacsoft, the company that provided cybersecurity technologies to K-Voting, had omitted a cryptographic feature in the voting machine (Kim, 2015). This mistake left the machine with no effective means of encryption—no hashing, key exchange, or authentication process—that would have protected the users' private information and voting records. The database administrator could have easily distorted the data and the election results. The machine has been updated since then, but the finding undermined already low public trust in voting procedures (Kim, 2015). Since then, some Korean academics have urged the government to reinforce voting systems, arguing that incorporating blockchain technology into voting machines would strengthen election security (Yu, 2016; Byeon, 2018).

Social Media Meddling

In South Korea, social media has been an effective election meddling tool. While the government has used social media to manipulate public opinion, it has also been used to spread

fake news and undermine trust in the government during the two most recent presidential election cycles. Two major cases of social media meddling support this observation: the National Intelligence Agency (NIA) election meddling incident during the 2012 election and the fake ballot incident during the 2017 election.

Internet Use Profile

88.3 percent of the South Korean population—about 44 million people—are Internet users (Korean Internet and Security Association [KISA], 2016). 99.2 percent of South Korean households have access to the Internet, and 98.9 percent of South Korean Internet users use Internet at least once a week (KISA, 2016). South Koreans are also avid users of social media. 65.2 percent of Internet users older than six use social media (KISA, 2016). The five most frequently used social networks in the country are Kakao Story, Facebook, Naver Band, Instagram, and Naver Café, respectively (KISA, 2016).

Fake News and Rumors

Fake news has always been a major issue in South Korean politics, particularly during election season. Russian interference in the 2016 US election emphasized the importance of recognizing fake news as a grave danger to South Korean election integrity (Kim, 2017). South Korean academics started conversations to define fake news and how to respond to it (Kim, 2017). Researchers found that Korean Internet users tend to choose news sources that already resemble their current interests and opinions because of (1) the vast pool of information available in contrast to one's limited attention span, (2) low digital literacy, and (3) social media algorithms that display posts only relevant to the users' interest (Kim, 2017).

The 2017 election experienced instances of fake news. Paper ballots were designed to include a margin space between each presidential candidate's checkbox to prevent ambiguous marking. Claims arose on some online communities, such as Naver Band, that some ballots did not have these margin spaces, an anomaly that they believed invalidated the ballots. Since it is illegal to take a photo of a ballot, this controversy was difficult to disprove. (Korea Herald Business, 2017).

Shortly after the election, the National Election Commission announced that the claim was fake news and sued 11 people (Korea Herald Business, 2017).

Other: Use of Government Agencies to Promote a Specific Party

During the 2012 election campaign, a former employee from the NIA reported that the government agency organized teams to comment or express agreement or disagreement on

political social media posts, including the ongoing election, particularly those criticizing Moon Jae-In as a candidate and advocating for Lee Myung-Bak administration's projects and policies (Park, 2013). It is illegal for a South Korean government agency or its employees to engage in any form of election promotion.

Moon's party reported one particular NIA agent to the police (Jo, 2012). When the police went to her residence with a search warrant, the agent locked herself in and refused to face the police for about 40 hours, during which she was suspected of destroying the evidence of her online activities (Jo, 2012). She later claimed that she always maintained political neutrality and did not post anything political online (Jo, 2012). To confirm her claims, the police announced in their mid-investigation briefing that they did not find any suspicious or illegal activity from her online history (Jeon, 2013).

However, it later surfaced that she produced over 120 political posts online, including some criticizing Moon. Other posts defended government projects and policies--for example the Four Major Rivers Project--many of which were facing controversy and public distrust (Park, 2013). This discovery pointed to the police as being part of the corruption and carrying out a deliberately perfunctory investigation (Park, 2013). However, the NIA and the Liberty Korea Party claimed that the agent's online activities were only to counter psychological warfare attempts from North Korea, and that they targeted online communities where North Korean agents and sympathizers were alleged to be active (Jang, 2017).

Coverage of the incident resurfaced in 2017 following Park's impeachment and Moon's election (Ha & Jeong, 2018). Investigations afterward excavated many more hidden details and proved that the NIA was indeed involved in election meddling attempts on social media (Jung, 2018). Today, several former government agents are facing charges on wrongful election promotion and corruption (Ha & Jeong, 2018).

Conclusion

The election of president Moon turned the tide in Korean politics in many ways. The power transition from conservative to liberal, accompanied by the fast-paced socioeconomic change, has spawned fear and shame among traditional South Koreans (Chang & Seok, 2017). They have vented these sentiments through social media and online communities, resulting in a dangerous degree of fake news. The South Korean government and academia will have to agree on how to respond to prevent further election meddling in the near future.

Case Study: Senegal

By Safy Sayoud

Internet based election interference was not prevalent in the 2012 Senegal Presidential Elections. Although election interference is not a major concern for Senegal, this case study focuses on the susceptibility to the upcoming 2019 Senegal Presidential Elections and the effects that may come from growing Internet use.

Table 10: Election Interference in Senegal	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	N
Bots/Computational Propaganda	N
Troll Armies	N
Online Communities	N
Election Manipulation Actors	
No outside actors inflicted on election processes in Senegal.	

Recent Election

The most recent presidential election in Senegal occurred in 2012. In that election Alliance pour la République (translated to Alliance for the Republic or APR) candidate Macky Sall, the former mayor of Dakar (the Senegalese Capitol), and Parti Démocratique Sénégalais (Senegalese Democratic Republic or PDS) candidate Abdoulaye Wade, the former Senegalese President, ran against each other. During the campaign, corruption was a leading issue for both of the candidates.

Before 2012, the current President, Abdoulaye Wade had been elected in 2000 and re-elected in 2007. Wade oversaw amendments to the Senegalese constitution that changed the Senegalese President's term from seven years to five. Wade also amended the constitution to make the presidency limited to two terms. To run for reelection in 2012, Wade argued that the constitutional changes he had made did not apply to him since he had come to office before their implementation – this decision was controversial and provoked anger among Senegalese political opposition. Senegalais were also critical of Wade because of accusations of corruption and

nepotism, as well as high tariffs on imported goods and self-seeking profit extraction, activities which had been detrimental to the country's economy (Jahateh, 2012).

Partly due to the political weakness of his competitor, Sall handily defeated the incumbent Wade – Sall would receive 65 percent of the vote to Wade's 35 percent. (Fessy, 2012)

Background Context

Senegal has seen a dramatic decrease in its population's trust of the nation's political institutions. In 2000, after the first election of Wade, 73 percent of the population held great trust in the president (Sall, 2015). Following bouts of violence in street protests and other issues, trust in the president and other political institutions dropped (Fessy, 2012). Trust in the president decreased substantially, form 73 percent to 46 percent (Sall, 2015).

Since the election of Macky Sall in 2012, trust has increased, although not to previous levels. Digital media, particularly social media, is having a growing impact on society in Senegal. Senegalese citizens have become more active on social media as a platform for communication. The most visited sites for news in Senegal are Seneweb, Senenews, Senego, and Dakaractu. (Sall, 2017) Freedom House rates Senegal as "free" (Freedom House, n.d.).

Election Infrastructure and Policy Background

Senegal participated in forms of voting prior to gaining its independence from France. The Trans-Saharan Elections Project at the university of Florida claims that they have been voting since 1848. The ability to vote in the nation has transitioned from only white and mixed-race populations to the whole of the population in 1946, after the conclusion of World War II (Trans-Saharan Election Project, n.d.). The Republic of Senegal uses multiple paper ballots to cast votes.

Paper ballots are simplified so that uneducated portions of the population are still able to adequately cast a vote in the process (Trans-Saharan Election Project, n.d.). Senegal has considered shifting to a single ballot system; yet former President Abdoulaye Wade has said the nation is not ready for a single ballot system (Trans-Saharan Election Project, n.d.).

Election Infrastructure Meddling

There is no evidence of election manipulation through the Internet in efforts to effect or tamper with elections in Senegal. One of the only recent examples of tampering of voters efforts to cast their votes at voting stations comes from the 2017 Parliamentary elections, where hundreds of Sengalese voters were unable to vote as they did not have their voter identification cards to access the polls. Although the citizens who were set to vote had gone through the

processes to ensure they would receive their voter id cards to be able to cast votes, delays in the population's distribution had left the voters off of the voting lists (Ba, 2017).

As Senegal is a central hub for African Internet service providers, linking neighboring countries with connections to Europe and the United States, Senegal could be considered a target in actions meant to impact the West African region more broadly.

Social Media Meddling

The most important social media sites to users in Senegal are Facebook, Instagram, and Twitter. Other popular applications used for social media and information sharing are Viber, LinkedIn, and WhatsApp. As a 2017 sample shows, 25 percent of adolescents connect on Facebook or WhatsApp a minimum of ten times in a single day.

As social media becomes a medium for classrooms and the workplace, the population becomes more reliant upon the platform to access to news. Senegalais gain political perspectives from social media. As social media continues to spread throughout Senegal, people have become more inclined to accept first seen news without verification. The fast speed of news dissemination in Senegal has impacted citizens ability to determine the veracity of information (Sall, 2017).

Conclusion

Although it is still developing its Internet infrastructure and its electoral process, Senegal has long been a nation of traditional voting systems with no cases of electoral tampering. The country has long been pushing efforts to create a more transparent executive branch, as citizens are angered at endemic corruption. The key element in Senegal for this case study is their centrality to the African continent and the hub it plays as an Internet service provider to itself and other nations. As Senegal continues to connect to the Internet, its susceptibility to Internet-based election interference increases.

Case Study: Spain

By Qi Cheng

Internet-based election interference played a significant role in the 2017 Catalan independence referendum. Interference included attempts to influence social disclosure through fake news and social media bots. Interference operations were likely sourced from the Russian Government, as well as domestic political actors. As an illegal election marked by the Spanish central government and European Union Commission, pro-independence parties appear to have committed most of the meddling.

Table 11: Election Interference in Catalonia, Spain	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	N
Online Communities	N
Election Manipulation Actors	
Pro-Independence Parties Russian Federation	

Recent Election

The Spanish region of Catalan held an independence referendum in October 2017. The October 1 referendum, led by Catalonia's separatist government, asked voters whether Catalan should seek independence from Spain and become a sovereign state. The Spanish government argued the election was unconstitutional, and determined it illegal (Said-Moorhouse, 2017). Despite the banning from the Spanish central government, the election was approved by the Parliament of Catalonia and was still held within the Catalan region (Lauren, 2017).

The Catalan government claimed that 92.3 percent of the region's citizens supported independence (Catalan Parliament Report, 2017). However, only 43 percent of Catalans actually turned out to vote. On October 2, the day after the government of Catalonia declared their independence, the Spanish government declared the election nullified. The president of Catalonia, Carles Puigdemont, decided to defer the independence process and negotiate with the

Spanish government over Catalonia's autonomy. On October 27th, probably due to a breakdown in negotiations, Spanish Prime Minister Mariano Rajoy declared that Puigdemont was dismissed and that the Spanish government would take over governance of Catalonia. The Spanish central government decided to hold a new Catalan regional parliamentary election on December 21st.

Background Context

Spanish democracy began in 1975, following the death of military dictator Francisco Franco. Catalonia has a history of seeking independence from Spain, existing prior to 1975. For centuries, Catalonians fought for gaining higher autonomy. Artur Mas, who was President of the Generalitat of Catalonia from 2010 to 2015, officially started the referendum process in 2014.

According to surveys, Catalan citizens hold little trust in the Madrid government (Manevich, 2017). 91 percent of Catalans say they do not trust Madrid and 81 percent saying they are not satisfied with the current democracy in Spain (Manevich, 2017). At the same time, Catalonia accounts for one-fifth of Spain's economy and pays a significant tax to the central government (Manevich, 2017). Compared to other states, Catalonia argues it does not get enough operational budget funding for infrastructures and services (Comissió d'Economia Catalana, n.d.). This perceived imbalanced economic situation drove Catalan's dissatisfaction with the central government and helped lead to the independence referendum.

While all major national political parties opposed the Catalan referendum, parties at the federal level in Spain span the political spectrum on other issues. Podemos (the third largest political party in Spain) is a left-wing political party who opposed independence, but supported the independence referendum itself, believing that the election could solve the long-existing disputes in Catalonia (Castaño, 2017). The Spanish Socialist Workers' Party (PSOE) is a center-left party that remained neutral (Castaño, 2017). Citizens (Cs), another political party in Spain, opposed Catalan independence and believed that the central government should reconsider regional autonomy (Castaño, 2017). In Catalonia however, parties that supported independence accounted for the majority in the Catalonian parliament prior to the independence referendum. These regional parties include Republican Left of Catalonia (ERC) and Catalonia European Democrats (PDEC) (Sengupta, 2017).

Pro-constitution and pro-independence parties in Spain both have incentives to interfere with the outcome of the Catalan independence referendum. The pro-constitution parties believed that the referendum is illegal and would like to maintain Spanish unity. This could be because

Catalonia pays a significant portion of taxes to the central government, which can be used by Madrid to support other institutions and maintain the normal infrastructure of Spain. The pro-independence parties hope that Catalonia can get rid of the control of the Spanish government and foster better economic development on their own ("Catalonia: Did Voters Face", 2017).

Election Infrastructure and Policy Background

The Catalan election used paper ballots, removing the chance of cyber related meddling. The Catalan referendum is marked as illegal by both the Spanish government and the European Commission, while "the United Nations had called on Spanish authorities to respect the Catalan people's rights to freedom of expression, assembly and participation in the vote". (Deardon, 2017) As an unconstitutional activity, the Spanish prime minister sent federal police to stop election-related activities. Police also tried to prevent voting by keeping citizens away from polling stations. The prime minister gave a televised address with the purpose of suspending the referendum (Deardon, 2017). Although the Spanish central government blocked and removed the legal status of the referendum, it did not forbid the media coverage, as the pro-independence broadcaster TV3 was still able to broadcast (Hedgecoe, 2017) and the Catalonia vice president was able to deliver pro-independence remarks through social media (Deardon, 2017).

Election Infrastructure Meddling

Since the Catalan election used a paper ballot, it cannot be meddled through the Internet. The only equipment that can be accessed through the Internet was the ballot scanner. Although this system was connected to the Internet, there is no evidence that the system was tampered with.

Social Media Meddling

During the referendum campaign, fake news, bots, and hacking were all used to influence the outcome of the election.

With EU support, the Spanish government was able to block websites affiliated with the independence process (Smith, 2017). In order to maintain the Catalan referendum census site for pro-independence parties, Russian hackers became involved in mirroring the site. Their job was like "permanently creating new links in order to have so many copies of the census site that it will be impossible for the Spanish judiciary and police to shut them down." (Madrid News, 2017)

Internet Use Profile

Over 80 percent of the Spanish population has Internet connections at home (World Bank). WhatsApp is the most used social media application, followed by Twitter and Facebook. Social media was heavily used during the referendum. Many tense incidents in the streets before and during the independence referendum period were recorded and posted on social media (Child, 2017).

Fake News and Rumors

The Catalan government held the independence referendum with the aim of gaining autonomy. To gain support from citizens, Jordi Turull, the spokesman for Catalan government, declared that they couldn't earn complete democracy under the Spanish government (Deardon, 2017). In order to expand prominence of the slogan, the Catalan regional government used fake news to justify their words. Before the referendum, photos posted on Twitter showed that the federal police were using extremely violent actions to threaten voters. For example, photos were spread of a disabled voter being kicked by a federal policeman and of firefighters fighting against the local police officers. These photos were posted on October 1st to give the voters a feeling that their democracy was being denied by the central government. However, it was soon proved that the scenes in those photos did not occur during the election period. The photos came from blogs shared by others and even from some newspapers from years prior ("Catalonia: Did Voters Face Worst", 2017). This way, fake news worked to discredit the Spanish government and encourage a "yes" vote on the referendum.

Bots

Bots were used to influence the direction of public opinions and spread disinformation during the Catalan referendum. During the referendum campaign, the word "Catalonian" or "Catalan" was used with a 7500 percent increase before and during the referendum period (David, 2017). According to a news article, "a total of 87 percent of the 65 accounts that most shared RT and Sputnik content were automated. Those accounts helped ensure that Russian news outlets were the fourth most influential in the digital conversation about Catalonia." (Lesaca, 2017) Instead of spreading fake news, bot accounts, but instead spread negative news about the Spanish government. Bot armies on Twitter focused on corruption scandals and economic issues caused by the Spanish government (Lesaca, 2017), content intended to push Catalonians to believe that becoming independent could bring a better economic situation. Many bots were documented as originating in Russia, implying Russian Government involvement on the pro-

independence side of the referendum, possibly as a tool to destabilize the EU (Deiz & Mateo, 2017).

Conclusion

The Catalan Referendum was one of the largest crises for Spanish democracy since its creation in 1975. Transcending Spanish borders, the cyberattacks linked to the election impacted the whole European Union. The Spanish government, in attempting to stop the referendum, took action to block information from prospective Catalan voters. However, there is no evidence showing Madrid got involved in other cyber-related interference. The Catalan government, with the purpose of driving the independent process, used fake news, bots and hacking to sway public opinion.

Case Study: Ukraine

By Julia Summers

Internet based election interference was very prominent in Ukraine during the 2014 Presidential and Parliamentary Elections. Interference included attempts to influence social discourse through Fake News, Social Media Bots, Troll Armies and direct cyberattacks against the country's electoral systems and government websites. Interference operations were sourced from Russia. Ukraine found itself a test ground for Russian cyber offensive activities intended to sow discord, create confusion among Ukraine's population and promote a very particular narrative that would not only have an influence on Ukraine's domestic affairs and policies, but also create confusion outside of its borders about the situation within Ukraine (Euromaidan Press, 2017.

Table 12: Election Interference in Ukraine	
Election Infrastructure	
Government Hacking	Yes
Political Hacking	Yes
Government Website Hacking	Yes
Election Systems Hacking	Yes
Social Influence Operations	
Fake News	Yes
Bots/Computational Propaganda	Yes
Troll Armies	Yes
Online Communities	Yes
Election Manipulation Actors	
Russian Federation	

Recent Election

Ukraine held its last presidential election in May 2014, following the ouster of former president Victor Yanukovych earlier that year. Ukraine's most recent parliamentary elections were held in November 2014.

The top contenders (endpoint) were pro-Western business magnate and politician Petro Poroshenko with 54.70 percent of the vote and former prime minister Yuliya Tymoshenko, who received 12.81 percent of popular vote. The November 2014 parliamentary elections yielded similar results, with leading positions taken by the Narodni Front with 22.14 percent of the votes and President Poroshenko's party with 21.82 percent, both pro-Western parties. Pro-Russian

party “Opozytsiynyy bloc,” formerly known as the “Party of Regions,” came in fourth with 9.43 percent of votes (Extraordinary Parliamentary Election, 2014).

Background Context

Pro-Western protests ousted Ukrainian President Victor Yanukovych, who was considered an ally of Russian President Vladimir Putin, in 2014 (“Ukraine Protests After Yanukovych”, 2013), triggering elections for his replacement. The protests were opposed to Russian influence in Ukraine – thus against Russian interests in Ukraine (Applebaum, 2017).

Russia has worked to destabilize the Ukraine Government and through covert military and offensive cyber activities, including meddling in Ukraine’s 2014 presidential and parliamentary elections. In March 2014, Russia annexed Crimea, a region of Ukraine, and started an insurgency in the East Ukrainian regions of Donetsk and Lugansk.

The majority of Ukrainians speak both Ukrainian and Russian (Fisher, 2014). This made an intensive Russian Internet – based misinformation campaign possible, because it was easier for Russian native-speakers to produce it.

Trust in Ukraine’s media is low. According to a survey conducted by the National Academy of Sciences of Ukraine, only 25.2 percent of Ukrainians trusted the media, and 45.4 percent did not trust the media (Reporters Without Borders, 2016). Most private media channels in Ukraine are owned by Ukraine’s oligarchs, and are thus perceived as serving particular interests. Since 2014, independent media projects such as Hromadske.tv have gained popularity (Reporters Without Borders, 2016).

Election Infrastructure and Policy Background

The President of Ukraine and the Parliament are elected every five years. The President is elected for no more than two consecutive terms by direct popular vote by citizens above age 18. Ukraine presidential elections are carried out through a two-round system, where the second round is held between the two candidates that received the most votes in the first round. If any candidate receives an absolute majority during the first round, the second round does not take place.

In Parliamentary Elections, 450 representatives are elected via a mixed election system. Half of the representatives are elected via first-past-the-post voting from constituencies. The other 225 are elected from national closed-party lists that are distributed between the parties

using a five percent threshold quota. Both presidential and parliamentary elections use paper ballots systems for voting (Keyishian, 2016).

Because of the Russian occupation of Crimea, Crimeans who wanted to cast their votes in 2014 Ukrainian elections were only able to do so on the Ukrainian mainland, and both Crimean Peninsula and Eastern regions occupied by Russia supported forces had the lowest voter turnout during 2014 elections (Organization for Security and Cooperation in Europe, 2014).

Election Infrastructure Meddling

Ukrainian Election Systems were hacked during both the presidential and parliamentary elections of 2014 (UNIAN, 2014). On the eve of presidential elections, the Ukrainian Election System ballot processing software was subject to a cyberattack (PROVCE, 2014). CyberBerkut, a hacking group connected to Russian state hackers, took credit for the hack (Greenberg, 2017). CyberBerkut disabled election websites and shared personal emails of employees and acquired election files (KyivPost, 2014). Additionally, hackers attempted to make it seem that the leader of Ukraine's, Dmitry Yarosh, nationalist party had won the presidential election (Greenberg, 2017). While the attack was caught and fraudulent results were not released, Russian state media broadcasted the forged results domestically (Najibullah, 2014). Yarosh's party holds ultra nationalist views and is unpopular amongst European leaders and the Russian public – a Yarosh victory could increase European hostility toward Ukraine (Stern, 2015).

During the 2014 parliamentary elections, Ukraine's electoral systems encountered another cyberattack. In addition to disrupting election software, some reports say that the outdoor screens playing election materials were replaced with "scary and horrible" images, such as destroyed buildings, dead bodies, and two politicians tagged as "war criminals" (Phys Org, 2014).

Social Media Meddling

Social media was a main tool used during the 2014 presidential and parliamentary elections. The disinformation campaign included the use of troll armies, bots, memes on social media, and other means to alter popular opinions and sentiment.

Internet Use Profile

In 2016, over half of Ukrainians are Internet users (The World Factbook, 2018), an increase from 43.5 percent in 2012 (Yarovaya, 2013). Online social networks such as Facebook, Twitter, Odnoklassniki, and Vkontakte (VK) are popular among Ukrainians. In 2013, almost

three million Ukrainians used Facebook (Minchenko, 2013). Social media has been prominent in Ukraine as a platform for collective action, including during the 2013-14 protests (Yaffa, 2016).

In 2013, Russian social network VK was the most visited website in Ukraine (Alexa). In January 2012, some 20 million Ukrainians were registered users on VK, and about 10 million Ukrainians visited VK on daily basis, about 20 percent of daily visitors to the website. Odnoklassniki, a social media platform monitored by the Russian government (Soldatov), has wide popularity as well, with a 2013 daily user base of 4.8 million Ukrainian visitors (Yarovaya, 2013). During the elections, troll armies were active on VK, Odnoklassniki and Facebook. Following his dismissal in 2014, the founder of VK claimed that he had been pressured by the Russian government to reveal details on Ukrainian protesters (Henni, 2014).

Russian social media networks and software imported from Russia were banned from Ukraine by executive order in the spring of 2017 (Radio Free Europe, 2017). However, the policy has raised questions about the Internet freedom. In response to the prohibition, Russian websites have released information on how to dodge the ban (Kiselyova, 2017).

Fake News and Rumors

Extensive disinformation campaigns conducted by the Russian government in Ukraine began with protests in 2013 and lasted through the 2014 elections. Troll armies, bots, and Russian state-run TV media channels used online resources, such as Facebook, Twitter, VK, Odnoklassniki and YouTube to disseminate fake news. Fake news ranged from coverage minimizing the scale and significance of protests to staged footage of false events in the conflict in Eastern Ukraine. Stories were mainly broadcasted on Russian state media, targeting Eastern Ukraine and the Crimean Peninsula, but also were shared on YouTube and broadcasted on the Russian state-owned news agency RT. The fake news narrative suggested a growing presence of nationalists in Kiev usurping power and killing innocent people for their support of pro-Russian sentiment. For example, one story featured a 3 year old boy who was said to have been crucified by Ukrainian soldiers. The story was told by a woman claiming to be his mother, and was later debunked as being fake (Alexander, 2015). Fake news was designed to disqualify and discredit the pro-Western government in Kiev, swaying popular sentiment towards Russia.

Bots

Bots were used on Facebook and Twitter in Ukraine. Facebook bots sent thousands of complaints to Facebook's moderators team to suspend Ukrainian users' accounts. Bots were used

to send thousands of complaints to Facebook's abuse team to cause blocking of anti-Russian opinions online (Zhdanova, 2017).

Twitter bots designed to look like real users spread conflicting and manipulated information on Ukrainian events. While increasing their following and establishing an online presence, bots spread fake news, instilled fear and confused audiences. For instance, a Twitter user named @TimurKhorev noticed that each time somebody used the #MH17 hashtag (related to the shooting down of a commercial airliner by pro-Russian forces in Eastern Ukraine) in tweets in Russian, a bot would post a link with a fake article countering the results of the investigation. Third type of bots were called impact bots. Other bots worked to boost information prominence in search engines, or created artificial trending issues (Zhdanova, 2017).

Ukrainian government and society have engaged in efforts to counter interference with mixed success. In 2015, the Ukrainian Government announced the creation of an "Internet Army" made up of volunteers to fight Russia in an information war. Around 40,000 people became "information soldiers". While the project has shown mixed results, the media and civil society have undertaken a more effective approach by creating online resources on debunking fake news. For example, the StopFake.org project, consisting of 17 websites run by a university has debunked over 1,000 fake stories (Zhdanova, 2017).

Troll Armies

Trolls used Facebook and VK to spread pro-Russian and anti-Western propaganda and create fear and confusion. For example, one post made by a troll posing as a Ukrainian read, "Brigades of westerners are now on their way to rob and kill us,"(Applebaum, 2017). Trolls flooded comment sections on news media websites. After Yanukovych fled Ukraine, a user made the following post in the comment section of a British news website: "There was a coup in Ukraine. I live in Kiev. I was on the Maidan, but peaceful protest ended two months ago, when we were displaced by armed nationalists. It's a nightmare." (Applebaum, 2017) The information Galitsin shared was not accurate, and supported a Russian narrative of Ukraine being taken over by nationalists.

Facebook trolls submitted complaints against pro-Western activists and media posting updates the conflict in Eastern Ukraine. As a result, the accounts of many activists, journalists, politicians and even certain TV channels were repeatedly suspended or blocked altogether, often just hours after being unblocked (Sheth, 2017). Numerous Ukrainian social media accounts were

blocked for sharing the photo of a little girl receiving a medal "For Valour and Bravery" for her late father who died in Eastern Ukraine (Minchenko, 2015).

In response to the banning campaign, Ukrainian activists petitioned Facebook and asked for a local office to be opened to deal with the banning campaign. However, the requests received no immediate attention from Facebook. In March 2014, the Ukrainian Crisis Media Center, a non-governmental organization that provides information on events in Ukraine, set up an emergency help desk to provide assistance to those banned on Facebook for political reasons. According to the Center, about 1000-1500 Ukrainians were banned on Facebook daily during the height of the banning campaign in 2014 (Minchenko, 2015).

Online Communities and Meme Factories

Online communities operating as meme factories also supported the political influence campaign Ukraine experienced in 2014. Memes disseminated critiques of pro-Western candidates, often portraying them as homosexuals or zombies and depicting Putin as cool, messianic and threatening. Facebook, Twitter, and VK were the primary outlets for memes, spreading rumors and conspiracy theories (Newton, 2017). For instance, the Twitter user @RuNetMemes posted a map of Ukraine pictured as a chocolate bar that looked like the pieces of it being broken off, with the tag "New Ukraine", referring to newly elected President Poroshenko's confectionary business. (Wiggins, 2014).

Conclusion

In Ukraine, trying to protect its interests, Russia has weaponized information in order to influence public opinions. Through various means, including social media and cyberattacks, the Russian Government has attempted to sow discord and sway the public vote away from candidates supporting a pro-Western course of development for Ukraine. At the same time, these acts have brought a sense of instability within the country that has increased distrust among the citizens of Ukraine towards their government.

Case Study: United Kingdom

By Safy Sayoud

Internet based election interference played a prominent role in the United Kingdom's decision to leave the European Union in 2016. Interference included attempts to influence social discourse through fake news and social media bots. Interference operations were likely sourced from foreign actors, including the Russian Federation, as well as domestic right-wing partisans. The UK referendum is an example of the power of social media meddling to promote nationalist or populist sentiment in one of the world's oldest democratic systems (Polyakova, Alina, et al., 2016).

Table 13: Election Interference in the United Kingdom	
Election Infrastructure	
Government Hacking	N
Political Hacking	N
Government Website Hacking	N
Election Systems Hacking	N
Social Influence Operations	
Fake News	Y
Bots/Computational Propaganda	Y
Troll Armies	N
Online Communities	N
Election Manipulation Actors	
Russian Federation	

Recent Elections

The United Kingdom (UK) held their most recent parliamentary elections in June 2017. This case study will also focus on the 2015 UK General Elections and the 2016 Referendum deciding whether the UK should exit from the European Union (Brexit Referendum). The 2017 Elections were held early following the resignation of Prime Minister David Cameron after the Brexit Referendum, and succeeding Prime Minister Theresa May's decision to call early elections. David Cameron had been elected in 2010 as the leader of the conservative party, winning 36.9 percent of the vote in comparison to the Labour Party's 30 percent ("Election 2015: United Kingdom Results", 2015). A year after the campaign, the Brexit Referendum resulted in a "yes" vote to leave the EU. On March 29, 2017, the UK announced their intention to separate from the EU (Millichap, 2018). The Brexit Referendum vote was close, with 48.1 percent of

voters in favor of remaining within the Union while 51.9 percent voted to exit (The Electoral Commission, n.d.). As a vocal opponent of Brexit, Cameron announced his resignation following the referendum results and was replaced as Prime Ministry by Home Secretary Theresa May. In the 2017 British Elections, Theresa May advanced as the new leader of the Conservative Party, while Jeremy Corbyn represented the Labour Party. The 2017 elections resulted in 45.6 percent of votes for the conservative party, while Labour received 41.9 percent ("Election 2017: United Kingdom Results", 2017)

Background Context

UK citizens generally hold little trust in their government. In 2018, roughly 36 percent of UK citizens held trust in the government, while 32 percent said they held trust in the media (Ries, 2018). The UK Government has accused Russia of attempting to "sow discord" during the Brexit Referendum, and that Russia would like to the EU weakened. (Booth, 2017).

Election Infrastructure and Policy Background

UK elections consist of a parliamentary election within five years as enumerated in the Fixed-term Parliamentary Act of 2011. British voters elect Members of Parliament to represent districts in the House of Commons. An election may occur if one of two motions are enacted: a "motion of no confidence is passed in Her Majesty's Government by a simple majority" or two-thirds of the House of Commons come to an agreement that there is a necessity for a general election (General Elections, n.d.).

The UK has been a unitary parliamentary constitutional monarchy since 1918. To vote in the UK, a person must be a British, Irish, or Commonwealth nation citizen that is at least 18 years old on the day of the election, as well as a resident holding a UK address. Exceptions exist for those who are abroad at the time of an election, where a citizen must prove involvement in parliamentary elections within the prior 15 years ("EU Referendum Results", n.d.).

Parliamentary elections in the United Kingdom use paper ballots inserted into ballot boxes at polling booths. (Brown, 2017) There is much debate on whether the UK should replace the long-established style of vote casting to modern voting machines and whether the cost-benefit analysis on saving time and money are worth the risks of meddling in the processes. (Hern, 2015)

Election Infrastructure Meddling

While the UK election system was not hacked during the Brexit Referendum or other recent elections, Russian government hackers likely targeted British broadcasters and government agencies.

Leaks through Hacking

Russian hackers were involved in attempts to disrupt recent British elections, particularly the 2015 elections. The group APT28 (Fancy Bear) put their efforts towards targeting television broadcast servers, including BBC, Channel 4 and Sky News, as well as Whitewall servers, which include the UK Government Home Office, Foreign Office, and the Ministry of Defense (Mortimer, 2016).

Individuals associated with Fancy Bear were known to rent computers from a service known as Crookservers, which claims that the probable Russian affiliated hacktivists used "bogus identities, private networks, and hard-to-trace payment systems" to hide their identities (Vallence, 2017). Through Crookservers, hackers such as Fancy Bear were persistent in efforts to disrupt government practices, although no cyberattacks were publicly successful.

Social Media Meddling

Social media meddling has played a large role in United Kingdom elections, where bots were leveraged to influence British public opinion.

Bots

During the Brexit Referendum, bots were used to influence public discourse on the UK's potential exit from the EU. Bots were used tactically by deploying hashtags designed to attract and influence undecided voters (Gallacher et al., 2017).

Facebook played a major role in social media discussions prior to the UK elections and referendum. In April 2017, Members of the UK Parliament requested that Facebook better prepare itself to combat fake news, indicating concern about voters in that "they could be voting based on lies" ("Facebook Publishes Fake News" 2017) Since cases such as the 2016 US Presidential Election, Facebook taken down many of the fake accounts that were tracked in the UK.

Conclusion

While there is no clear evidence recent UK elections were directly tampered with by outside actors, the elections served as examples of social media influence being used to tamper with an election outcome through meddling tools such as bots. Attribution continues to be a

difficulty in election meddling and situations involving hacktivists, yet the Russian Government was likely involved in notable hacks against British broadcasters and government agencies. The UK government has announced its intention to combat these meddling attempts, and that they expect that meddling will occur in future elections. While the UK has rebuffed major election interfering attempts in the immediate term, advances in their ability to protect from influence campaigns and cyberattacks will likely be necessary to secure their democracy in the future.

Bibliography

2016 November General Election Turnout Rates (n.d.). United States Elections Project. Retrieved January 26, 2018, from http://www.electproject.org/2016g

2017 시민의 선택. (2017, February). Kyung-Hyang Newspapers. Retrieved from http://vote2017.khan.co.kr/"

Abellan, L. (2017, November 9). Romanian eurodeputy: Catalonia is another case of malicious Russian meddling. *El Pais*. Reteieved from https://elpais.com/elpais/2017/11/09/inenglish/1510240697_816819.html

Access to electricity (% of population). (n.d.). Retrieved February 26, 2018, from https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS

Access to electricity (percent of population). (2014). World Bank. Retrieved from https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=BR

African Studies Center. (n.d.). East Africa Living Encyclopedia. Retrieved February 24, 2018, from http://www.africa.upenn.edu/NEH/kethnic.htm

Agrawal, N. (2016, December 21). The U.S. is no stranger to interfering in the elections of other countries. *LA Times*. Retrieved January 26, 2018, from http://www.latimes.com/nation/la-na-us-intervention-foreign-elections-20161213-story.html

Aladente, D. (2017, Oct 2). There's fake news in Catalonia too. *El Pais*. Retrieved from https://elpais.com/elpais/2017/10/02/inenglish/1506943013_999238.html

Alessi, Gil. (2018, Feburary 8). "Voto impresso, o retorno ao passado que opõe Bolsonaro e a Procuradoria Geral." *El País Brasil*. Retrieved fro, https://brasil.elpais.com/brasil/2018/02/07/politica/1518009776_100288.html.

Alexa. (n.d.). Retrieved January 22, 2018, from https://www.alexa.com/topsites/countries

Alexander, L. (2015, December 24). Massive LiveJournal Troll Network Pushes Pro-Kremlin Narratives. *StopFake*. Retrieved February 25, 2018 from https://www.stopfake.org/en/massive-livejournal-troll-network-pushes-pro-kremlin-narratives/

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. The Journal of Economic Perspectives, 31(2), 211–235.

Almost 700 paid news cases detected in 2014 Lok Sabha elections. (2014, May 18*). Daily News and Analysis.* Retrieved February 23, 2018, from http://www.dnaindia.com/india/report-almost-700-paid-news-cases-detected-in-2014-lok-sabha-elections-1989485

AngloInfo Italy. (n.d.). Voting in Italy, for Foreigners. Retrieved February 11, 2018, from https://www.angloinfo.com/how-to/italy/moving/voting

Anonymous. (2018, October 14). Brazil court dismisses hacker threat at presidential vote. *BBC*. Retrieved from http://www.bbc.com/news/world-latin-america-29493790

App Annie. (n.d.). Retrieved from http://www.appannie.com

Applebaum, A. (2017, October 20). Why does Putin want to control Ukraine? Ask Stalin. *The Washington Post*. Retrieved February 26, 2018, from https://www.washingtonpost.com/outlook/why-does-putin-want-control-ukraine-ask-stalin/2017/10/20/800a7afe-b427-11e7-a908-a3470754bbb9_story.html?utm_term=.d8702b71538c

Aranha, D. (2014). Fiscalize a Eleição. *Você Fiscal.* Retrieved from http://www.vocefiscal.org

Aranha, D. (2014a). Você Fiscal. Retrieved from http://www.vocefiscal.org

Arnaudo, D. (2017). Brazil, the Internet and Digital Bill of Rights. *Igarapé Institute*, 1–42. Retrieved from https://igarape.org.br/marcocivil/assets/downloads/igarape_brazil-the-internet-and-the-digital-bill-of-rights.pdf

Arnaudo, D. (2017). Computational Propaganda in Brazil: Social Bots during Elections. *Computational Propaganda Research Project*, 1–27.

Association for Democratic Reforms. (n.d.). FAQ on Election Petition. National Election Watch. Retrieved from https://adrindia.org/sites/default/files/FAQ%20on%20What%20is%20an%20election%20petition_English.pdf

Association for Demoratic Reforms. (n.d.). FAQ on Election Petition. National Election Watch. Retrieved from https://adrindia.org/sites/default/files/FAQ%20on%20What%20is%20an%20election%20petition_English.pdf

Auchincloss, L. (1985). Honorable men. Boston: Houghton Mifflin.

Ba, Diadie, et al. (2017, July 30). Senegal Parliamentary Elections Marred by Voting Problems. *Reuters.* Retrieved February 10, 2018, from www.reuters.com/article/us-senegal-politics/senegal-parliamentary-elections-marred-by-voting-problems-idUSKBN1AF0P3.

Bali, S. (2015, February 2). Edelman Trust Barometer 2015: Trust in businesses, government and media rises in India. Retrieved February 9, 2018, from

Barron, L. (February 6, 2018). North Korean Hackers May Have Stolen $530 Million From a Japanese Cryptocurrency Exchange. Fortune. Retrieved from http://fortune.com/2018/02/06/north-korea-coincheck-hack/

Baru, S. The Indian Parliamentary Elections of 2014. (2014. December 12). Encyclopedia Britannica. Retrieved from https://www.britannica.com/topic/Indian-Parliamentary-Elections-of-2014-The-2004659.

Barzachka, N. (2017, April 25). Bulgaria's government will include far-right nationalist parties for the first time. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2017/04/25/bulgarias-government-will-include-nationalist-parties-on-the-far-right-heres-why-and-what-this-means/

Baunov, A., Jarobik, B., & Golubov, A. (2015, February 25). A year After Maidan: Why did Viktor Yanukovych Flee After Signing the Agreement with the Opposition? Retrieved February 25, 2018 from http://carnegie.ru/commentary/59172

Bechev, D. (2016, November 14). A very Bulgarian drama: What Rumen Radev's presidential election victory means for Bulgarian politics. Retrieved February 9, 2018, from http://blogs.lse.ac.uk/europpblog/2016/11/14/rumen-radev-bulgaria-russia-president/

Benedictus, L. (2016, November 6). Invasion of the troll armies: 'Social media where the war goes on'. *The Guardian*. Retrieved January 21, 2018, from http://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russia

Benjamin, I. (2017, June 9). IEBC voter verification ends today. Retrieved February 9, 2018, from http://www.the-star.co.ke/news/2017/06/09/iebc-voter-verification-ends-today_c1576790

Bergamasco, D., Bronzatto, T., & Gonçalves, E. (2018, January 12). A Ameaça das "Fake News." *Veja*. Retrieved from https://veja.abril.com.br/revista-veja/a-ameaca-das-fake-news/

Berkowitz, K. (2017, October 31). Russian hacking of Illinois voter registration system did not compromise election results, experts say. *Chicago Tribune*. Retrieved February 9, 2018, from http://www.chicagotribune.com/suburbs/highland-park/news/ct-hpn-election-integrity-forum-tl-1102-20171031-story.html

Beyer, J., & Park, D. (2017, December 22). Commentary: Making sense of North Korea's hacking strategy. *Reuters.* Retrieved from https://www.reuters.com/article/us-beyer-nkorea-commentary/commentary-making-sense-of-north-koreas-hacking-strategy-idUSKBN1EF28F

Bhatnagar, G. V. (2017, May 9). AAP "Demonstrates EVM Tampering" in Delhi Assembly. *The Wire.* Retrieved February 9, 2018, from https://thewire.in/133854/aap-evm-tampering-bjp/

Bhattacharya, S. (2014, March 5). India's Election by Mind-Blowing Numbers. Retrieved February 9, 2018, from https://blogs.wsj.com/indiarealtime/2014/03/05/indias-election-by-mind-blowing-numbers/

Bhowmick, N. (2014, April 18). What Do India's 150 Million First Time Voters Want From their Leaders? *Time*. Retrieved February 9, 2018, from http://time.com/65071/india-elections-youth/

Binnie, I. (2018, February 13). Italy's Northern League dangles EU exit in election campaign. Reuters. Retrieved February 17, 2018, from https://www.reuters.com/article/us-italy-election-eu-league/italys-northern-league-dangles-eu-exit-in-election-campaign-idUSKCN1FX28Z

Biray, K. (2015, November 10). Communist nostalgia in Eastern Europe: longing for the past | openDemocracy. Retrieved February 9, 2018, from https://www.opendemocracy.net/can-europe-make-it/kurt-biray/communist-nostalgia-in-eastern-europe-longing-for-past

Birch, S. (1995). The Ukrainian parliamentary and presidential elections of 1994. Electoral Studies, 14(1), 93-99. doi:10.1016/0261-3794(95)95775-6https://ac.els-cdn.com/0261379495957756/1-s2.0-0261379495957756-main.pdf?_tid=7ed4eaf0-0d11-11e8-8980-00000aab0f01&acdnat=1518123123_7ad78f789017ed849c8c80be8a4f17b0

Bivol. (2017a, March 19). Local Trolls Spin Factory for Hybrid News and Propaganda in Favor of Bulgarian Socialists [Text]. Retrieved February 17, 2018, from https://bivol.bg/en/local-trolls-spin-factory-for-hybrid-news-and-propaganda-in-favor-of-bulgarian-socialists.html

Bivol. (2017b, March 20). V as in Vendetta, T as in Troll… [Text]. Retrieved February 17, 2018, from https://bivol.bg/en/v-as-in-vendetta-t-as-in-troll.html

Blaze, M., Braun, J., Hursti, H., Lorenzo Hall, J., MacAlpine, M., & Moss, J. (2017).

Boghassian, B. (2018, January 31). Sem Lula, Bolsonaro lidera e disputa por vaga no segundo turno se acirra. *Folha de São Paulo*. Retrieved from https://www1.folha.uol.com.br/poder/2018/01/1954606-sem-lula-disputa-por-vaga-no-segundo-turno-se-acirra.shtml

Booth, W. (2017, 14 November). Britain's May Slams Russia for Election Meddling and Fake News (Unlike President Trump). *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2017/11/14/britains-may-slams-russia-for-election-meddling-and-fake-news-unlike-president-trump/?utm_term.

Booth, W., & Birnbaum, M. (2017, November 14). Britain and Spain: Russian entities meddled in elections. *The Chicago Tribune*. Retrieved from

http://www.chicagotribune.com/news/nationworld/ct-britain-spain-russian-meddling-20171114-story.html
Booth, W., & Birnbaum, M. (2017, November 14). British and Spanish leaders say Russian trolls meddled in their elections. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/britain-and-spanish-leaders-say-russian-trolls-meddled-in-their-elections/2017/11/14/51ffb64a-c950-11e7-b506-8a10ed11ecf5_story.html?utm_term=.c23a18903ad7
Boykoff, P., Kwon, K. J., & Griffiths, J. (2017, May 10). South Korea election: Moon Jae-in declared winner. *CNN*. Retrieved from https://edition.cnn.com/2017/05/09/asia/south-korea-election/index.html
Brandt, S. T. and J. (2017, March 2). What Putin is up to, and why he may have overplayed his hand. *Brookings*. Retrieved January 26, 2018, from https://www.brookings.edu/opinions/what-putin-is-up-to-and-why-he-may-have-overplayed-his-hand/
Brazil court dismisses hacker threat at presidential vote. (2014, October 7). *BBC*. Retrieved from http://www.bbc.com/news/world-latin-america-29493790
Brazil: most popular social network apps as of June 2016. (2016, June). Statista. Retrieved from https://www.statista.com/statistics/746969/most-popular-social-network-apps-brazil/
Brazilian Mobile Operators in a Nutshell. (2014, December 9). TechInBrazil. Retrieved from https://techinbrazil.com/brazilian-mobile-operators-in-a-nutshell
Briggs, H. (1987). The International Court of Justice Lives up to its Name. The American Journal of International Law, 81(1), 78-86. doi:10.2307/2202133
Bright Election Promotion Foundation Incorporated (2013, July) 46th Lower House General Election Nationwide Opinion Survey. (財団法人 明るい選挙推進協会): 第 46 回衆議院議員総選挙全国意識調査. Retrieved from http://www.akaruisenkyo.or.jp/wp/wp-content/uploads/2013/06/070seihon1.pdf
Bright Election Promotion Foundation Incorporated (2015, August). 47th Lower House General Election Nationwide Opinion Survey. (財団法人 明るい選挙推進協会) 第47回衆議院議員総選挙全国意識調査. Retrieved from http://www.akaruisenkyo.or.jp/wp/wp-content/uploads/2011/10/47syuishikicyosa-1.pdf
Broder, J. M. (1997, March 31). Political Meddling by Outsiders: Not New for U.S. *The New York Times*. Retrieved from https://www.nytimes.com/1997/03/31/us/political-meddling-by-outsiders-not-new-for-us.html
Broderick, R. (2017, April 25). Here's How Far-Right Trolls Are Spreading Hoaxes About French Presidential Candidate Emmanuel Macron. *Buzzfeed*. Retrieved from Ihttps://www.buzzfeed.com/ryanhatesthis/heres-how-far-right-trolls-are-spreading-hoaxes-about?utm_term=.bjDE9alkKj#.qgx90w83A7
Brown, J M. (2017, May 5). Financial Times Paper-Based Voting System Slows down UK Election Results. *The Financial Times*. Retrieved from https://www.ft.com/content/57f42c12-31a1-11e7-9555-23ef563ecf9a.
Bruce Stokes. (2017, October 17). Mixed feelings on Japan's democracy. Retrieved from http://www.pewglobal.org/2017/10/17/mixed-feelings-on-japans-democracy/
Brum, E. (2016, March 18). Brazil is in danger of turning the clock back on democracy. *The Guardian*. Retrieved from

https://www.theguardian.com/commentisfree/2016/mar/18/brazil-judiciary-democracy-sergio-moro-impeach-dilma-rousseff
Bulgaria PM Borisov quits after presidential election blow. (2016, November 14). *BBC*. Retrieved January 26, 2018, from http://www.bbc.com/news/world-europe-37972526
Bulgaria World Profile. (2017, January 20) Freedom House. Retrieved February 9, 2018, from https://freedomhouse.org/report/freedom-world/2017/bulgaria
Burke, J. (2014, May 16). Narendra Modi's landslide victory shatters Congress's grip on India. *The Guardian.* Retrieved February 23, 2018, from https://www.theguardian.com/world/2014/may/16/narendra-modi-victory-congress-india-election
Burke, J., & team, G. I. (2014, April 7). Indian election 2014: your interactive guide to the world's biggest vote. *The Guardian*. Retrieved January 26, 2018, from http://www.theguardian.com/world/2014/apr/07/-sp-indian-election-2014-interactive-guide-narendra-modi-rahul-gandhi
Byeon, J. Y. (2018, Jan 18). '전자투표'에 '블록체인' 기술 활용한다. 산업일보. Retrieved from http://www.kidd.co.kr/news/199600
Byers, D. (2017, October 30). Facebook estimates 126 million people were served content from Russia-linked pages. Retrieved February 9, 2018, from http://money.cnn.com/2017/10/30/media/russia-facebook-126-million-users/index.html
Cakebread, C. (2017, September 25). Brazil is more worried about fake news than any other country. *Business Insider.* Retrieved from http://www.businessinsider.com/brazil-is-more-worried-about-fake-news-than-any-other-country-chart-2017-9
Carolina. (2016, Mach 16). Hackers can change election result using flaws in Electronic Voting Machines. *HackRead*. Retrieved from https://www.hackread.com/electronic-voting-machines-hacking-flaw/
Castaño, P. (2017, Deecmber 22). Independence parties have kept their majority in Catalonia, but right-wing parties were the real winners. *The Independent.* Retrieved from http://www.independent.co.uk/voices/catalan-elections-catalonia-independence-party-separatists-nationalist-spain-debate-a8124176.html
Castillo, M. (2011, July 22). Nicaragua may revive $17 billion claim against U.S. *CNN* Retrieved February 8, 2018, from http://www.cnn.com/2011/WORLD/americas/07/21/nicaragua.us.claim/index.html
Catalonia Election: Full Results. (2017, December 22). *The Guardian*. Retrieved from https://www.theguardian.com/world/ng-interactive/2017/dec/21/catalonia-election-full-results
Catalonia: Did voters face worst police violence ever seen in the EU? (2017, October 27). *BBC*. Retrieved from: http://www.bbc.com/news/world-europe-41677911
Catalonia's bid for independence from Spain explained. (2017, Dec 22). *BBC*. Retrieved from http://www.bbc.com/news/world-europe-29478415
Cavanaugh, D. (2016, October 30). The CIA and KGB Both Tried to Blackmail This World Leader With Sex Tapes. Retrieved February 8, 2018, from https://medium.com/war-is-boring/the-cia-and-kgb-tried-to-blackmail-this-world-leader-with-sex-tapes-927fc7ddbd48
Central Election Commission. (n.d.). Extraordinary parliamentary election 2014. Retrieved February 25, 2018 from http://www.cvk.gov.ua/pls/vnd2014/wp300e?PT001F01=910

Chacha, E. (2018, September 1). Top 10 Most Downloaded Mobile Apps in Kenya in 2018. Kenyayote. Retrieved February 25, 2018, from http://kenyayote.com/top-10-downloaded-mobile-apps-kenya-2018/

Chang, A. & Seok, S. H. (2017). 극우주의의 프레임과 감정 정치: 언어네트워크방법론을 통한 일베커뮤니티 분석 [Frame of right-wing Extremism and Emotional Politics: Analysis of Ilbe Community through Language Network Methodology]. Korean Society, 18, 3-42.

Chege, N. (2017, July 23). How campaigns are posting toxic online propaganda. Retrieved February 9, 2018, from https://www.nation.co.ke/news/politics/How-campaigns-are-posting-toxic-online-propaganda-/1064-4027764-6h3b7pz/index.html

Cheresheva, M. (2017, March 20). Turkey's Hand in Bulgarian Election Angers Sofia. Retrieved February 18, 2018, from http://www.balkaninsight.com/en/article/turkey-s-hand-in-bulgarian-election-angers-sofia-03-19-2017

Child, D. (2017, October 1). Catalonia Vote: Social media mirrors street tensions. *Al Jazeera.* Retrieved from http://www.aljazeera.com/news/2017/10/catalonia-vote-social-media-mirrors-street-tension-171001144341704.html

Chou, M. (2011, November 30). CCP interference in Taiwanese elections. Retrieved February 8, 2018, from http://blogs.nottingham.ac.uk/politics/2011/11/30/ccp-interference-in-taiwanese-elections/

Chrisanthi, A. (2013). Explaining Trust in IT-Mediated Elections: A Case Study of E-Voting in Brazil. *Journal of the Association for Information Systems*, *14*(8), 420–451.

Clayton, Mark. (2014, June 17). Ukraine election narrowly avoided wanton destruction from hackers. Retrieved February 26, 2018, from https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Clifton, D. (2017, October 12). Russian content and fake news on Twitter peaked in a key swing state right before Trump won. Retrieved January 26, 2018, from https://www.motherjones.com/politics/2017/10/twitter-bots-distorted-the-2016-election-including-many-controlled-by-russia/

Cole, M., Esposito, R., Biddle, S., & Grim, R. (2017, June 5). Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election. Retrieved January 22, 2018, from https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

Comissió d'Economia Catalana. (2015, August 25). The Economy of Catalonia - Questions and answers on the economic impact of independence. Retrieved from http://www.coleconomistes.cat/pdf/the.economy.of.catalonia.pdf

Communications Authority of Kenya. (2017). *First Quarter Sector Statistics Report for The Financial Year 2017/2018 (July-September 2017)*. Retrieved from http://ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q1%20%202017-18.pdf

Congress Passes Law Restricting Online Criticism of Candidates. (2017, October 5). *Reuters*. Retrieved from https://www.reuters.com/article/brazil-politics-censorship/brazil-congress-passes-law-restricting-online-criticism-of-candidates-idUSL8N1MG6GV

Connecting internet, telephone and TV in France. (n.d.). Expatica. Retrieved from https://www.expatica.com/fr/moving-to/A-guide-to-communication-services-in-France_101110.html

Corker, et al. (2018). Putin's Asymmetric Assault On Democracy In Russia Aand Europe: Implications For U.S. National Security. Report Prepared For The Use Of The Commitee On Foreign Relations, United States Senate.

Crampton, T. (2007, April 17). France to choose president with help of electronic voting. *The New York Times*. Retrieved from http://www.nytimes.com/2007/04/17/technology/17iht-evote.4.5324501.html

Dahir, A. L., & Kuo, L. (2017, August 9). Kenya's opposition says the election was hacked in the president's favor. Retrieved February 25, 2018, from https://qz.com/1049814/elections-in-kenya-2017-raila-odinga-says-results-were-hacked-for-president-uhuru-kenyatta/

Daniels, L. (2017, September 27). Russian Active Measures in Germany and the United States: Analog Lessons From the Cold War. Retrieved January 25, 2018, from https://warontherocks.com/2017/09/russian-active-measures-in-germany-and-the-united-states-analog-lessons-from-the-cold-war/

Daniyal, S. (2017, October 25) Congress Bots to BJP Trolls: Does Social Media Engagement Really Shape Voter Choices in India? Accessed February 9, 2018. https://scroll.in/article/855266/congress-bots-to-bjp-trolls-does-social-media-engagement-really-shape-voter-choices-in-india.

DataBank: World Development Indicators. (n.d.). The World Bank. Retrieved from http://databank.worldbank.org/data/reports.aspx?source=world-development-indicators

De Lara, B. (2018, January 16). Bate-boca Entre MBL e Bolsonaristas Alimenta Racha no Antipetismo. *Piauí*. Retrieved from http://piaui.folha.uol.com.br/bate-boca-entre-mbl-e-bolsonaristas-alimenta-racha-no-antipetismo/

Dearden, L. (2017, May 6). Emmanuel Macron hacked emails: French media ordered by electoral commission not to publish content of messages. *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/emmanuel-macron-email-hack-leaks-election-marine-le-pen-russia-media-ordered-not-publish-commission-a7721111.html

Deardon, L. (2017, Oct 2). Catalan Independence Referendum illegal under Spanish Constitution, European Commission Confirms. Retrieved from http://www.independent.co.uk/news/world/europe/catalan-independence-referendum-not-legal-spanish-constitution-european-commission-juncker-spain-law-a7978386.html

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty. (1966). The American Journal of International Law, 60(3), 662-664.

DEFCON 25 Voting Machine Hacking Village (p. 18). Retrieved from https://www.defcon.org/images/defcon-25/DEF %20CON %2025 %20voting%20village%20report.pdf

Deiz, A., & Mateo, M. (2017, Nov 10). Government confirms intervention of Russian hackers in Catalan Crisis. El Pais. Retrieved from https://elpais.com/elpais/2017/11/10/inenglish/1510329788_994258.html?rel=mas

Del Pero, M. (2001). The United States and "Psychological Warfare" in Italy, 1948-1955. The Journal of American History,87(4), 1304-1334. doi:10.2307/2674730

Desierto, D. (2017, September 16). Reopening Proceedings for Reparations and Abuse of Process at the International Court of Justice. Retrieved February 9, 2018, from https://www.ejiltalk.org/reopening-proceedings-for-reparations-and-abuse-of-process-at-the-international-court-of-justice/

Dewan, A. (2017, December 22). Separatist parties in Spain's Catalonia win majority in election. *CNN*. Retrieved from https://www.cnn.com/2017/12/21/europe/catalonia-election-results-independence-spain-intl/index.html

Dimitrova, S. (2014, October 17). Media concentration and media ownership in Bulgaria. Retrieved February 17, 2018, from https://www.balcanicaucaso.org/eng/Areas/Bulgaria/Media-concentration-and-media-ownership-in-Bulgaria-156381

Divine, R. (1972). The Cold War and the Election of 1948. The Journal of American History, 59(1), 90-110. doi:10.2307/1888388

Donadio, R. (2013, February 25). Split Vote Sends One Clear Message in Italy: No to Austerity. *The New York Times*. Retrieved February 10, 2018, from http://www.nytimes.com/2013/02/26/world/europe/Italy-elections.html

Downie, A. (2018, January 30). Ahead of elections, Brazil's police announce plan to crackdown on "fake news." Retrieved from https://cpj.org/blog/2018/01/ahead-of-elections-brazils-police-announce-plan-to.php

Duggan, B., & Said-Moorhouse, L. (2017, August 20). Kenya Supreme Court delivers election verdict. *CNN*. Retrieved January 26, 2018, from https://www.cnn.com/2017/09/20/africa/kenya-election-supreme-court/index.html

Dzhambazova, B. (2017, March 26). Bulgaria's Ex-Premier Nears Return to Power in a Key Election for Europe. *The New York Times*. Retrieved from https://www.nytimes.com/2017/03/26/world/europe/bulgaria-election-boiko-borisov.html

Edelman Trust Barometer 2017: UK Findings. (n.d.) Retrieved February 28, 2018, from https://www.edelman.co.uk/magazine/posts/edelman-trust-barometer-2017-uk-findings/

Edelman. (2018). 2018 Edelman Trust Barometer: Global Report. Retrieved from:http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

Education Statistics | Education Expenditures. (n.d.). Retrieved February 8, 2018, from http://datatopics.worldbank.org/education/wDashboard/dqexpenditures

Edwards, C. (2017, December 15). What you need to know about Italy's 2018 election. The Local.it. Retrieved February 7, 2018, from https://www.thelocal.it/20171215/what-you-need-to-know-about-italys-upcoming-2018-election

Einaudi, M. (1948). The Italian Elections of 1948. The Review of Politics, 10(3), 346-361. Retrieved from http://www.jstor.org.offcampus.lib.washington.edu/stable/1404569

Election 2015: United Kingdom Results. (2015). BBC. Retrieved from https://www.bbc.com/news/election/2015/results.

Election 2017: united Kingdom Results. (2017). BBC. Retreived from https://www.bbc.com/news/election/2017/results/england.

Election Commission of India. (2007, June 4). Right to Information Act 2005. Retrieved from https://www.scribd.com/document/6794194/Expert-Committee-Report-on-EVM

Election Commission of India. (n.d.). The Function (Electoral System). Retrieved February 9, 2018, from http://eci.nic.in/eci_main1/the_function.aspx#presidentandvicepresident

Election Guide: Democracy Assistance and Elections News. (n.d.). Country Profile: Republic of Senegal. Retrieved from https://www.electionguide.org/countries/id/190/.
Eleven Paths. (2016, March 13). Trend Report: Vulnerabilities Trends in the Second Semester of 2016. Retrieved from https://www.elevenpaths.com/informe-sobre-tendencias-en-vulnerabilidades-del-segundo-semestre-de-2016-2/index.html
Elkana, J. (2017, August 8). IEBC clerk arrested for issuing double ballot papers in Changamwe. *The Star*. Retrieved February 9, 2018, from http://www.the-star.co.ke/news/2017/08/08/iebc-clerk-arrested-for-issuing-double-ballot-papers-in-changamwe_c1612444
Enten, H. (2016, December 23). How Much Did WikiLeaks Hurt Hillary Clinton? Retrieved January 26, 2018, from https://fivethirtyeight.com/features/wikileaks-hillary-clinton/
Etter, L., Silver, V., & Frier, S. (2017, December 21). The Facebook Team Helping Regimes That Fight Their Opposition. Bloomberg.Com. Retrieved from https://www.bloomberg.com/news/features/2017-12-21/inside-the-facebook-team-helping-regimes-that-reach-out-and-crack-down
EU Referendum Results. (n.d.). The Electoral Commision. Retrieved February 28, 2018, from https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information
Eur-Lex. (2014). Voting rights and eligibility in European Parliament elections. EU legislation, Europe. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l23025
European Union Referendum Results. (n.d). The Electoral Commission. Retrieved from https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information.
Facebook Publishes Fake News Ads in UK Papers. (2017, May 8). *BBC*. Retrieved from https://www.bbc.com/news/technology-39840803.
Fagundez, I. (2018, May 26). Como exército de voluntários se organiza nas redes para bombar campanha de Bolsonaro a 2018. *BBC Brasil*. Retrieved from http://www.bbc.com/portuguese/salasocial-39837332
Fake News in the French Election. (2017, April 5). *BBC News*. Retrieved from http://www.bbc.com/news/world-europe-39495635
Faris, S. (2010, March 27). New Media Shaking Up Italy's Media Landscape. *Time.* Retrieved February 17, 2018, from http://content.time.com/time/world/article/0,8599,1975240,00.html
Felons and Voting Rights - Elections & Voting - WA Secretary of State. (n.d.). Retrieved February 8, 2018, from https://www.sos.wa.gov/elections/voters/felons-and-voting-rights.aspx
Fessler. (n.d.). 10 Months After Election Day, Feds Tell States More About Russian Hacking. Retrieved January 26, 2018, from https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking
Fessy, T. (2012, March 26). Senegal's President-Elect Macky Sall Hails 'New Era'. *BBC*. Retrieved from http://www.bbc.com/news/world-africa-17508098
Fisher, M. (2014, January 30). 9 questions about Ukraine you were to embarrassed to ask. *The Washington Post.* Retrieved February 25, 2018 from

https://www.washingtonpost.com/news/worldviews/wp/2014/01/30/9-questions-about-ukraine-you-were-too-embarrassed-to-ask/?utm_term=.955e3369f86c
Fisher, M. (2014, May 16). Who is Narendra Modi and why is the world afraid of him leading India? *Vox*. Retrieved February 9, 2018, from https://www.vox.com/2014/4/10/5597644/narendra-modi-india-elections
Fletcher, A. (2016, September 29). Russian Hacking and the U.S. Election: Against International Law? Retrieved February 7, 2018, from http://www.mjilonline.org/russian-hacking-and-the-u-s-election-against-international-law
France drops electronic voting for citizens abroad over cybersecurity fears. (2017, March 6). *Reuters.* Retrieved from https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233
France: social media usage 2016-2017 | Survey. (n.d.). Retrieved from https://www.statista.com/statistics/569791/distribution-of-social-media-used-france/
Freedom House. (2016, November 14). Freedom on the Net: Italy Country Profile. Retrieved February 17, 2018, from https://freedomhouse.org/report/freedom-net/2016/italy
Freedom House. (2017, January 26).Freedom in the World 2018: The United States . Retrieved January 22, 2018, from https://freedomhouse.org/report/freedom-world/2018/united-states
Freedom House. (2017, November 14) India Country Report | Freedom on the Net 2017. Retrieved form https://freedomhouse.org/report/freedom-net/2017/india.
Freedom House.(2016, November 22). Freedom on the Net 2016: Country Profile Ukraine. Retrieved February 26, 2018, from https://freedomhouse.org/report/freedom-net/2016/ukraine
Freedom in the World 2018: South Korea. (2018, January 5). Freedom House. Retrieved February 17, 2018, from https://freedomhouse.org/report/freedom-world/2018/south-korea
French election: Macron takes action over offshore claims. (2017, May 4). *BBC*. Retrieved from http://www.bbc.com/news/world-europe-39802776
French election: Turnout sharply down in Le Pen-Macron battle. (2017, May 7). *BBC*. Retrieved from http://www.bbc.com/news/world-europe-39833831
Fundamental Structure of the Government of Japan. (n.d.). [.go.jp]. Retrieved from http://japan.kantei.go.jp/constitution_and_government_of_japan/fundamental_e.html
Funke, D. (2014, February 19). Here's Why Fighting "Fake News" is Harder on WhatsApp than on Facebook. *Pontyer*. Retrieved from https://www.poynter.org/news/heres-why-fighting-fake-news-harder-whatsapp-facebook
Furuta, D. (October 9th, 2017) The General Election in a Period where authenticity dangers Fake News. Japan j;too has began to Fact Check. 真偽が危ういフェイクニュース時代の総選挙 日本でもファクトチェックが始まった. Buzzfeed. Retrieved from: https://www.buzzfeed.com/jp/daisukefuruta/fake-vs-fact-check-in-japan?utm_term=.epYQdPLGP#.fq3MJO5YO
Gallacher, J., et al. (2017, May 31). Junk News and Bots During the 2017 UK General Election: What Are UK Voters Sharing Over Twitter? University of Oxford. Retrieved from comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Junk-News-and-Bots-during-the-2017-UK-General-Election.pdf.
General Elections. (n.d). United Kingdom Parliament. Retrieved from www.parliament.uk/about/how/elections-and-voting/general/.

Germany starts enforcing hate speech law. (2018, January 1). *BBC*. Retrieved March 1, 2018, from http://www.bbc.com/news/technology-42510868

Gettleman, J. (2007, December 31). Disputed Vote Plunges Kenya Into Bloodshed. *The New York Times*. Retrieved from https://www.nytimes.com/2007/12/31/world/africa/31kenya.html

Gillett, F. (2017, June 12). Emmanuel Macron's La République en Marche: All you need to know about the French President's groundbreaking new party ahead of the elections. *London Evening Standard*. Retrieved from https://www.standard.co.uk/news/world/emmanuel-macrons-la-r-publique-en-marche-all-you-need-to-know-about-the-french-presidents-a3563256.html

Giuffrida, A. (2018, January 19). Italians asked to report fake news to police in run-up to election. *The Guardian.* Retrieved January 22, 2018, from https://www.theguardian.com/world/2018/jan/19/italians-asked-report-fake-news-police-run-up-election

Goldman, J. (2015). The Central Intelligence Agency : An encyclopedia of covert ops, intelligence gathering, and spies. Santa Barbara, California: ABC-CLIO, an imprint of ABC-CLIO, LLC.

Gorchinskaya, K., Rudenko, O., Schreiber, W. (2014, May 25). Authorities: Hackers foiled in bid to rig Ukraine presidential election results. KyivPost. Retreived February 25, 2018, fromhttps://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html

Gragnani, J. (2017, December 8). Exclusivo: investigação revela exército de perfis falsos usados para influenciar eleições no Brasil. *BBC Brasil*. Retrieved from http://www.bbc.com/portuguese/brasil-42172146

Gragnani, J. (2018, December 12). Como suas curtidas, "parabéns" e até cantadas dão credibilidade a fakes. *BBC Brasil*. Retrieved from http://www.bbc.com/portuguese/brasil-42173799

Gragnani, J. (2018b, December 16). Como identificar os diferentes tipos de fakes e robôs que atuam nas redes. *BBC Brasil*. Retrieved from http://www.bbc.com/portuguese/brasil-42172154

Greenberg, A. (2017, June 9). Everything we know about Russia's Election-Hacking Playbook. *Wired*. Retrieved February 25, 2018 from https://www.wired.com/story/russia-election-hacking-playbook/

Greenberg, A. (n.d.). US Hits Russia With Biggest Spying Retaliation "Since the Cold War." *Wired*. Retrieved January 31, 2018, from https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/

Greenwald, G. (2018, January 10). First France, Now Brazil Unveils Plan to Empower the Government to Censor the Internet in the Name of Stopping "Fake News." *The Intercept*. Retrieved from *https://theintercept.com/2018/01/10/first-france-now-brazil-unveils-plans-to-empower-the-government-to-censure-the-internet-in-the-name-of-stopping-fake-news/*

Greenwood, S., Perrin, rew, & Duggan, M. (2016, November 11). Social Media Update 2016. Retrieved January 26, 2018, from http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Grover, P. (2018, January 23). Public faith in Indian govt, media and NGOs dips: Edelman Trust report. Retrieved February 9, 2018, from https://theprint.in/2018/01/23/public-faith-indian-govt-media-ngos-dips-edelman-trust-report/

Gup, T. (2000). Book of Honor : Covert lives and classified deaths at the CIA (1st ed.). New York: Doubleday.

Ha, A.-Y., & Jeong, H.-B. (2018, January 29). 작전명 '레드펜'…MB 사이버사, 누리꾼 블랙리스트 관리. 한겨레. Retrieved February 9, 2018, from http://www.hani.co.kr/arti/society/society_general/829773.html

Hackers target Ukraine's election website. (2014, October 26). Phys.org. Retrieved February 25, 2018 from https://phys.org/news/2014-10-hackers-ukraine-election-website.html

Hamburger, T., & Tumulty, K. (2016, July 22). WikiLeaks releases thousands of documents about Clinton and internal deliberations. *The Washington Post.* Retrieved February 9, 2018, from https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/

Harris, S. (2016, October 16). Election Hackers Could Erase You. Retrieved February 9, 2018, from https://www.thedailybeast.com/election-hackers-could-erase-you

Hatachi, K. 2017. Was the Greatly Spread "Adolescent Japanese girls raped by a Korean person" Fake News? Websites Are Full of Errors. 大量拡散の「韓国人による日本人女児強姦」はデマニュースか　サイトは間違いだらけ. Buzzfeed. Retrieved from https://www.buzzfeed.com/jp/kotahatachi/korean-news-xyz?utm_term=.mqRXrxyqk#.ysWmBXY5Q.

Hedgecoe, G. (2017, October 6). Catalonian media reflect polarised Spanish society. BBC. Retrieved from http://www.bbc.com/news/world-europe-41517569

Henni, A. (2014, April 22). Vkontakte founder forced to resign after revealing anti-maidan pressure from FSB. Retrieved February 25, 2018 from http://www.ewdn.com/2014/04/22/durov-says-he-gave-up-vkontakte-share-because-of-anti-maidan-pressure-from-fsb/

Hern, A. (2015, February 26). Should Britain introduce electronic voting*? The Guardian*. Retrieved February 28, 2018, from https://www.theguardian.com/technology/2015/feb/26/should-britain-introduce-electronic-voting

Hill, J. (2014, February 24). In India's National Election, Don't Trust the Polls. The Diplomat. Retrieved February 9, 2018, from https://thediplomat.com/2014/02/in-indias-national-election-dont-trust-the-polls/

Hill, S. (2017). Bulgaria. In *World Encyclopedia of the Nations* (14th ed., pp. 131–149). *Farmington Hills, MI: Gale*. Retrieved from http://go.galegroup.com.offcampus.lib.washington.edu/ps/retrieve.do?docId=GALE%7CCX3652100248&userGroupName=wash_main&inPS=true&contentSegment=&sort=RELEVANCE&prodId=GVRL&searchId=R1&tabID=T003&resultListType=RESULT_LIST&curren&curren=&authCount=1&u=wash_main#

Hootsuite. (2017, January 26). Digital in 2017: Southern Europe. Retrieved February 18, 2018, from https://www.slideshare.net/wearesocialsg/digital-in-2017-southern-europe

Horowitz, J. (2016, December 2). Spread of Fake News Provokes Anxiety in Italy. *The New York Times*. Retrieved February 19, 2018, from

https://www.nytimes.com/2016/12/02/world/europe/italy-fake-news.html?mtrref=www.google.com
Horowitz, J. (2017, October 18). In Italian Schools, Reading, Writing and Recognizing Fake News. *The New York Times*. Retrieved January 22, 2018, from https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html
Hosenball, M. (2017, May 9). U.S. increasingly convinced that Russia hacked French election: sources. *Reuters*. Retrieved from https://www.reuters.com/article/us-france-election-russia/u-s-increasingly-convinced-that-russia-hacked-french-election-sources-idUSKBN1852KO
Hume, T. (2018, January 31).Modi Might Be the Only World Leader Whose Twitter Use Is More Problematic than Trump's. *VICE News*. Retrieved from https://news.vice.com/en_us/article/zmqaq3/modi-might-be-the-only-world-leader-whose-twitter-use-is-more-problematic-than-trumps.
Hussein, A. (2017, August 10). All you need to know about Form 34A and 34B in the just concluded Kenyan election. Retrieved February 9, 2018, from https://www.tuko.co.ke/248970-all-form-34a-34b-concluded-kenyan-election.html
Hwang, B.-Y., & Son, B.-K. (2007, December 19). 이명박 48.7%, 정동영 26.2%, 이회창 15.1%. Oh My News. Retrieved February 9, 2018, from http://www.ohmynews.com/nws_web/view/at_pg.aspx?CNTN_CD=A0000794353
Ignatius, D. (2010, February 25). Tehran's vote-buying in Iraq. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/24/AR2010022403479.html
In the face of Catalan insurrection, the law but not just the law. (2017, October 2). *El Pais*. Retrieved from https://elpais.com/elpais/2017/10/02/inenglish/1506937805_216609.html
Independent Electoral and Boundaries Commision . (2017, October 30). Fresh Presidential Election Results County Summary. Retrieved from https://www.iebc.or.ke/uploads/resources/A1wUl9EnMM.pdf
Individuals using the Internet (% of population) | Data. (n.d.). [International Organization]. Retrieved January 22, 2018, from https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=US
Internet Service Providers in Brazil. (2015, November 12). TechInBrazil. Retrieved from https://techinbrazil.com/internet-service-providers-in-brazil
Internet Usage In Brazil. (2016). Statista. Retrieved from https://www.statista.com/topics/2045/internet-usage-in-brazil/
Internet World Stats. (n.d.) Senegal Internet Usage and Telecommunications Reports, Retrieved from https://www.internetworldstats.com/af/sn.htm
Ishikawa Shourai (2017) General Election Prefectural Police Management Headquarters / Ishikawa. ２０１７衆院選：県警が取締本部　／石川 2017
Italy's foreign ministry came under cyber attack in 2016: (2017, February 10). Reuters. Retrieved January 22, 2018, from https://www.reuters.com/article/us-italy-cyber/italys-foreign-ministry-came-under-cyber-attack-in-2016-source-idUSKBN15P25K
J-NSC LDP Net Supporters Club 自民党ネットサポーターズクラブ. (n.d.). Retrieved from http://www.j-nsc.jp/
Jackson, Mark. (n.d.). Top 10 Broadband ISPs. IS Preview, Retrieved from www.ispreview.co.uk/review/top10.php.

Jahateh, L. (2012, January 28). Controversy of Abdoulaye Wade's Presidential Bid. *Al Jazeera*. Retrieved from https://www.aljazeera.com/indepth/opinion/2012/01/201212712295177724.html .

Jang, M.-R. (2013, January 31). 국정원, 여직원 대선 개입 의혹 일축. Frontier Times. Retrieved February 9, 2018, from http://frontiertimes.co.kr/news/htmls/2013/01/20130131103276.html?ckattempt2

Japan |United Nations Educational, Scientific and Cultural Organization. (n.d.) Retrieved from http://uis.unesco.org/country/JP.

Jeon, S.-M. (2013, February 4). 김기용 경찰청장 "국정원 여직원 수사 왜곡·은폐 없다" Naver News, News1. Retrieved February 9, 2018, from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=421&aid=0000155638&sid1=001

Jeong, J.-H. (2017, September 7). 해결사로 뜬 케이보팅, 단식농성 부른 대학갈등까지 끝내. *Korea Times*. Retrieved February 17, 2018, from http://www.hankookilbo.com/v/39328be053704452a527df2c955ac23d

Jo, H.-R. (2012, December 12). 국정원 직원 "문재인 후보 비방 댓글 단 적 없다" Naver News, NoCut News. Retrieved February 9, 2018, from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=079&aid=0002422919&sid1=001

Jones, G., & Cinelli, A. (2017, October 5). Hacking attacks: a pre-election setback for Italy's 5-Star Movement. *Reuters*. Retrieved January 22, 2018, from https://www.reuters.com/article/us-italy-politics-5star/hacking-attacks-a-pre-election-setback-for-italys-5-star-movement-idUSKBN1CA1TM

Joshua Arnold WIlliams. (2017). Electoral Campaigning and the Internet in Japan in the 2010s (Dissertation). University of Washington, Seattle, Washington.

Kamara, A. (2017, March 5). Senegal: Why Did President Sall Pardon a Rival Convicted of Embezzling over $200 Million?. African Arguments. Retrieved from https://www.africanarguments.org/2016/07/26/senegal-why-did-president-sall-pardon-a-rival-convicted-of-embezzling-over-200-million/.

Kapur, A., & Saradzhyan, S. (n.d.). For Russia and America, Election Interference Is Nothing New: 25 Stories | Russia Matters. Retrieved January 25, 2018, from https://www.russiamatters.org/analysis/russia-and-america-election-interference-nothing-new-25-stories

Karimi, F., Elbagir, N., & Smith-Spark, L. (2013, March 31). Kenya's top court upholds Kenyatta win in disputed election. *CNN*. Retrieved February 24, 2018, from https://www.cnn.com/2013/03/30/world/africa/kenya-election-ruling/index.html

Karpenko, O. (2013, March 4). Почти 10 млн пользователей из Украины заходят во «ВКонтакте» каждые сутки. Retrieved from https://ain.ua/2013/03/04/ukraincy-generiruyut-20-vsego-trafika-vkontakte

Kelley, K. (2017, December 14). US media firm targeted Raila with attack ads: Report. *Daily Nation*. Retrieved February 17, 2018, from https://www.nation.co.ke/news/politics/US-media-firm-targeted-Raila-with-attack-ad/1064-4228788-32k95t/index.html

Kemp, S. (2017, January 24). Digital in 2017: Global Overview. *We Are Social*. Retrieved from https://wearesocial.com/special-reports/digital-in-2017-global-overview

Kenya Results Hacked, Opposition Says. (2017, August 9). *BBC News*. Retrieved from http://www.bbc.com/news/world-africa-40872778

Kenya's election may turn nasty as the opposition disputes the count. (2017, August 10). *The Economist*. Retrieved from https://www.economist.com/news/middle-east-and-africa/21726096-opposition-leader-raila-odinga-refuses-accept-defeat-or-tell-his-followers

Keyishian, A. (2016, November 07). This is what voting looks like around the world. Retrieved February 26, 2018, from https://www.recode.net/2016/11/7/13507916/voting-images-around-world-polling-ballots

Kim, H. J. (2014). 인터넷 커뮤니티 '일베저장소'에서 나타나는 혐오와 열광의 감정동학 [Dynamics of Cyber Hate and Effervescence: Focusing on the Korean Internet Community "Ilbe-Joejangso']. Seoul National University.

Kim, H. Y. (2017). 토픽 모델링을 활용한 가짜 뉴스에 관한 탐색적 연구 [An Exploratory Study on Fake News Using Topic Modeling]. Yonsei University.

Kim, J. W. (2015, Aug 11). 선관위 온라인 투표 시스템 '보안 결함'. Korea Times. Retrieved from http://www.hankookilbo.com/v/3de424b91f724abfb6267054a01801d5

Kimutai, C., & Okumu, P. (2017, August 12). Uhuru Kenyatta got 8.2 million votes against Raila's 6.7 million. Retrieved February 24, 2018, from https://www.standardmedia.co.ke/article/2001251033/uhuru-kenyatta-got-8-2-million-votes-against-raila-s-6-7-million

Kirchgaessner, S. (2017, February 10). Russia suspected over hacking attack on Italian foreign ministry. *The Guardian*. Retrieved January 22, 2018, from https://www.theguardian.com/world/2017/feb/10/russia-suspected-over-hacking-attack-on-italian-foreign-ministry

Kirkpatrick, D. (2017, November 14) British Cybersecurity Chief Warns of Russian Hacking. *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/14/world/europe/britain-russia-cybersecurity-hacking.html.

Kiselyova, M., Prentice, A. (2017, May 17). Russian social media site tells Ukrainians how to dodge web block. *Reuters*. Retrieved from https://www.reuters.com/article/us-ukraine-crisis-sanctions/russian-social-media-site-tells-ukrainians-how-to-dodge-web-block-idUSKCN18D1ZY

Klein, A. (2017, August 23). NSA Whistleblower: Russia 'Hack' of DNC Server an 'Outright Lie.' *Breitbart*. Retrieved February 9, 2018, from http://www.breitbart.com/jerusalem/2017/08/23/exclusive-nsa-whistleblower-russia-hack-dnc-server-outright-lie/

Kohlil, K. (2013, October 11). Congress vs BJP: The curious case of trolls and politics. *Times of India*. Retrieved February 23, 2018, from https://timesofindia.indiatimes.com/india/Congress-vs-BJP-The-curious-case-of-trolls-and-politics/articleshow/23970818.cms

Kota, H., Daichi, I., & Craig, S. (February 8th, 2017). This Unemployed Guy Made Japanese Fake News And Ended Up Losing A Bunch Of Money. *Buzzfeed*. Retrieved from https://www.buzzfeed.com/kotahatachi/fake-in-japan?

Kramer, M. (2017, January 10). The Deep Soviet Roots Of The Russian Election-Hacking Campaign. Retrieved February 8, 2018, from http://www.wbur.org/cognoscenti/2017/01/10/vladimir-putin-donald-trump-mark-kramer

Kriegler, J., & Aboud, I. (2008). *Report of the Independent Review Commission on the General Elections held in Kenya on 27 December 2007* (p. 153). Nairobi: Harambee House. Retrieved from http://aceproject.org/regions-en/countries-and-territories/KE/reports/independent-review-commission-on-the-general

Krishnan, M. (2017, September 10). How fake news is widening social rifts in India | Asia| An in-depth look at news from across the continent. DW News. Retrieved February 23, 2018, from http://www.dw.com/en/how-fake-news-is-widening-social-rifts-in-india/a-40875997

KTN News Kenya. (2017). *The Round Table: How the voting process will be conducted (Tutorial)*. Mombasa Road: Standard Group Centre. Retrieved from https://www.youtube.com/watch?v=995zvG_ih4A

Kumar, R. (2017, December 11). The growing tide of fake news in India. *Al Jazeera.* Retrieved February 23, 2018, from http://www.aljazeera.com/news/2017/12/growing-tide-fake-news-india-171210122732217.html

Kumar, S. (2014, May 30). Who did India's Muslims vote for in general election?. *BBC*. Retrieved February 23, 2018, from http://www.bbc.com/news/world-

Kwong, J. (2017, September 28). Twitter Users Got More Fake News Than Real News Before Trump Won Election [News]. Retrieved February 9, 2018, from http://www.newsweek.com/twitter-users-got-more-fake-news-real-news-trump-won-election-673720

Lakimova, M., & Vatsov, D. (2017, October 18). Co-opting discontent: Russian propaganda in the Bulgarian media. *Eurozine*. Retrieved January 26, 2018, from http://www.eurozine.com/co-opting-discontent-russian-propaganda-in-the-bulgarian-media/?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_rts_editorial_strategy_and_a_list_of_regular_visitors&utm_term=2017-10-24

Lal, A. (2017). India Social: How Social Media is Leading the Charge and Changing the County. Hachette India.

Lang'at, P., & Ngirachu, J. (2018, October 30). Uhuru Kenyatta declared winner of repeat poll. *Daily Nation*. Retrieved January 25, 2018, from https://www.nation.co.ke/news/politics/Uhuru-winner-of-repeat-poll/1064-4162124-athns6/index.html

Législatives Assemblée Nationale - Questions About Voting. (n.d.). Retrieved from http://www.elections-legislatives.fr/en/voting.asp

Lesaca, J. (2017, November 13). The Zombies of Disinformation. El Pais. Retrieved from https://elpais.com/elpais/2017/11/13/inenglish/1510570815_085847.html

Leviev-Sawyer, C. (2017, December 8). More than 67% of Bulgarian households have home internet, close to 18% shop online. *Independent Balkan News Agency.* Retrieved January 26, 2018, from http://www.balkaneu.com/more-than-67-of-bulgarian-households-have-home-internet-close-to-18-shop-online/

Levin, D. (2016). Partisan electoral interventions by the great powers: Introducing the PEIG Dataset. Conflict Management and Peace Science, 073889421666119.

Lewis, P., & Times, S. to the N. Y. (1986, June 28). World Court Supports Nicaragua After U.s. Rejected Judges' Role. *The New York Times.* Retrieved from

http://www.nytimes.com/1986/06/28/world/world-court-supports-nicaragua-after-us-rejected-judges-role.html
List of ISP in Senegel. (n.d). Satellite Providers. Retrieved from www.allisps.com/en/offers/SENEGAL.
Lister, T. (2012, April 18). Sex and espionage: A long and sordid history [CNN]. Retrieved February 8, 2018, from http://security.blogs.cnn.com/2012/04/18/sex-and-espionage-a-long-and-sordid-history/
Local Governance (Policy Making and Civil Society) (2007) 地方自治研修 (2007). Election System in Japan. 選挙制度. Retrieved from http://www.parliament.am/library/norelectoral%20law/chaponia.pdf
Londoño, E. (2018, February 28). Brasil combate notícias falsas antes das eleições. Retrieved from http://internacional.estadao.com.br/noticias/nytiw,brasil-combate-noticias-falsas-antes-das-eleicoes,70002206845
Luconi, S. (2000). Anticommunism, Americanization, and Ethnic Identity: Italian Americans and the 1948 Parliamentary Elections in Italy. The Historian, 62(2), 285-302. Retrieved from http://www.jstor.org.offcampus.lib.washington.edu/stable/2445209
Lynch, G. (2011, November 1). *I Say to You: Ethnic Politics and the Kalenjin in Kenya*. Chicago: University of Chicago Press. Print.
Macron plans law to fight "fake news" in 2018. (2018, January 3). *Reuters*. Retrieved March 1, 2018, fromhttps://www.reuters.com/article/us-france-macron/macron-plans-law-to-fight-fake-news-in-2018-idUSKBN1ES1LJ
Makarenko, Olena, (2017, November 10). Why the Ukrainian parliament voted to change the election system against its own will. Retrieved February 26, 2018, from http://euromaidanpress.com/2017/11/11/why-the-ukrainian-parliament-voted-to-change-the-election-system-against-its-own-will/
Manevich, D. (2017, November 6). Dissatisfaction was widespread in Spain even before Catalan secession vote. Retrieved from http://www.pewresearch.org/fact-tank/2017/11/06/dissatisfaction-was-widespread-in-spain-even-before-catalan-secession-vote/
Mari, A. (2014, October 3). Fraud Possible in Brazil's E-Voting System. ZDNet. Retrieved from http://www.zdnet.com/article/fraud-possible-in-brazils-e-voting-system/
Markoff, M. (2017, June 26). Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved March 1, 2018, from /remarks/7880
Marwick, A., & Lewis, R. (2017). Media Manipulation and Disinformation Online. Data & Society Research Institute. Retrieved from https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf
Masters, J. (2017, August 3). Kenyan elections 2017: What you need to know. *CNN*. Retrieved February 9, 2018, from https://www.cnn.com/2017/08/02/africa/kenya-election-guide/index.html
Matoso, F. (n.d.). Governo Dilma tem aprovação de 9% aponta pesquisa IBOPE [News Article]. Retrieved from https://web.archive.org/web/20170108192305/http://g1.globo.com/politica/noticia/2015/07/governo-dilma-tem-aprovacao-de-9-aponta-pesquisa-ibope.html

Matthew M. Carlson, S. R. R. (2018). *Political Corruption and Scandals in Japan*. Cornell University Press.

Mattila, L. (2017, February 14). International Law and Election Interference. Retrieved February 7, 2018, from https://5clpp.com/2017/02/13/international-law-and-election-interference/

McAuley, J. (2017, May 6). France starts probing 'massive' hack of emails and documents reported by Macron campaign. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/macrons-campaign-says-it-has-been-hit-by-massive-hack-of-emails-and-documents/2017/05/05/fc638f18-3020-11e7-a335-fa0ae1940305_story.html

McCurry, J. (2017, June 25). Park Geun-hye: South Korean court removes president over scandal. *The Guardian.* Retrieved from https://www.theguardian.com/world/2017/mar/10/south-korea-president-park-geun-hye-constitutional-court-impeachment

Media users in Spain 2016, (2016). Statista. Retrieved from https://www.statista.com/statistics/759290/media-users-in-spain-by-type-of-media-and-gender/

Mejdini, F., Rudic, F., Theresheva, M., Marusic, S. J., & Morina, D. (2017, December 7). Fight-Back Starts Against Balkan 'Fake News' Machines. Retrieved February 17, 2018, from http://www.balkaninsight.com/en/article/fight-back-starts-against-balkan-fake-news-machines-12-01-2017

Menon, Rajan and Rumer, Boris (2015) Conflict in Ukraine: the Unwinding of the Post-Cold War Order, Boston, MA: MIT Press.

Menya, W., Mwere, D., Githae, W., Ngirachu, J., & Langat, P. (2017, August 10). Shock and surprise in Day Two of vote count. *Daily Nation*. Retrieved February 17, 2018, from https://www.nation.co.ke/news/politics/Raila-digs-in-on-electoral-fraud-claims--Uhuru-widening-gap/1064-4051944-u6ha7x/index.html

Meyer, J. (n.d.). Cozy Bear Explained: What You Need to Know About the Russian Hacks - *NBC News*. Retrieved February 9, 2018, from https://www.nbcnews.com/storyline/hacking-in-america/cozy-bear-explained-what-you-need-know-about-russian-hacks-n648541

Mian, A., & Rosenthal, H. (2016). Introduction: Big Data in Political Economy. RSF: The Russell Sage Foundation Journal of the Social Sciences, 2(7), 1. doi:10.7758/rsf.2016.2.7.01https://rsf.org/sites/default/files/journalists_and_media_in_ukraine_-_rsf_2016.pdf

Mikule. (n.d.). 25 February 1948 - the Communists' "bloodless coup" | Radio Prague. Retrieved January 25, 2018, from http://www.radio.cz/en/section/curraffrs/25-february-1948-the-communists-bloodless-coup

Miller, James. (2006). "Roughhouse Diplomacy: The United States Confronts Italian Communism, 1945-1958," Storia delle Relazioni Internazionali (Florence), 5 (no. 2, 1989), 295;

Millichap, Sion. (2018, January 30). Brexit: Newsroom - European Commission. Retrieved from https://europa.eu/newsroom/highlights/special-coverage/brexit_en.

Millichip, S. (2018, January 30). Brexit. Retrieved February 28, 2018, from https://europa.eu/newsroom/highlights/special-coverage/brexit_en

Millions of social bots invaded Twitter! – Emilio Ferrara, Ph.D. (n.d.). Retrieved January 26, 2018, from http://www.emilio.ferrara.name/2017/03/14/millions-of-social-bots-invaded-twitter/

Minchenko, O. (2013, October 25). Вже 3 мільйони українців користуються Facebook. *Watcher*. Retrieved from http://watcher.com.ua/2013/10/25/vzhe-3-milyony-ukrayintsiv-korystuyutsya-facebook/

Minder, R. (2017, December 21). Catalonia Election Gives Separatists New Lift. *The New York Times.* Retrieved from https://www.nytimes.com/2017/12/21/world/europe/catalan-separatists-keep-majority-in-regional-vote.html

Ministry of Internal Affairs and Communications (MIC). 総務所. 電磁的記録式投票制度について. About Electronic Record Type Voting System http://www.soumu.go.jp/senkyo/senkyo_s/news/touhyou/denjiteki/index.html.

Mireya Solís, J. M. (2017, October 25). Four questions about Japan's snap election, answered. Brookings. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2017/10/25/four-questions-about-japans-snap-election-answered/

Misukiru. (n.d.). Netto Uyo Largely Spies by the LDP Confirmed! Large Mobilization of Part Time Workers Online Counterplan ネトウヨが自民党工作員だった事実が判明！バイトの大量動員でネット対策. Naver. Retrieved from https://matome.naver.jp/odai/2144299876931181001

Mitra, S. K., & Schöttli, J. (2016). India's 2014 General Elections. Asian Survey, 56(4), 605. https://doi.org/10.1525/as.2016.56.4.605

Mortimer, C. (2016, September 25). Russian Hackers Tried to Disrupt UK General Election, Security Sources Say. The Independent. Retrieved from https://www.independent.co.uk/news/uk/home-news/russian-hackers-tried-to-disrupt-uk-general-election-security-sources-say-a7329406.html.

Most popular social networks in Japan as of October 2017, ranked by audience reach. (October, 2017). Statista. Retrieved from https://www.statista.com/statistics/258849/most-popular-social-networks-in-japan-ranked-by-reach/

Murdered official's identity used to "hack Kenyan election results". (2017, August 9). Agence France-Presse. Retrieved January 26, 2018, from http://www.thejournal.ie/kenya-election-2-3536460-Aug2017/

Mutahi, P. (2016, May 16). Eight years later, little has been learnt from the Kriegler Commission. *Daily Nation.* Retrieved February 25, 2018, from https://www.nation.co.ke/oped/opinion/-little-has-been-learnt-from-the-Kriegler-Commission/440808-3204984-6rgechz/index.html

Mutung'u, G. (2017, January 4). A Brief on Technology and Elections in Kenya 2017. Retrieved January 25, 2018, from http://www.diplointernetgovernance.org/profiles/blogs/a-brief-on-technology-and-elections-in-kenya-2017

Najibullah, F. (2014, May 26). Russian TV announces Right Sector Leader Led Ukrainian Polls. Retrieved February 25, 2018 from https://www.rferl.org/a/russian-tv-announces-right-sector-leader-yarosh-led-ukraine-polls/25398882.html

Nardelli, A., & Silverman, C. (2016, November 29). Italy's Most Popular Political Party Is Leading Europe In Fake News And Kremlin Propaganda. *Buzzfeed.* Retrieved February 11, 2018, from https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fak?utm_term=.tjJpnjWWZ#.aol5wvZZ4

National Election Commission. (n.d.) Retrieved February 28, 2018, Retreived from http://www.nec.go.kr/portal/bbs/list/B0000254.do?menuNo=200054
National Law Information Center. (n.d.). [representative legal information website]. Retrieved January 23, 2018, from http://www.law.go.kr/lsInfoP.do?lsiSeq=195320&chrClsCd=010202&urlMode=lsInfoP&efYd=20170726#0000
Naydenov, M. (2017, December 16). Hybrid war as a challenge to the national security of Bulgaria. *StopFake*. Retrieved January 25, 2018, from https://www.stopfake.org/en/hybrid-war-as-a-challenge-to-the-national-security-of-bulgaria/
Ndonga, S. (2017, October 10). IEBC systems were never hacked, says Chiloba. Retrieved February 25, 2018, from https://www.capitalfm.co.ke/news/2017/08/iebc-systems-were-never-hacked-says-chiloba/
Newton, M. (2017, September 6). Russia Media Profile: Digital Patriotism and a Nationalist Agenda. International Policy Institute. The Henry M. Jackson School of International Studies. University of Washington. Retrieved February 26, 2018, from https://jsis.washington.edu/news/russia-media-profile-digital-patriotism-nationalist-agenda/
Nimmo, B., & Pellegatta, A. (2018, January 25). #ElectionWatch: Italy's Self-Made Bots. Medium. Retrieved February 9, 2018, from https://medium.com/dfrlab/electionwatch-italys-self-made-bots-200e2e268d0e
Noack, R. (2018, February 19). In the war against election interference, Italy takes the lead. *The Washington Post*. Retrieved February 24, 2018, from https://www.washingtonpost.com/news/worldviews/wp/2018/02/19/in-the-war-against-election-meddling-italy-takes-the-lead/?utm_term=.6cf4b8b4d7e0
Nougayrède, N. (2017, April 12). Spectre of Russian influence looms large over French election. *The Guardian.* Retrieved from https://www.theguardian.com/world/2017/apr/12/russian-influence-looms-over-french-election
Odhiambo, N. (2017, October 11). Where are Msando killers? Family asks. *Daily Nation*. Retrieved January 26, 2018, from https://www.nation.co.ke/news/Chris-Msando-family-cries-for-justice/1056-4135182-5oh8nw/index.html
Odinga, R. (2017a, August 9). NASA Presidential Campaign Secretariat Briefing on the 2017 Presidential Elections We Got Them. Retrieved from http://www.odm.co.ke/component/content/article/111-breaking-news/359-briefing-on-the-2017-presidential-elections?Itemid=437
Odinga, R. (2017b, August 9). Presidential Election 2017 Briefing: COMPUTER LOGS | Facebook. Retrieved February 17, 2018, from https://www.facebook.com/media/set/?set=a.1197985420306852.1073741844.301058486666221&type=3
Odo, S., & Stapczynski, S. (October 4, 2017). A 3-Day-Old Japanese Political Party Has Already Overtaken Abe's on Twitter. Retrieved from https://www.bloomberg.com/news/articles/2017-10-05/in-days-this-party-gains-more-twitter-followers-than-abe-s-ldp
OECD (2018), Internet access (indicator). doi: 10.1787/69c2b997-en (Accessed on 18 February 2018) Retrieved from https://data.oecd.org/ict/internet-access.htm

Office for Democratic Institutions and Human Rights. (2016). Republic of Bulgaria Presidential Election 2016. Retrieved from http://www.osce.org/office-for-democratic-institutions-and-human-rights/elections/bulgaria/248771?download=true

Office for Democratic Institutions and Human Rights. (2017). Republic of Bulgaria Early Parliamentary Elections 26 March 2017. Retrieved from http://www.osce.org/odihr/elections/bulgaria/327171?download=true

Official 2016 Presidential General Election Results. (2017, January 30). Federal Elections Commission. Retrieved from https://transition.fec.gov/pubrec/fe2016/2016presgeresults.pdf

Ogemba, P., & Muthoni, K. (2017, August 31). Presidential petition: What scrutiny of key IEBC forms revealed. Retrieved February 9, 2018, from https://www.standardmedia.co.ke/article/2001253102/presidential-petition-what-scrutiny-of-key-iebc-forms-revealed

Okumu, P. (2017, September 1). Supreme Court upholds Raila's petition. Retrieved February 24, 2018, from https://www.standardmedia.co.ke/article/2001253270/supreme-court-upholds-raila-s-petition

Ombuor, R. (2017, September 5). Kenyan opposition leader rejects new presidential poll, demands 'guarantees' against fraud. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/africa/kenyan-opposition-leader-rejects-new-presidential-election-demands-guarantees-against-fraud/2017/09/05/ee6e5312-9244-11e7-89fa-bb822a46da5b_story.html?utm_term=.054da67f633d

Organization for Security and Cooperation in Europe. (2014, May 30). Ukraine's 2014 Early Presidential Election in Numbers. Retrieved February 25, 2018 from http://www.osce.org/odihr/elections/ukraine/119271

Organization for Security and Cooperation in Europe. (n.d.). Ukraine, Early Presidential Elections 25 May 2014: Final Report. Retrieved February 26, 2018, from http://www.osce.org/odihr/elections/ukraine/120549

Ortega Dolz, P. (2017, December 12). Spanish authorities working to combat bots, hackers ahead of Catalan election. *El Pais*. Retrieved from: https://elpais.com/elpais/2017/12/12/inenglish/1513072524_230884.html

Ortega Dolz, P. (2017, December 21). Spanish authorities working to combat bots, hackers ahead of Catalan election. *El Pais*. Retrieved from https://elpais.com/elpais/2017/12/12/inenglish/1513072524_230884.html

Osnos, E., Remnick, D., & Yaffa, J. (2017, February 24). Trump, Putin, and the New Cold War. *The New Yorker.* Retrieved from https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

Owino, S. (2017, August 10). IEBC: There was attempt to hack system, it failed. *Daily Nation*. Retrieved February 17, 2018, from https://www.nation.co.ke/news/Kenya-Election-Hacking-IEBC-/1056-4051976-dv9uvyz/index.html

Paganini, P. (2017, February 10). Russia suspected over cyber espionage campaign on the Italian foreign ministry. Security Affairs. Retrieved February 17, 2018, from http://securityaffairs.co/wordpress/56157/intelligence/italian-foreign-ministry-hacked.html

Panda, A. (2014, March 19). How India's National Elections Work. The Diplomat. Retrieved February 9, 2018, from https://thediplomat.com/2014/03/how-indias-national-elections-work/

Pandey, A. (2017, November 24). Electronic Voting Machine EVM Tampering Accusations In Uttar Pradesh UP Local Body Polls. New Delhi Television Limited. Retrieved February 23, 2018, from https://www.ndtv.com/india-news/electronic-voting-machine-tampering-accusations-in-up-local-body-polls-1779349

Park, W.-K. (2013, February 6). 양파껍질처럼 계속 나오는 국정원 여직원 사건. Naver News, SBS. Retrieved February 9, 2018, from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=096&aid=0000224739&sid1=001

Parkinson, J., & Kantchev, G. (2017, March 23). Document: Russia Uses Rigged Polls, Fake News to Sway Foreign Elections. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/how-does-russia-meddle-in-elections-look-at-bulgaria-1490282352

Penev, D. (2017, November 20). Anatomy of Fake News: The Bulgarian Case. *South East European Network for Professionalization of Media.* Retrieved January 26, 2018, from http://seenpm.org/anatomy-fake-news-bulgarian-case/

Perlroth, N., Wines, M., & Rosenberg, M. (n.d.). Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny. The New York Times. Retrieved February 9, 2018, from https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html

Polling Place Equipment - November 2016. (2013, August 1). *The Verifier*. Retrieved January 22, 2018, from https://www.verifiedvoting.org/verifier/

Polyakova, A., et al. (2016, November 15) The Kremlin's Trojan Horses. The Atlantic Council. Retrieved from http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses

Population Clock. (2018, January 21). [Government]. Retrieved January 22, 2018, from https://www.census.gov/popclock/

Population Estimates by Age (Five-Year Groups) and, Sex August 1, 2017 (Final estimates), January 1, 2018 (Provisional estimates). (n.d.) Statistics Bureau, Ministry of Internal Affairs and Communications. Retrieved from http://www.stat.go.jp/english/data/jinsui/tsuki/index.htm

Population, total | Data. (n.d.). World Bank. Retrieved January 24, 2018, from https://data.worldbank.org/indicator/SP.POP.TOTL

Poroshenko Restricts Access to Russian Websites, Social Networks. (2017, May 17). RadioFreeEurope. Retrieved February 25, 2018 from https://www.rferl.org/a/ukraine-poroshenko-restricts-access-yandex-vkontakte/28490951.html

Poroshenko wins presidential election with 54.7% of vote-CEC. (2014, May 29). Ukrainian Radio. Retrieved February 25, 2018 from https://web.archive.org/web/20140529212731/http://www.nrcu.gov.ua/en/148/566632/

Poushter, Jacob. (2007, June 1). British Divided on Brexit Impact as New Elections Loom. Pew Research Center's Global Attitudes Project. Retrieved from https://www.pewglobal.org/2017/06/01/british-divided-on-brexit-impact-as-new-elections-loom/.

Prasad, Y. (2014, December 31). The India Elections 2014. Retrieved February 9, 2018, from http://infoweb.newsbank.com/apps/news/document-view?p=WORLDNEWS&t=pubname%3APNHK%21New%2BHorizons%2B%2528Karachi%252C%2BPakistan%2529&sort=YMD_date%3AD&fld-base-0=alltext&maxresults=20&val-base-0=india%20elections%202014&docref=news/14FED0FCD0494408

Privacy International. (2017, December 13). Texas media company hired by Trump created Kenyan president's viral 'anonymous' attack campaign. Retrieved February 9, 2018, from https://medium.com/@privacyint/texas-media-company-hired-by-trump-created-kenyan-presidents-viral-anonymous-attack-campaign-edd507812039

Program for the International Assessment for Adult Competencies (PIAAC) - What does the cognitive assessment of PIAAC measure? (2014). Retrieved January 22, 2018, from https://nces.ed.gov/surveys/piaac/results/summary.aspx

Public Election Law Violation Suspects, Towards Work on 60 cases, the End of The Lower House election 公選法違反容疑、６０件の捜査着手へ　衆院選の終了後. (October, 2017). Asahi Shinbun. Retrieved from https://www.asahi.com/articles/ASKBP5D7JKBPUTIL017.html

Public Office Election Law 公職選挙法. (n.d.). e-Gov. Ministry of Internal Affairs and Communications. Retrieved from http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=325AC1000000100&openerCode=1#1374

Rajah, N. L. (2014, May 19). Don't dismiss those election petitions. *The Hindu*. Retrieved from http://www.thehindu.com/opinion/op-ed/Don%E2%80%99t-dismiss-those-election-petitions/article11640697.ece

Reiji, Y. (2014, December 14). Low voter turnout mars Abe's claim of election triumph. The Japan Times. Retrieved from https://www.japantimes.co.jp/news/2014/12/17/national/politics-diplomacy/low-voter-turnout-mars-abes-claim-election-triumph/

Reporters Without Borders. (2016, June). Facing Reality After the Euromaidan: The Situation of Journalists and Media in Ukraine. Retrieved February 25, 2018, from https://rsf.org/sites/default/files/journalists_and_media_in_ukraine_-_rsf_2016.pdf

Rogers, S. (2013, February 25). Italian election results: an interactive guide. *The Guardian*. Retrieved from https://www.theguardian.com/news/datablog/interactive/2013/feb/25/italian-elections-results-interactive-guide

Rosenstein, R. (2017, May 17). Rod Rosenstein's Letter Appointing Mueller Special Counsel. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2017/05/17/us/politics/document-Robert-Mueller-Special-Counsel-Russia.html

Rupawat, P. (2017, December 9). BJP's Social Media Strategy in Gujarat: A Flood of Fake News. Retrieved February 9, 2018, from http://newsclick.in/bjps-social-media-strategy-gujarat-flood-fake-news

Russia has often tried to influence elections, with little success. (2016, December 17). *The Economist.* Retrieved from https://www.economist.com/news/united-states/21711908-interference-behalf-donald-trump-probably-didnt-change-result-russian

Russian "hackers" help keep banned Catalan referendum census site online. (2017, September 28). *El Pais*. Retrieved from https://elpais.com/elpais/2017/09/28/inenglish/1506588970_026442.html

Rutenberg, J. (2017, January 8). In Election Hacking, Julian Assange's Years-Old Vision Becomes Reality. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/08/business/media/assange-wikileaks-dnc-hacks.html

Said-Moorhouse, L. (2017, September 28). Catalan referendum, explained: What's behind the push to break from Spain? *CNN*. Retrieved from https://www.cnn.com/2017/09/27/europe/catalan-referendum-explained/index.html
Said-Moorhouse, L., & van Heerden, D. (2017, August 3). Kenyan election official was strangled, authorities confirm. *CNN.* Retrieved February 9, 2018, from https://www.cnn.com/2017/08/03/africa/kenya-election-official-chris-msando/index.html
Sall, O. (2012, June 5). *The Impact of Social and Digital Medias on Senegalese Society.* Redfame Publishing. Retrieved from https://www.redfame.com/journal/index.php/smc/article/view/2422.
Sandoval, G. (2017, December 20). How Spain is waging Internet war on Catalan separatists. *The Paralla.* Retrieved from https://www.the-parallax.com/2017/12/20/spain-internet-war-catalonia/
Satter, R. (n.d.). Inside story: How Russians hacked the Democrats' emails. Retrieved January 22, 2018, from https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a
Sauti za Wananchi. (2017). *Constitution, Devolution and Inclusion : Citizens' Views on Governance in Kenya* (Brief) (p. 14). Nairobi: Twaweza East Africa. Retrieved from http://www.twaweza.org/uploads/files/SzW-Kenya-Governance-EN-FINAL.pdf
Savanevsky, M. (2015, May 13). Mr. Zuckenberg, Please Don't Let Facebook turn into KGBook. *Watcher*. Retrieved February 25, 2018 from http://watcher.com.ua/2015/05/13/mr-zukerberg-please-don-t-let-facebook-turn-into-kgbook/
Sayuri, U. (2015, June 24). Japan: Voting Age Lowered from 20 to 18. Library of Congress. Retrieved from https://www.loc.gov/law/foreign-news/article/japan-voting-age-lowered-from-20-to-18/
Schäfer, F, Evert, S, & Heinrich, P. (2017). Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe's Hidden Nationalist Agenda. Big Data, 5(4), 294–309. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5733662/
Schmidt, K. (2016, December 19). A Historic Number of Electors Defected, and Most Were Supposed to Vote for Clinton. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2016/12/19/us/elections/electoral-college-results.html
School enrollment, primary and secondary (gross), gender parity index (GPI) | Data. (n.d.). [International Organization]. Retrieved January 22, 2018, from https://data.worldbank.org/indicator/SE.ENR.PRSC.FM.ZS?locations=US
School enrollment, tertiary (gross), gender parity index (GPI) | Data. (n.d.). [International Organization]. Retrieved January 22, 2018, from https://data.worldbank.org/indicator/SE.ENR.TERT.FM.ZS?end=2015&locations=US&start=1971&view=chart
Secure Internet servers (per 1 million people) | Data. (n.d.). Retrieved January 22, 2018, from https://data.worldbank.org/indicator/IT.NET.SECR.P6?locations=US
Senegal: Country Profile. (2018). World Bank. Retrieved February 28, 2018, from http://databank.worldbank.org/data/Views/Reports/ReportWidgetCustom.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=SEN
Senegal. (2018, January 16). Freedom House. Retrieved February 28, 2018, from https://freedomhouse.org/report/freedom-world/2018/senegal

Sengupta, K. (2017, December 21). Catalonia election: Surveys suggest pro-independence parties have narrow advantage as region votes in crucial poll. *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/catalonia-election-vote-today-polls-independence-spain-barcelona-a8123211.html

Serhan, Y. (2018, February 24). Italy Scrambles to Fight Misinformation Ahead of Its Elections. *The Atlantic.* Retrieved February 28, 2018, from https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/

Sevenzo, F. (2017, August 1). Kenya election: Fake CNN, BBC reports target voters. *CNN*. Retrieved January 26, 2018, from https://www.cnn.com/2017/07/31/africa/kenya-election-fake-news/index.html

Shane, S. (2017a, September 7). The Fake Americans Russia Created to Influence the Election. *The New York Times*. Retrieved from https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

Shane, S. (2017b, November 1). These Are the Ads Russia Bought on Facebook in 2016. *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2017). The spread of misinformation by social bots. Indiana University Bloomington. Retrieved from http://arxiv.org/abs/1707.07592

Sheth, S. (2017, September 27). Russia's disinformation campaign on Facebook could have been more widespread than we knew. Business Insider. Retrieved February 25, 2018 from http://www.businessinsider.com/russia-trolls-facebook-ukraine-activists-disinformation-2017-9

Siddle, J. (2010, May 18). Indian voting machines "hacked." *BBC*. Retrieved from http://www.bbc.com/news/10123478

Sieff, K. (2017, September 20). Kenya's Supreme Court: Here's why we annulled the results of the presidential election. It was a mess. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/kenyas-supreme-court-heres-why-we-annulled-the-results-of-the-presidential-election-it-was-a-mess/2017/09/20/c22066cf-7fcf-4bc8-8655-33657c584afa_story.html

Silva, R. (2013, January). Hacker de 19 anos diz que fraudou eleições municipais. Tecnoblog. Retrieved from: https://tecnoblog.net/120215/hacker-19-anos-fraude-eleitoral/

Silverman, C. (2016, November 16). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. Retrieved January 26, 2018, from https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

Similar Web. (2018, January 1). Top Websites - SimilarWeb Website Ranking. Retrieved February 9, 2018, from https://www.similarweb.com/top-websites

Smith, L. (2017, September 28). Catalan independence websites blocked by Spanish government in bid to stop referendum. BBC. Retrieved from http://www.independent.co.uk/news/world/europe/catalan-independence-referendum-spain-websites-blocked-spanish-constitution-votes-a7971751.html

Sofia News Agency. (2017, March 3). Bulgaria Marks 139th Anniversary of Liberation from Ottoman Rule. *Noinvite.com*. Retrieved February 8, 2018, from http://www.novinite.com/articles/179101/Bulgaria+Marks+139th+Anniversary+of+Liberation+from+Ottoman+Rule

Soldatov, A. and Borogan, I. (2013, September 12). Russia's Surveillance State. Retrieved February 28, 2018, from http://255.576.mwp.accessdomain.com/2013/09/12/russias-surveillance-state/

South East Europe Media Organization. (2016). Curbing Media, Crippling Debate Soft Censorship in Bulgaria. *World Association of Newspapers and News Publishers*. Retrieved from http://www.wan-ifra.org/sites/default/files/field_article_file/SC%20Bulgaria%20final%202016%20%282%29.pdf

Srecko, G. (2014, June 18). The Protection of media freedom in Europe. *Council of Europe*. Retrieved from http://www.cfom.org.uk/wp-content/uploads/2014/07/PACE-HORSLEY-FINAL-2014-REPORT-AAC-25_14-Flego-protection-of-media-freedom-18-June.pdf

Star Team. (2017, November 14). The millions Raila paid US consultants for election. Retrieved February 17, 2018, from http://www.the-star.co.ke/news/2017/11/14/the-millions-raila-paid-us-consultants-for-election_c1669124

Starbird, K. (2017, March 15). Information Wars: A Window into the Alternative Media Ecosystem. Retrieved February 20, 2018, from https://medium.com/hci-design-at-uw/information-wars-a-window-into-the-alternative-media-ecosystem-a1347f32fd8f

Statista. (2015). Bulgaria: number of smartphone users 2015-2022 | Forecast. Retrieved February 8, 2018, from https://www.statista.com/statistics/566061/predicted-number-of-smartphone-users-in-bulgaria/

Statista. (2016). Household internet access in Bulgaria 2007-2016 | Statistic. Retrieved January 24, 2018, from https://www.statista.com/statistics/377643/household-internet-access-in-bulgaria/

Statista. (2017, January). Active social media penetration in European countries 2017 | Statistic. Retrieved January 24, 2018, from https://www.statista.com/statistics/295660/active-social-media-penetration-in-european-countries/

Statista. (2017a, June). Bulgaria: Facebook users by age 2017 | Statistic. Retrieved February 18, 2018, from https://www.statista.com/statistics/805460/facebook-users-bulgaria/

Statista. (2017b, June). Bulgaria: Instagram users by age 2017 | Statistic. Retrieved February 18, 2018, from https://www.statista.com/statistics/805455/instagram-users-bulgaria/

Statistica. (n.d.). Topic: Internet usage in India. Retrieved February 23, 2018, from https://www.statista.com/topics/2157/internet-usage-in-india/

Stent, Angela R., The Limits of Partnership: US-Russia Relations in the 21st Century, Princeton University Press, 2014

Stern, D. (2015, April 08). Ukraine crisis: Tension over rise of nationalist Yarosh. BBC. Retrieved February 26, 2018, from http://www.bbc.com/news/world-europe-32216738

Subramanian, S. (2014, May 16). The Stunning Result in India's Elections. *The New Yorker*. Retrieved from https://www.newyorker.com/news/news-desk/the-stunning-result-in-indias-elections.

Subranian, S. (2017, February 15). Meet the Macedonian Teens Who Mastered Fake News and Corrupted the US Election. *Wired.* Retrieved January 26, 2018, from https://www.wired.com/2017/02/veles-macedonia-fake-news/

Superior Electoral Tribunal of Brazil. (n.d.). Estatísticas eleitorais 2014. Retrieved from http://www.tse.jus.br/eleitor-e-eleicoes/estatisticas/eleicoes/eleicoes-anteriores/estatisticas-candidaturas-2014/estatisticas-eleitorais-2014-resultados

Syeed, N. (2017, November 29). Vote-Hacking Fears Help State Officials Get Security Clearances . Bloomberg. Retrieved February 9, 2018, from https://www.bloomberg.com/news/articles/2017-11-29/vote-hacking-fears-help-state-officials-get-security-clearances

Talyor, A. (2017, January 4). Italian populist leader suggests juries of random people should decide what's 'fake news'. *The Washington Post*. Retrieved February 18, 2018, from https://www.washingtonpost.com/news/worldviews/wp/2017/01/04/italian-populist-leader-suggests-juries-of-random-people-should-decide-whats-fake-news/?utm_term=.a3c49722a56b

Tanaka, H. (2017) "Fake News Complete Failure." Abe Pushing for Media Decay. iRONNA
田中秀臣. (2017). 「フェイクニュースの惨敗」メディアの腐敗が後押しした安倍一強. iRONNA. Retrieved from http://ironna.jp/article/8000?p=2

Tanev, M. (2017, June 28). Nearly 25% of Bulgarians encounter fake news on daily basis - poll. *SeeNews*. Retrieved February 17, 2018, from https://seenews.com/news/nearly-25-of-bulgarians-encounter-fake-news-on-daily-basis-poll-573769

Teruya, H. (n.d.) Legislative Elections underneath the US Armed Forces Rule. The Problem of American Government Election Interference and Trial Transfer. 米軍統治下における立法院議員選挙 : 米民政府の選挙干渉と裁判移送問題. Okinawa International University.

Tharoor, I. (2015, April 2). The key moments in the long history of U.S.-Iran tensions. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2015/03/31/the-key-moments-in-the-long-history-of-u-s-iran-tensions/

Tharoor, I. (2016, October 13). Analysis | The long history of the U.S. interfering with elections elsewhere. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2016/10/13/the-long-history-of-the-u-s-interfering-with-elections-elsewhere/

The Constitution of Japan. (n.d.). [.go.jp]. The Prime Minister of Japan and His Cabinet Retrieved from http://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

The Sofia Globe Staff. (2016, April 14). Bulgaria unveils proposals to boost cybersecurity. Retrieved February 18, 2018, from https://sofiaglobe.com/2016/04/14/bulgaria-unveils-proposals-to-boost-cybersecurity/

The World Factbook Ukraine. (2018, January 17). Central Intelligence Agency. Retrieved February 25, 2018 https://www.cia.gov/library/publications/the-world-factbook/geos/up.html

Thorsen, E., & Sreedharan, C. (2015) India Elections 2014: First Reflections. Great Britian: Centre for the Study of Journalism, Culture & Community Bournemouth University. https://www.dropbox.com/s/fq8qpe0xf7ajqzq/2015-India_Election_2014-Thorsen_and_Sreedharan_v1.pdf?dl=0#pageContainer165.

Tomohiro Osaki, Reiji Yoshida. 2016. "DPJ Endorses Merger with Ishin No To; New Party to Form next Month." The Japan Times. Retrieved from https://www.japantimes.co.jp/news/2016/02/24/national/politics-diplomacy/dpj-endorses-merger-ishin-no-new-party-form-next-month/#.Vs2vTf3MdFw.

Top Sites Ranking for All Categories. (n.d.) SimilarWeb. Retrieved from https://www.similarweb.com/top-websites.
Toshkov, Veselin (2017, March 26). Center-right party tops Bulgaria election; Socialists yield – *The Denver Post*. Retrieved February 8, 2018, from https://www.denverpost.com/2017/03/26/bulgaria-election/
Trading Economics. (n.d.). Senegal - Access to Electricity (% of Population). Retrieved from https://www.tradingeconomics.com/senegal/access-to-electricity-percent-of-population-wb-data.html.
Trans-Saharan Elections Project. (n.d.). The University of Florida. Retrieved from https://www.tsep.africa.ufl.edu/the-ballot/senegal/.
Translate Media. (2018). Brazil Social Media. Retrieved from https://www.translatemedia.com/translation-services/social-media/brazil-social-media
Transparency International - United States of America. (2016). [Non-Profit]. Retrieved January 22, 2018, from https://www.transparency.org/country/USA
Transparency International-Japan. (n.d.). Transparency International. Retrieved from https://www.transparency.org/country/JPN#chapterInfo
Traynor, I. (2013, April 24). Crisis for Europe as trust hits record low. The Guardian. Retrieved February 17, 2018, from https://www.theguardian.com/world/2013/apr/24/trust-eu-falls-record-low
U.S. official: Hackers targeted voter registration systems of 20 states. (n.d.). Chicago Tribune. Retrieved February 8, 2018, from http://www.chicagotribune.com/news/nationworld/ct-hackers-target-election-systems-20160930-story.html
Ukraine elections: Runners and risks. (2014, May 25). *BBC*. Retrieved February 25, 2018 from http://www.bbc.com/news/world-europe-27518989
Ukraine protests after Yanukovych EU deal rejection. (2013, November 30). *BBC*. Retrieved February 25, 2018 from http://www.bbc.com/news/world-europe-25162563
Ukraine protests after Yanukovych EU deal rejection. (2013, November 30). *BBC*. Retrieved February 25, 2018 from http://www.bbc.com/news/world-europe-25162563
UN Charter art. 2.
UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: http://www.refworld.org/docid/3ae6b3aa0.html [accessed 25 February 2018]
Underhill, W. (2018, January 5). Voter Identification Requirements | Voter ID Laws. Retrieved February 8, 2018, from http://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx
Unian. (2014, May 26). Сервер Центрвиборчкому піддається активним хакерським атакам. Retrieved February 25, 2018 from https://www.unian.ua/politics/921929-server-tsentrviborchkomu-piddaetsya-aktivnim-hakerskim-atakam.html
United Kingdom Country Profile. (n.d.). Retrieved February 28, 2018, from http://databank.worldbank.org/data/Views/Reports/ReportWidgetCustom.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=GBR
Unknown. (n.d.). The CIA and the Marshall Plan — Central Intelligence Agency. Retrieved January 25, 2018, from https://www.cia.gov/news-information/featured-story-archive/2011-featured-story-archive/the-cia-and-the-marshall-plan.html
Uyehara E., G. (1910). The Political Development of Japan, 1867-1909. London : Constable. Retrieved from www.law.nihon-u.ac.jp/publication/pdf/seikei/53_2/10.pdf

Vallance, C. (2017, Nov. 23) Russian Fancy Bear Hackers' UK Link Revealed. BBC. Retrieved from www.bbc.com/news/technology-42056555.
Van De Velde, J. (2017). The Law of Cyber Interference in Elections. SSRN Electronic Journal, SSRN Electronic Journal, 2017.
Varol, O., Ferrara, E., Davis, C. A., Menczer, F., & Flammini, A. (2017). Online Human-Bot Interactions: Detection, Estimation, and Characterization. ArXiv:1703.03107 [Cs]. Retrieved from http://arxiv.org/abs/1703.03107
Velayanikal, M. (2016, September 6). The Latest Numbers on Web, Mobile, and Social Media. Tech in Asia. Retrieved from https://www.techinasia.com/india-web-mobile-data-series-2016.
Vicens, A. (n.d.). Two State Elections Databases Have Been Hacked. The Russians Aren't the Only Suspects. Mother Jones. Retrieved February 9, 2018, from https://www.motherjones.com/politics/2016/10/state-election-hacks-undermine-voters-confidence/
Vinocur, J., & Times, S. to the N. Y. (1983, July 26). K.G.B. Officers Try to Infiltrate Antiwar Groups. *The New York Times*. Retrieved from http://www.nytimes.com/1983/07/26/world/kgb-officers-try-to-infiltrate-antiwar-groups.html
Volchek, D. (2015, June 17). Facebook's block policy accused of facilitating pro-Kremlin trolls. *The Guardian.* Retrieved February 26, 2018, from https://www.theguardian.com/world/2015/jun/17/facebook-pro-kremlin-attacks-russia
Voter turnout at Rada election 52.42% at all 198 constituencies - CEC. (n.d.). Interfax Ukraine. Retrieved February 26, 2018, from http://en.interfax.com.ua/news/general/231065.html
Voter Turnout at UK General Elections 1945 – 2017. (n.d). UK Political Info. Retrieved from www.ukpolitical.info/Turnout45.htm.
VVPAT slips match EVM data at 182 booths: EC. (2017, December 20). The Indian Express. Retrieved February 9, 2018, from http://indianexpress.com/elections/gujarat-assembly-elections-2017/vvpat-slips-match-evm-data-at-182-booths-ec-4990699/
Vyawahare, M. (2014, April 25). Election Watchdog Fights Lonely Battle on Paid News Coverage. *The New York Times*. Retrieved February 23, 2018, from //india.blogs.nytimes.com/2014/04/25/election-watchdog-fights-lonely-battle-on-paid-news-coverage/
Waki, P., McFadyen, G., & Pascal, K. (2008). *International Commission of Inquiry on Post-Election Violence* (p. 529). Retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/15A00F569813F4D549257607001F459D-Full_Report.pdf
Walcott, J., & Strobel, W. (2016, October 13). Russia has "playbook" for covert influence in
Wangari, F. (2016, September 9). Top ten most popular apps in Kenya. *Daily Nation*. Retrieved February 25, 2018, from https://www.nation.co.ke/lifestyle/saturday/Top-ten-most-popular-apps-in-Kenya-/1216-3375194-9guewkz/index.html
Warner, M. (1998). The CIA's Office of Policy Coordination: From NSC 10/2 to NSC 68. International Journal of Intelligence and Counterintelligence, 11, 211-220.
Warren, S. (2016, October 13). Russia has a new playbookfor cover influence in Eastern Europe. *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-security-usa/russia-has-playbook-for-covert-influence-in-eastern-europe-study-idUSKCN12D13Q

Waterman, S. (2016, November 08). Research: Russia seeks to discredit, not hack election results. Retrieved February 26, 2018, from https://www.cyberscoop.com/russia-hacking-2016-election-flashpoint/

Weisbrot, M. (2018, January 23). Brazil's Democracy Pushed Into the Abyss. *The New York Times*. Retrieved from https://www.nytimes.com/2018/01/23/opinion/brazil-lula-democracy-corruption.html

Weiss, A. S. (2017, February 17). Vladimir Putin's Political Meddling Revives Old KGB Tactics. Retrieved January 25, 2018, from http://carnegieendowment.org/2017/02/17/vladimir-putin-s-political-meddling-revives-old-kgb-tactics-pub-68043

Who Is Eligible to Vote at a UK General Election? (n.d.). The Electoral Commissions. Retrieved from www.electoralcommission.org.uk/faq/voting-and-registration/who-is-eligible-to-vote-at-a-uk-general-election.

Wiggins, B. (2014, September 22). How the Russia-Ukraine crisis became a magnet for memes. The Conversation. Retrieved February 25, 2018 from http://theconversation.com/how-the-russia-ukraine-crisis-became-a-magnet-for-memes-31199

World Bank, Urban population (percent of total). (n.d.). World Bank. Retrieved from https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS

World Heritage Encyclopedia. (n.d.). Italian General Election 2013. Retrieved from National Public Library Website:http://nationalpubliclibrary.com/articles/eng/Italian_general_election,_2013

Wroclavsky, D. (2015, August 20). Brazil speaker, former president charged in Petrobras corruption. Retrieved from https://www.yahoo.com/news/former-brazil-president-collor-charged-petrobras-corruption-205108912.html

Yaffa, J. (2016, September 5). Reforming Ukraine after the revolutions. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2016/09/05/reforming-ukraine-after-maidan

Yamamoto, M, Lee Tien-Tsung, and Ran, W. "Media Trust in a Community Context A Multilevel Analysis of Individual- and Prefecture-Level Sources of Media Trust in Japan." (December 30, 2014) http://journals.sagepub.com/doi/abs/10.1177/0093650214565894#articleCitationDownloadContainer.

Yarovaya, M. (2013, February 12). Госстат считает, что в Украине 5 млн интернет-пользователей. Retrieved February 25, 2018 from https://ain.ua/2013/02/12/gosstat-schitaet-chto-v-ukraine-5-mln-internet-polzovatelej

Yu, H. (2016). 블록체인 방식의 전자투표 시스템 구현 및 성능 개선 방안 연구 [A Study on Performance Improvement and Implementation of Electronic Voting System using Blockchain]. Ajou University.

Zetter, K. (2010, August 23). Researcher Arrested in India After Disclosing Problems With Voting Machines. *Wired*. Retrieved February 23, 2018, from https://www.wired.com/2010/08/researcher-arrested-in-india/

Про Все. (2014, Травень 25). На систему "Вибори" ЦВК була здійснена хакерська атака. Retrieved February 25, 2018 from http://provce.ck.ua/na-systemu-vybory-tsvk-bula-zdijsnena-hakerska-ataka/

아무리 해명에도 “내것도 가짜 투표 용지”… 왜? (2017). Korean Herald Business.Retrieved from http://heraldk.com/2017/05/10/아무리-해명에도-내것도-가짜-투표-용지/

중앙선거관리위원회 [National Election Commission]. (2013).

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON