CREATIVE

INTEGRATED DIGITAL STANDARDS FRAMEWORK FOR ELECTIONS

AUTHORED BY:

Emily Marks
B.A. candidate, University of Maryland

Advised by Jeffrey Fischer
Senior Electoral Advisor, Electoral Education & Integrity

Creative Associates International

© Copyright 2018, Creative Associates International, Washington, DC. All Rights Reserved. No part of this document may be reproduced in any form or fashion without written consent from Creative Associates International.

ABSTRACT:

This paper offers a model legislative and regulatory framework addressing digital disruption of elections that can be implemented within international electoral standards. It examines different forms of digital disinformation, gaps in current electoral standards regarding disinformation, and existing legislative efforts and deterrence initiatives being implemented by national governments and private stakeholders.

TABLE OF CONTENTS

Introduction

Along with the rise of social media in the digital age, disinformation campaigns have become a significant threat to electoral integrity and there is a growing need to address online disinformation without undermining the benefits of digital media and jeopardizing free speech and freedom of expression. The creation of an international legislative and regulatory framework addressing disinformation surrounding democratic elections and the development of commensurate electoral standards will be critical to reducing electoral disruption, maintaining public confidence in the electoral process and the media, encouraging an informed public debate, and promoting electoral integrity.

The goal of this project is to create a model legislative and regulatory framework addressing digital disruption of elections that can be implemented within international electoral standards. This will be achieved by examining how disinformation disrupts elections, highlighting gaps within current electoral standards, analyzing legislative and regulatory efforts implemented by national governments, and evaluating disinformation deterrence initiatives executed by social media companies, search engines, advertising networks, and independent fact checking organizations. These analyses will inform the development of a legislative and regulatory framework that can be used as a model for combatting digital disinformation surrounding democratic elections.

1. Background on disinformation surrounding elections

Definitions

Along with the rise of digital disinformation, a new lexicon of terms has emerged to classify factual distortion and manipulation on the internet. It is important to distinguish between these terms before exploring the impact of disinformation on elections around the world. The National

Endowment for Democracy has recently developed several definitions that help differentiate between the terms that are widely used to characterize manipulation on the web. *Misinformation* refers to the inadvertent sharing of false information. Misinformation is always unintentional; however, it still poses an problem because it can distort public opinion even though it is not malicious in intent. *Disinformation*, on the other hand, is always purposeful and contributes to a larger plan or agenda, although it is not necessarily comprised of outright lies. Disinformation can be mostly true facts that have been taken out of context or blended with falsehoods.[1]

The most difficult term to define is *fake news*, which has also become the most popularized term for factual distortion on the web. According to the National Endowment for Democracy, fake news generally refers to intentionally misleading content found on the internet, especially on social media. They identify five types of fake news, which include intentionally deceptive content, jokes taken at face value, large-scale hoaxes, slanted reporting of real facts, and coverage where the truth may be uncertain or contentious.[2] Fake news can either be driven by political ideology or financial motivations. In the latter scenario, producers of fake news tailor false content targeted at specific viewers, generating online interactions such as clicks or sharing that create advertising revenue.[3] While fake news can manifest in many forms, the underlying commonality is the intentional distortion of facts with the purpose of misleading people and influencing public opinion, whether motivated by money or ideology.

However, the term *fake news* can be problematic because it is often misused by people who do not fully understand the true definition and implications of the term. It is also deliberately

[1] National Endowment for Democracy. “Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News.’” Published October 17, 2017. Accessed June 3, 2018.

[2] Ibid.

[3] National Endowment for Democracy. “Issue Brief.”

misused by public figures with the aim of undermining the legitimacy of the mainstream media. The phrase first emerged on a large scale during the 2016 US presidential election, but Donald Trump's campaign distorted its meaning to criticize liberal-leaning media outlets who were presenting Trump in a negative light.[4] It is important to distinguish the real definition of fake news from the appropriated definition, because fake news is not defined by liberal versus conservative leanings, but rather by intentional falsities meant to distort public opinion, create confusion, and/or make a profit. The term *disinformation* will be used for the purposes of this paper in order to avoid any misconceptions.

Explanatory factors for the rise of disinformation

Digital disinformation has become a growing threat to democratic elections throughout the past decade. According to Freedom House's 2017 Freedom on the Net Report, digital disinformation has contributed to a decline in internet freedom worldwide for the seventh consecutive year.[5] There are several explanatory factors contributing to the steady increase of disinformation on the web. First, the widespread use of social media has democratized the exchange of information and has created a participatory platform for sharing news, opinions, and ideas. The dissemination of information is no longer restricted to established news outlets; now anyone who has internet access can produce and spread anything they want over the internet, which can be difficult to distinguish from high-quality information.[6]

Second, the centralization of distribution channels via social networks makes it feasible to reach an enormous audience in a short period of time. Platforms such as Facebook and Twitter

[4] Niklewicz, Konrad. "Weeding Out Fake News: An Approach to Social Media Regulation." Wilfried Martens Centre for European Studies. Published 2017. Accessed June 14, 2018. Page 16.

[5] Freedom House. "Freedom On The Net 2017: Manipulating Social Media to Undermine Society." Published November 2017. Accessed June 20, 2018.

[6] Information Society Project. "Fighting Fake News: Workshop Report." Yale Law School. Published March 7, 2017. Accessed July 2, 2018. Page 3.

have billions of active users, meaning that there is a low barrier to entry and it is easy to spread false information quickly.[7]

Third, the rise of social media has created a business model that values attention-grabbing material over high-quality news. Although people claim to desire credible news that has been edited and fact checked, this type of journalism is not valued in the internet marketplace. This idea is highlighted in a Data&Society publication entitled "Media Manipulation and Disinformation Online." "Social media—and largely, the internet as a whole—is an attention economy where the most valued content is that which is most likely to attract attention. The overload of information enabled by the internet makes attention an extremely valuable resource. Viral content, from funny videos to sensational headlines, garners the clicks, retweets, and likes, and thus advertising revenue."[8] Furthermore, the speed at which information is posted and spread is faster than ever, therefore it is often not worthwhile to carefully fact check an article if it means that it will take too long to publish.

Fourth, advertising companies have monetized the internet and created a market that encourages disinformation and clickbait. When users click or comment on pieces of media, the producers make money from advertising revenue. There is an incentive to create sensationalist articles that will drive a lot of traffic to a website in order to turn a profit.[9]

Fifth, the "filter bubble" phenomenon makes it even easier for false information to quickly spread within certain networks of people. According to the Wilfried Martens Centre for European Studies, the filter bubble is the idea that "groups of social media users consume - whether

[7] Freedom House. "Freedom on the Net 2017."

[8] Marwick, Alice and Lewis, Rebecca. "Media Manipulation and Disinformation Online." Data&Society. Published May 15, 2017. Accessed July 3, 2018. Page 42.

[9] Hwang, Tim. "Digital Disinformation: A Primer." Atlantic Council. Published September 2017. Accessed July 13, 2018. Page 4.

consciously or not - the same content and are basically not offered alternative information or opinions".[10] Filter bubbles are unintentionally created because people tend to follow others with similar views on social media, while blocking people who they do not agree with. These types of environments are easy to exploit because disinformation spreads quickly through close-knit networks of like-minded individuals.

Consequences of digital disinformation

Digital disinformation has numerous consequences that negatively impact the integrity of the electoral process. Primarily, widespread disinformation causes confusion and distrust in the media and political institutions.[11] When there are contradictory articles, unverified content, and sensational stories on the internet, it becomes difficult for people to determine what is fact and what is fiction. In this way disinformation devalues legitimate news sources and voices of expertise, because high-quality content becomes mixed in with non-credible sources. This is an especially harmful consequence during election cycles, because the media agenda powerfully impacts public opinion concerning candidates and political platforms. If a media manipulator successfully provokes the mainstream media into covering their story, it will impact the public agenda even if the media is simply trying to debunk the story.[12] Overall, digital disinformation during elections undermines rational public discourse that is rooted in verifiable facts and informed opinions.[13]

Prominence of disinformation during elections

[10] Niklewicz. "Weeding Out Fake News." Page 17.

[11] Weedon, Jen, Nuland, William, and Stamos, Alex. "Information Operations and Facebook." Facebook. Published April 27, 2017. Accessed June 27, 2018. Page 4.

[12] Marwick and Lewis. "Media Manipulation and Disinformation Online." Page 39.

[13] Information Society Project. "Fighting Fake News." Page 3.

Disinformation tactics played a role in elections in the following 23 countries since January 2016:

Table 1. Elections that were affected by disinformation since 2016

North America	United States, Mexico
South America	Ecuador, Venezuela, Colombia
Europe	Czech Republic, Germany, Russia, United Kingdom, France, Italy, Netherlands, Spain
South/East Asia	Philippines, Indonesia, South Korea
West/Central Asia	Turkey, Armenia
Africa	Angola, Gambia, Kenya, Rwanda, Zambia

[14][15][16]

This demonstrates that factual distortion poses a threat to electoral processes worldwide. A selection of these elections will be explored in further detail in a following section, however, there are several key characteristics that each of these examples share in common. When individuals and/or organizations intentionally manipulate the media during the election cycle, there are several core goals that they are trying to achieve. First, media manipulators often aim to simulate grassroots support for candidates (also known as “astroturfing”) by creating the illusion that their chosen candidate is more popular than they actually are in reality. Second, they try to spread false information about political opponents to make them seem incapable or unpopular. Third, media manipulators aim to stir up controversy and animosity amongst voters.[17] False,

[14] Freedom House. “Freedom on the Net 2017.”

[15] Niklewicz. “Weeding Out Fake News.” Page 23.

[16] Brattberg, Eric and Maurer, Tim. “Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks.” Carnegie Endowment for International Peace. Published May 23, 2018. Accessed July 14, 2018.

[17] Freedom House. “Freedom on the Net 2017.”

sensational stories about controversial issues contributes to the polarization of constituents during the election cycle, because people are naturally drawn to over-the-top stories and “hot-button” issues over run-of-the-mill political news and policy platforms since those are often dull and highly technical. Consequently, in this digital campaign environment driven by shared posts on Facebook and trending hashtags on Twitter, elections become focused on exaggerated, surface-level topics rather than concrete political agendas and verifiable facts.

Perpetrators

There are numerous types of perpetrators that contribute to media manipulation with the aim of disrupting the electoral process. The first type of perpetrators are state-affiliated cyber troops. State-affiliated cyber troops are teams sponsored or controlled by the government or military committed to manipulating public opinion over social media, blogs, and message boards targeted at niche populations.[18] According to the Computational Propaganda Project at Oxford University, “cyber troops have an overarching communications strategy that involves creating official government applications, websites, or platforms for disseminating content; using accounts—either real, fake, or automated—to interact with users on social media; or creating substantive content such as images, videos or blog posts”.[19]

Cyber troops have grown dramatically in scale and quantity over the past decade. As of 2017, Oxford has identified state-affiliated cyber troops in the following 28 countries:

Table 2. Countries using state-affiliated cyber troops as of 2017

North America	United States, Mexico
South America	Argentina, Brazil, Ecuador, Venezuela

[18] Bradshaw, Samantha and Howard, Philip N. “Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.” University of Oxford Computational Propaganda Research Project. Published December 2017. Accessed June 12, 2018. Page 9.

[19] Ibid. Page 9.

Europe	Czech Republic, Germany, Poland, Russia, Serbia, the United Kingdom, Ukraine
South/East Asia	China, North Korea, Philippines, Vietnam, Taiwan, South Korea, India
West/Central Asia	Azerbaijan, Iran, Turkey
Middle East	Bahrain, Saudi Arabia, Syria, Israel
Oceania	Australia

[20]

The second type of perpetrators that contribute to disinformation during elections is political parties and politicians. Political parties have been manipulating public opinion during campaigns for hundreds of years by either attacking their opponents or glorifying their own successes. However, in the digital age this type of manipulative campaigning has taken on a new and more insidious form. Political parties will purposely target their opponent's support bases by spreading disinformation about their candidates. Certain political parties have also utilized fake accounts to inflate the number of likes, followers, shares, or retweets a candidate receives. This creates an artificial sense of popularity and credibility for that candidate.[21]

A third category of disinformation perpetrators are citizen groups. Citizen groups are independent networks of people working together to manipulate public opinion. These groups actively collaborate to spread political messages and create false content on the internet. They can either be ideologically motivated or seeking compensation from advertisement revenues.[22]

[20] Ibid. Page 4.

[21] Ibid. Page 15.

[22] Ibid. Page 16.

The fourth category of perpetrators are internet trolls. Internet trolls are anonymous citizens on the internet who deliberately bait others with the objective of achieving an emotional response. Trolls are often not motivated by a specific ideology, rather they are interested in offending people with shocking material in order to disrupt electoral proceedings and cause confusion.[23] Internet trolls often work together in digital campaigns that are coordinated through informal, anonymous groups of users. Some of their techniques include fabricating documents and pictures and attempting to directly engage and mislead other users on the internet.[24]

The fifth and final category of perpetrators is hyperpartisan media. Hyperpartisan media platforms are either extremely far to the right or to the left of the political spectrum, and they are known for "combining decontextualized truths, repeated falsehoods, and leaps of logic to create a fundamentally misleading view of the world".[25] These outlets frequently spread rumors, conspiracy theories, sensational stories, and attack the mainstream media. Breitbart News is an example of a right-wing hyperpartisan media outlet, and Occupy Democrats is an example of a left-wing hyperpartisan group.

Tactics

Disinformation perpetrators utilize a wide range of tactics to conduct their manipulation campaigns. The first tactic is false amplification, which refers to "coordinated activity by inauthentic accounts with the intent of manipulating political discussion".[26] These inauthentic accounts are knowns as "bots," which are pieces of code that mimic real accounts on social media and interact with online content and other users in a realistic manner. Bots are used for false

[23] Marwick and Lewis. "Media Manipulation and Disinformation Online." Page 4.

[24] Hwang. "Digital Disinformation: A Primer." Page 6.

[25] Tucker, Joshua A. et al. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." Hewlett Foundation. Published March 2018. Accessed June 28, 2018. Page 26.

[26] Weedon, Nuland, and Stamos. "Information Operations and Facebook." Page 5.

amplification tactics because they can amplify marginal voices and ideas by inflating the number of interactions on a piece of media, creating an artificial sense of popularity.[27] For example, they can make an unpopular candidate, a false article, or an obscure idea seem extremely relevant during an election by augmenting the amount of online interactions surrounding that content.

The second prevalent disinformation tactic is the creation of false content. This can include writing completely fake stories and publishing them in a fake news outlet that is made to look like a real news outlet. It can also involve using a piece of true information and twisting it, removing if from context, and surrounding it by artificial details.[28] Finally, content creation also encompasses doctoring and manipulating images and videos.

The third tactic is targeted data collection, which Facebook defines as "stealing, and often exposing, non-public information that can provide unique opportunities for controlling public discourse".[29] This includes hijacking social media accounts, gathering information on users, cyber operations against organizations or individuals, and data theft.[30]

The fourth disinformation tactic is selective censorship, which involves removing certain pieces of content from internet platforms, while allowing other pieces to remain. This effectively takes facts out of context and creates a false and misinformed narrative for any user who comes across the content.[31]

The fifth tactic is manipulating search algorithms in order to make certain stories or pieces of disinformation more likely to appear in a search. According to a publication by the Martens Centre for European Studies, this can be achieved with the following methods: "keyword stuffing

[27] Bradshaw and Howard. "Troops, Trolls, and Troublemakers." Page 11.
[28] Niklewicz. "Weeding Out Fake News." Page 15.
[29] Weedon, Nuland, and Stamos. "Information Operations and Facebook." Page 6.
[30] Ibid. Page 6.
[31] Tucker, Joshua A. et al. "Social Media, Political Polarization, and Political Disinformation." Page 30.

(adding popular keywords to promote websites in search engine rankings); link bombs (using anchor text in links to relate specific search queries); and creating mutual admiration societies (groups of websites with links pointing to each other)".[32] These tactics increase the likelihood that certain content will be viewed by a higher quantity of users.

Perpetrators of disinformation effectively use a combination of these five tactics in order to promote their ideological, political, or financial interests by manipulating democratic elections. The following subsections will highlight examples of three different elections that were influenced by coordinated disinformation perpetrators wielding these tactics to support their agenda.

Disinformation during the United States 2016 election

The United States 2016 presidential election was the catalyst for the current widespread discussion surrounding disinformation influencing electoral processes. It was an extremely high-profile election, particularly due to the controversial and unorthodox nature of the Republican candidate Donald Trump. Therefore, when it became clear that the election had been influenced by several coordinated manipulation efforts, disinformation became a topic of worldwide debate and research.

There were multiple disinformation perpetrators who attempted to influence the US 2016 election. The primary culprit was Russian cyber troops, who used numerous tactics to sway public opinion in favor of Donald Trump including false amplification, targeted data collection, and content creation. Russian sources produced false news articles to help promote their political interests, including stories about Pope Francis endorsing Donald Trump, Hillary Clinton selling weapons to ISIS, Hillary Clinton being disqualified from holding federal office, and the FBI director receiving millions from the Clinton Foundation.[33] Additionally, around 20% of the tweets

[32] Ibid. Page 30.

[33] West, Darrell M. "How to combat fake news and disinformation." Brookings Institution. Published

during the 2016 US presidential campaign were sent by Russian-generated bots, and bots made up 40% of all of Clinton and Trump's followers.[34] Finally, Russian agents gained access to the email server of Clinton's campaign chairman, John Podesta, as well as to the servers of the Democratic National Committee. The emails that were subsequently published on WikiLeaks following the Russian hacks gravely damaged the Clinton campaign.[35]

Other culprits include citizen groups and internet trolls. Collections of independent citizens seized the opportunity to profit off of the lucrative advertising revenues that were attainable during the high-profile presidential campaign. For example, a group of teenagers from Macedonia created false stories defaming Hillary Clinton because they could make a significant amount of money from advertisements placed on their sites.[36] In addition, internet trolls and far-right subculture groups made coordinated efforts to promote pro-Trump, populist messages, as well as spread false stories about Hillary such as the allegations that she was running a child sex-ring out of a pizza restaurant in Maryland.[37]

The disinformation surrounding the 2016 US presidential election had a widespread impact on the information landscape. The 20 largest false stories created by Russian cyber troops, independent citizen groups, and internet trolls generated 8.7 million shares, reactions, and comments, compared to 7.4 million interactions generated by the top 20 real news stories from major news sites. Furthermore, Facebook estimated that 126 million users saw articles and advertisements created by Russian sources, and Twitter found 2,752 accounts established by Russian groups that tweeted 1.4 million times in 2016.[38]

December 18, 2017. Accessed June 9, 2018.

[34] Niklewicz. "Weeding Out Fake News." Page 26.

[35] Harding, Luke. "What we know about Russia's interference in the US election." The Guardian. Published December 16, 2016. Accessed July 23, 2018.

[36] Niklewicz. "Weeding Out Fake News." Page 24.

[37] Marwick and Lewis. "Media Manipulation and Disinformation Online." Page 55.

[38] West. "How to combat fake news and disinformation."

Disinformation during the Philippines 2016 election

During the 2016 presidential election in the Philippines, the campaign for Rodrigo Duterte utilized a massive army of “keyboard trolls” to help secure his victory in April 2016. This keyboard army was a mixture of volunteers and payed employees hired to spread propaganda for Duterte in order to influence public opinion in his favor.[39] Their methods were referred to as “patriotic trolling,” and involved the use of targeted harassment, propaganda, and false amplification on social media. The hundreds of keyboard trolls were organized into four functional groups, three in the Philippines and one comprised of overseas Filipino workers, each tasked with distributing disinformation created by the campaign. Initially Facebook received complaints about inauthentic accounts and pages relating to the election, however the complaints eventually shifted into allegations over Duterte’s trolls circulating aggressive messages, insults, and threats of violence meant to intimidate people who did not support Duterte. As a result of his massive disinformation campaign, Duterte dominated the online political conversation thoroughly and was the subject of 64% of all Philippine election-related conversations on Facebook.[40]

Disinformation during the French 2017 election

Disinformation producers linked to Russia were reportedly very active during the French 2017 presidential election, using tactics such as targeted data collection, content creation, and false amplification to sway public opinion against Emmanuel Macron. Two Russian-backed news outlets, Sputnik France and RT France, were highly active on Twitter leading up to the election, with anti-Macron disinformation reaching more than 145,000 individuals. Assertions that Macron is an agent for U.S. financial interests and that he is secretly gay were among the false narratives

[39] Bradshaw and Howard. “Troops, Trolls, and Troublemakers.” Page 15.

[40] Etter, Lauren. “What Happens When the Government Uses Facebook as a Weapon?” Bloomberg Businessweek. Published December 7, 2017. Accessed July 16, 2018.

spread by Russian news outlets. Furthermore, a network of Russian-controlled bots helped promote these stories with impressive efficiency; a quarter of the political stories shared on Twitter in France during the election were based on Russian disinformation.[41]

Additionally, Facebook confirmed that Russian agents created twelve fake accounts posing as acquaintances of people close to Macron in an attempt to gain intelligence from campaign staffers. A Russian entity also gained access to campaign emails by posing as a fake Microsoft storage website and obtaining login data from staff members. On May 6, 2017, one day before the runoff vote between Macron and his conservative competitor Marine Le Pen, 9 gigabytes of stolen campaign files and 21,000 emails were uploaded to a platform called Pastebin. After the stolen files and emails were republished by WikiLeaks, the hashtag #MacronLeaks attached to leaked information spread rapidly across social media.[42]

2. Review of existing international electoral standards

With the growing threat of disinformation influencing democratic elections, it is critical that disinformation prevention is addressed in international electoral standards. International electoral standards constitute a values-based set of guidelines upon which election laws are constituted. These standards are meant to be applicable to any country in the world that hosts democratic elections and used to ensure fair democratic processes and equality of access for all citizens.[43] Numerous intergovernmental organizations, NGOs, and legislative bodies have contributed to the discussion of what values should be included in international electoral standards, but they are all based in similar ideologies derived from international sources such as the 1948 Universal Declaration of Human Rights.

[41] Brattberg and Maurer. "Russian Election Interference."

[42] Ibid.

[43] International IDEA. "International Electoral Standards: Guidelines for reviewing the legal framework of elections." Published 2002. Accessed July 9, 2018. Page 55.

This section will review current contributions to international electoral standards published by three credible institutions—the EU External Action Service, the Carter Center, and International IDEA—and identify gaps regarding digital disinformation influencing the integrity of elections. It is important to keep in mind that the Carter Center and International IDEA's publications were written before the age of social media. In general, these electoral standards advocate for democratic rights such as freedom of expression and freedom of the press, but they do so without reference to the damaging impact of intentional media manipulation on electoral integrity. It is crucial in the digital age that these standards are modernized to consider digital disinformation, while maintaining a delicate balance between freedom of speech and veracity of content.

Freedom of expression and communication

The existing international electoral standards published by the three institutions extensively discuss the right to freedom of expression. "Compendium of International Standards for Elections," created by the EU External Action Service, says that all citizens should have the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".[44] Similarly, "Election Obligations and Standards," written by The Carter Center, argues that "the right to free expression includes the ability for everyone to seek and receive information and ideas".[45] Finally, "Guidelines for Reviewing the Legal Framework of Elections," by International IDEA, says that "a democratic election is not possible where the legal framework for elections

[44] European Union External Action Service. "Compendium of International Standards for Elections." Published 2016. Accessed July 8, 2018. Page 69.

[45] The Carter Center. "Election Obligations and Standards: A Carter Center Assessment Manual." Published 2010. Accessed July 9, 2018. Page 71.

inhibits or dampens campaign speeches and free expression".[46] These excerpts demonstrate that freedom of expression, exchange of ideas, and equitable access to information are essential components of the existing international electoral standards. However, none of these publications consider how digital disinformation pollutes the quality and integrity of information, and therefore hinders citizens' abilities to make informed judgments.

Freedom of the press

The current international electoral standards also advocate for a free and uncensored press during elections. However, both International IDEA and The Carter Center touch on several regulatory stipulations to ensure that the media promotes a free and fair elections. International IDEA specifies that "the legal framework should ensure that all political parties and candidates have access to the media and are treated equitably by media…and that no unreasonable limitations are placed on the right of political parties and candidates to free expression during election campaigns".[47] The Carter Center argues that "reasonable limitations may be imposed on the media's right to free expression in order to ensure the fulfillment of other rights. For example, the media may be required to provide voter education and to air debates between candidates".[48] Finally, The Carter Center also advocates for the establishment of an independent regulatory body to monitor broadcasts, such as the Federal Communications Commission in the United States.[49] These excerpts demonstrate that the existing electoral standards value a free and uncensored press, but they simultaneously advocate for regulations aimed at encouraging fair coverage, informing a credible debate, and representing campaigns as accurately as possible. However, these standards

[46] International IDEA. "International Electoral Standards." Page 63.
[47] Ibid. Page 61.
[48] Carter Center. "Election Obligations and Standards." Page 138.
[49] Ibid. Page 135.

are only referring to traditional media outlets, and do not touch on influential and easily corruptible platforms such as social media.

Reasons for restricting freedom of expression and freedom of the press

The existing international electoral standards mention specific scenarios during which it is acceptable to restrict freedom of expression or freedom of the press. The EU External Action Service argues that these rights can be restricted only "for respect of the rights or reputations of others and for the protection of national security or of public order or of public health or morals".[50] The Carter Center adds that freedom of expression can be restricted if it involves incendiary hate speech, or to "prevent disclosure of information received in confidence".[51] These examples show that there are certain exceptions to freedom of expression in extenuating circumstances, but these circumstances do not extend to malevolent disinformation online.

Gaps in current electoral standards

After reviewing the existing international electoral standards, it is clear that digital disinformation surrounding elections is not incorporated into current standards. There is currently no acknowledgement of the damaging impacts of disinformation, or guidelines concerning preventative measures and mitigating recourse actions against disinformation. Again, it is important to keep in mind that "Election Obligations and Standards," by The Carter Center, and "Guidelines for Reviewing the Legal Framework of Elections," by International IDEA were published before the social media age and therefore before digital disinformation became a significant threat to electoral integrity. However, as disinformation has become an obstacle to the

[50] European Union External Action Service. "Compendium of International Standards for Elections." Page 77.

[51] Carter Center. "Election Obligations and Standards." Page 27.

credibility and veracity of elections, international electoral standards should be reconsidered to include disinformation prevention as part of their framework.

3. Examination of governmental initiatives

With the rising threat of disinformation damaging the integrity of electoral processes, many governments around the world have taken legislative or regulatory action to address disinformation within their territory. The national governments that have started anti-disinformation initiatives include: Germany, France, the United States, the Philippines, Indonesia, Ukraine, Thailand, Malaysia, Kenya, the United Kingdom, Ireland, Croatia, Brazil, Belgium, Belarus, Tanzania, Sweden, South Korea, and Italy. There are also instances of sub-states acting against disinformation, for example the state of West Bengal in India. Finally, the European Union, an intergovernmental organization, has made impressive progress towards mitigating disinformation within its member states.[52]

All of these governmental initiatives are in different stages of implementation; some governments have already passed comprehensive legislation, while others are still debating and drafting potential regulatory measures. The initiatives also vary in their methods and approaches. The different types of approaches can be broken down into the following categories: removing disinformation from the internet, passing prison sentences and large fines for disinformation producers, regulating advertisements for placement and transparency, and promoting high-quality news over untrustworthy news.

Removing disinformation from the internet

[52] Funke, Daniel. “A guide to anti-misinformation actions around the world.” Poynter. Last modified July 2, 2018. Accessed July 9, 2018.

Several governments have adopted the approach of removing disinformation from the internet, either directly or indirectly. Some countries have granted monitoring and removal power to public authorities, while others place the onus on social media platforms to monitor and remove suspicious content. For example, in June 2017 the German government passed a piece of legislation called the "Social Media Enforcement Law," which requires social media platforms to remove hate speech and disinformation within 24 hours of notification. If the social media platform does not remove the problematic post within one day, it can be subject to fines of up to 50 million euros. The legislation is deeply controversial, with many international watchdog organizations and other governments claiming that it is dangerously close to government-sanctioned censorship, and that it will incentivize social media platforms to preemptively delete any controversial content in order to avoid large fines.[53] In response to these criticisms, several revisions are being considered, including a process for getting incorrectly deleted content restored and having social media platforms set up independent bodies to review problematic posts.[54]

Whereas Germany places the burden of removing false content on social media platforms, Thailand gives that responsibility to public authorities. Thailand's Computer Crime Act was passed in 2017 and gives public authorities unprecedented power over web content, focusing on illegal content and disinformation. This legislation has extensive provisions and grants Thai authorities "comprehensive power to police and delete online content…and to detect and monitor online activities imposing requirements on all media and online companies operating in

[53] Freedom House. "Freedom on the Net 2017."
[54] Funke. "A guide to anti-misinformation actions."

Thailand".[55] This law involves far more governmental intervention than Germany's legislation, and has therefore faced massive criticism over state-imposed censorship of the internet.[56]

Passing prison sentences and fines for producers of disinformation

Other governments have moved to tackle digital disinformation at its source by targeting the producers and distributors of false content. In April 2018, Malaysia passed a law that criminalizes the creation or distribution of disinformation. The legislation makes publishing or sharing disinformation punishable by up to six years in prison and a fine of 500,000 ringgit, which is equal to $128,000. Anyone can submit a complaint about an alleged purveyor of disinformation, and Malaysian online service providers now have increased responsibility for monitoring third-party content.[57] The first person arrested under this law in late April was a Danish citizen who posted "inaccurate criticism of police on social media".[58] This is a poignant example of how lives can be negatively impacted when disinformation legislation is taken too far. There is a fine line between punishing malicious disinformation producers and unfairly criminalizing controversial online content, expression of opinion, or even honest mistakes.

Regulating advertisements

Some countries are attempting to eliminate untrustworthy online political advertisers by holding advertisements on social media platforms to the same standards as advertisements broadcasted on television and radio stations. The "Honest Ads Act" is a bill that was introduced in the United States in October 2017 that is attempting to accomplish exactly that: bring online political advertisements up to the standards that have been subscribed to radio and television

[55] Morris, James and Nguyen, Son. "Thai Government warns about fake news online as political discourse picks up before elections." Thai Examiner. Published June 21, 2018. Accessed July 17, 2018.

[56] Ibid.

[57] Funke. "A guide to anti-misinformation actions."

[58] Reuters Staff. "Danish national first to be convicted under Malaysia's fake news law." Reuters. Published April 30, 2018. Accessed July 18, 2018.

networks for decades. If it is passed, this bill would require social media companies that have more than 50 million monthly users to publicize information about any political advertiser that spends more than $500 on their platforms. The public information would include: digital copies of any advertisement that the group purchases, a description of the target audience, the number of times each advertisement was viewed, contact information for the ad's purchaser, and finally the amount they paid for the ad. Social media platforms would also be required to make "reasonable efforts" to ensure that political ads are not purchased by a foreign national.[59] The French government has also proposed a similar law that would enforce more financial transparency of online political advertisements up to five months before an election, and require social media platforms to publish information about who is purchasing sponsored political content and for what price.[60]

Facebook and Twitter have both confirmed their support for the United States' proposed Honest Ads Act, and both platforms have stated that they will comply with the provisions if the law is passed.[61] This proposed legislation in the US and France is a good start for combatting untrustworthy, misleading, and foreign-sponsored political advertisements during campaigns, and it is reassuring that the world's top social media platforms are on board with the regulations. However, this type of legislation does not address the many other types of online disinformation, therefore other measures would need to be taken in order to form an effective front against disinformation.

Promoting quality news

[59] Timmons, Heather. "Honest Ads Act: Congress finally has a bill to regulate Facebook. Here's what it says." Quartz. Published October 18, 2017. Accessed July 12, 2018.

[60] Funke. "A guide to anti-misinformation actions."

[61] Picchee, Aimee. "Facebook: What is the Honest Ads Act?" CBS News. Published April 11, 2018. Accessed July 12, 2018.

Finally, certain governments are approaching the disinformation issue using a positive reinforcement model rather than a deterrence model. Instead of directly fighting or indirectly deterring disinformation, they are promoting and encouraging credible, high-quality news. For example, the Croatian government has created an initiative to educate citizens on how to recognize and support factual content.[62] Sweden has created a "psychological defense" authority ahead of the 2018 general election that will "ensure that factual public information can be quickly and effectively communicated even under disruptive conditions".[63] These initiatives offer a different way of thinking about combatting disinformation; rather than simply sanctioning disinformation, it may prove more effective to promote high-quality sources and media literacy instead.

Efficacy of governmental initiatives

As most of these governmental initiatives are in their beginning stages, it is difficult to tell whether or not they will be effective in combatting disinformation surrounding elections. The newest initiatives are still being edited and debated by legislative or regulatory bodies, while the oldest have only been in effect for a year. It should be point of further consideration in upcoming years to examine which initiatives have proved effective and which have proved fruitless.

At this moment, however, one can see why government-lead initiatives in general are necessary for combatting disinformation and protecting electoral integrity. Governmental initiatives encourage a united front of many actors, including social media platforms, independent fact checking organizations, public authorities, and political advertisers. It is essential that these actors coordinate their efforts in the fight against disinformation in order to make efficient and positive change. Furthermore, governmental initiatives can bolster and incentivize initiatives that have already been taken on by private companies, which will be discussed in the following section.

[62] Funke. "A guide to anti-misinformation actions."
[63] Ibid.

On the other hand, there are many risks involved in government intervention on the internet that need to be considered. First, there is the issue of who gets to decide what constitutes as disinformation. Is the piece of online content proven false and intentionally misleading, or is it merely a controversial opinion or conjecture? Second, governmental interventions risk criminalizing investigative journalism and condoning censorship. Third, there is the danger of limiting an individual's right to freedom of expression and privacy. It is clear that, while governmental initiatives are necessary for coordinating, incentivizing, and bolstering anti-disinformation efforts, they need to be conducted with extreme caution and scrutiny in order to avoid grave consequences such as hindering freedom of expression on the internet.

4. Examination of disinformation deterrence initiatives in the private sector

Private sector companies are also doing their part to mitigate the impact of disinformation on elections around the world. Deterrence initiatives are an invaluable component of global efforts to combat digital disinformation, because these private organizations have a close link to disinformation producers that governmental bodies lack. Social media websites provide platforms where media manipulators can publish their material, search engines are responsible for filtering results, and advertising agencies place ads on sites often without regard to content quality. Because these organizations have a clear and direct connection to the disinformation ecosystem, they have a unique ability to implement regulatory initiatives and alter market incentives to assuage the effect of disinformation on elections.

Social media companies

Social media companies are arguably the most important actor in the disinformation ecosystem, because millions of people rely on social media to obtain their news. According to the Pew Research Center, 67% of American adults report that they use social media to get at least some of their news.[64] Furthermore, social media has a low barrier-to-entry, meaning that anyone with internet access can make an account and start writing or sharing articles.

Despite their importance to the news media landscape, particularly during elections, social media companies are not considered media companies and are therefore not subject to the press laws that regulate other news outlets. However, several social media platforms are acknowledging their importance in the news media landscape and taking the initiative to combat digital disinformation using their own regulatory devices and deterrence tactics. Facebook is the social media platform that has done the most to actively prevent the spread of disinformation, due to the fact that the company received an immense amount of criticism after the 2016 US presidential election. Now, Facebook is paving the way and setting examples for how social media platforms can take an active role in preventing disinformation. Facebook released a report in April 2017 called "Information Operations and Facebook," delineating the company's stance regarding information operations, which it defines as "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome".[65] This report is a clear statement that Facebook is working towards holding itself accountable for disinformation on the platform. It states that "it is important that [Facebook] acknowledges and takes steps to guard against the risks that can arise in online communities [because Facebook is] in a position to help constructively shape the emerging information ecosystem by ensuring [the] platform remains a safe and secure environment for authentic civic engagement." This demonstrates the company's recognition of its responsibility for helping fight disinformation, and its capability to do so.[66] Facebook is "[expanding their] security

[64] Shearer, Elisa and Gottfried, Jeffrey. "News Use Across Social Media Platforms 2017." Pew Research Center. Published September 7, 2017. Accessed July 2, 2018.

[65] Weedon, Nuland, and Stamos. "Information Operations and Facebook." Page 4.

[66] Ibid. Page 3.

focus from traditional abusive behavior such as account hacking, malware, spam, and financial scams, to include more subtle and insidious forms of misuse, including attempts to manipulate civic discourse and deceive people".[67] This shift could become a precedent for other social media companies, regulatory bodies, and legislative bodies to begin including malevolent disinformation in their discussions of abusive or illegal content.

Facebook has several focus areas for combatting digital disinformation. It is putting an emphasis on detecting and disabling fake accounts, changing its algorithm to promote meaningful content, blocking targeted data collection and account hacking, promoting advertising transparency, and launching educational campaigns. It has made impressive strides towards disabling fake accounts by using new analytical techniques and machine learning to discover and disable bots. It is aiming to identify patterns of artificial activity without assessing content in order avoid unintentionally censoring content created by real users.[68] The company has proven successful in this regard; it removed 30,000 fake accounts leading up to the French presidential election in 2017.[69]

Many of Facebook's efforts are driven by user involvement. Users are able to report alleged disinformation by clicking on a special dialogue box attached to each post. If the post is reported by a certain number of users, the content is passed on to human fact checkers. If the fact checkers confirm that the post is fake or intentionally manipulated, it will be flagged as "disputed." Although the post can be further shared, the flag will warn future readers about the controversy surrounding the content.[70] Similarly, users have the option to click on a dialogue box attached to every advertisement on their feed in order to see where the ad came from and why they are seeing

[67] Ibid. Page 3.
[68] Ibid. Page 10.
[69] Freedom House. "Freedom on the Net 2017."
[70] Niklewicz. "Weeding Out Fake News." Page 33.

it. This allows people to understand the demographic factors that affect the advertisements they see on their news feed, as well as provide insight as to who is sponsoring the ad.

Facebook has also spearheaded multiple educational campaigns around the world to encourage media literacy amongst its users. It has partnered with multiple third-party fact checking organizations such as First Draft and the News Integrity Coalition to publish educational tools and tutorials to improve the public's ability to make informed judgments about the news they consume. It has also implemented online ads linking to tips for recognizing disinformation, as well as put up physical advertisements warning about clickbait, bots, and fake news.[71]

Search engines and advertising companies

Search engines are also important players in the disinformation landscape, because they have the capability to influence search results and ad placement, as well as assess websites for content quality. Google, the world's most widely used search engine, has made strides in the past two years to help fight disinformation. First, Google has changed its search rankings to promote high-quality news outlets over questionable ones. To achieve this, Google has set new standards for its team of "raters," which is a staff of more than 10,000 people who assess search results and flag websites that run hoaxes, conspiracy theories, and fake content.[72] Furthermore, in February 2017, Google launched "The Perspective," which is an artificial intelligence tool able to find abusive content without human assistance. The software does not delete the content on its own, but reports it to human fact checkers who are then able to decide whether or not the content should be taken down.[73]

[71] Thomas, Daniel. "Facebook to tackle fake news with educational campaign." Published April 6, 2017. Accessed June 27, 2018.

[72] Caplan, Robyn, Hanson, Lauren, and Donovan, Joan. "Dead Reckoning: Navigating Content Moderation after 'Fake News.'" Data&Society. Published February 2018. Accessed July 10, 2018. Page 22.

[73] Niklewicz. "Weeding Out Fake News." Page 35.

Additionally, advertising companies such as Google AdSense and Facebook Audience Network are working with search engines and social media platforms to help demonetize disinformation by restricting advertising on sites that use “deceptive and misleading content”. With a combined market share of 63.1% of the US digital ad market, these two companies will be decisive in determining which content will or will not be monetized. They are planning on blocking advertising revenue from pages that “misrepresent, misstate, or conceal information about the publisher, the publisher’s content, or the primary purpose of the web property,” which will eliminate the financial motivation for producing disinformation and incentivize publishers to be more transparent about their identity and mission. So far, the companies are experiencing success with this endeavor; for example, Google AdSense banned advertising on 200 fake news sites in less than two months.[74]

Fact checking organizations

Third-party fact checking organizations have proved to be quite valuable in combatting disinformation. They are unique actors because they are not attached to a specific social media platform, search engine, or news outlet, and they are not making money off advertising revenues. This independence renders fact checking organizations fairly trustworthy because they have no direct financial stake in the disinformation economy. Some well-known fact checking establishments include First Draft News, Bellingcat, FactCheck.org, Snopes.com, TruthorFiction.com, HOPE not Hate, and Politifact.[75] These organizations investigate and debunk disinformation, as well as provide professional and citizen journalists with tools for verifying user-generated content, monitoring manipulation campaigns, and recognizing fake news.[76] Other fact

[74] Caplan, Hanson, and Donovan. “Dead Reckoning.” Page 21.

[75] Niklewicz. “Weeding Out Fake News.” Page 35.

[76] Freedom House. “Freedom on the Net 2017.”

checking organizations target their efforts towards advertising companies in an attempt to demonetize digital disinformation. Organizations and projects such as Open Brand Safety, the News Integrity Initiative, Storyful, and Moat develop whitelists of safe content for ad buys, in addition to working directly with advertisers to remove their ads from untrustworthy sites. They track web domains and video URLs that have been identified as spreaders of misinformation and then provide the information to platforms and advertisers who control ad placement.[77]

Efficacy of disinformation deterrence initiatives

There is a lot of potential for private organizations to create innovative and efficient ways of identifying and preventing the proliferation of disinformation because of their technical expertise, regulatory capacity, and influence over market structure. Disinformation deterrence initiatives can come from a wide range of actors, including social media platforms, search engines, advertising companies, and independent fact checking organizations. The initiatives can also utilize a variety of tactics, such as media literacy campaigns, blacklisting untrustworthy sources, altering advertising markets, using artificial intelligence to detect bots and fake sources, and improving search algorithms. That being said, it is crucial for these actors to coordinate their efforts in order to create effective disinformation deterrence initiatives that complement each other and work well together within the complex media disinformation landscape.

5. Model legislative and regulatory framework

Examining the methods and motivations behind digital disinformation, current governmental initiatives against disinformation, and private deterrence initiatives has helped inform the creation of a model legislative and regulatory framework that can be used as a guideline for preventing disinformation from damaging electoral integrity. This framework is applicable to

[77] Caplan, Hanson, and Donovan. "Dead Reckoning." Page 20.

any country that hosts democratic elections and can be modified slightly to better fit electoral procedures in a given country. It is meant to uphold existing international electoral standards, as well as modernize them to account for the constantly changing information landscape of the digitized and globalized 21st century.

There are certainly many challenges to developing and following an anti-disinformation framework, many of which mirror the challenges that governments and private organizations have faced while creating their own initiatives. First and foremost, there is the risk of infringing on the right to free speech and free expression. It is crucial to ensure that the initiatives in this framework are not manipulated to justify engaging in unlawful censorship or punishing journalists and citizens for having controversial views. Second, the internet is perceived as a free and open environment, therefore any attempt to regulate online content might be misconstrued as government-sanctioned censorship. Third, social media companies and advertising networks might be tempted to preemptively remove posts or advertisements before they are proven to be disinformation in order to comply with the framework and avoid criticism. Finally, there is no “one size fits all” model for regulation and legislation, because every country has its own press laws, internet laws, electoral standards, and perception of what constitutes as disinformation.

Despite these challenges, it remains increasingly important to develop a legislative and regulatory framework to help combat disinformation that threatens the integrity of elections. First, simply the act of creating a framework and constructing guidelines to mitigate disinformation will demonstrate that the global community is united under the common goal of protecting fair and credible elections. It will show that countries that value democratic elections are taking the threat of disinformation seriously, and hopefully will deter people, groups, and countries who are producing disinformation from continuing to manipulate elections. Second, developing a comprehensive framework could bolster the strength of initiatives that have already been taken on by private organizations such as social media companies and advertising networks.[78] Third, there are many actors in the anti-disinformation environment, including national governments, regulatory bodies, social media platforms, advertising networks, news outlets, search engines, and independent fact checking organizations, therefore an international framework would be helpful for coordinating all of these players and orienting them towards a common objective and methodology. Finally, while freedom of expression and freedom of speech should be inalienable rights for typical citizens, it is naïve to guarantee these unrestricted rights to those who produce and intentionally spread disinformation. The goal of disinformation producers is to stifle and confound the political discussion, spread confusion, promote certain ideologies, and drown out legitimate voices. In the long-term, their actions erode democratic values, therefore they should not be awarded the rights granted by the institution that they are undermining.[79] Therefore, it is necessary to construct a legislative and regulatory framework that demonstrates the global community's commitment to fighting electoral disinformation, bolsters existing anti-disinformation initiatives, brings together a variety of anti-disinformation actors, cripples the efforts of ill-intentioned disinformation producers, and protects democratic elections around the world.

Social media responsibility

Social media platforms are an integral component of this model legislative and regulatory framework, and their participation is crucial in its success. As previously stated, at this moment social media companies are not considered purveyors of the news. However, the digital landscape has shifted dramatically in the past decade, and social media companies as well as press regulation

[78] Information Society Project. "Fighting Fake News." Page 14.

[79] Niklewicz. "Weeding Out Fake News." Page 43.

bodies need to recognize the influential role that social media plays in today's information ecosystem. In December 2016, following the United States presidential election, Mark Zuckerberg himself admitted that Facebook is a 'media company', and not just a mere 'platform'.[80] In light of the current digital landscape, this framework considers social media platforms as quasi-media companies, and therefore they should be regulated by modified versions of existing press laws. This shift in mindset would allow governments to hold social media platforms more accountable for the content on their websites.[81] One-way regulatory bodies could enforce this is through a modified "notice and correct" procedure, which is a press law that has been applied to the traditional press for years. With the notice and correct procedure, social media platforms would have to correct or take down false information at the request of the genuinely affected party. That means that the legal responsibility of the social media platform would kick in the moment it receives notification of the content. The platform would not be obligated to monitor all content on its website in search of disinformation, because that would be inefficient, burdensome, and could lead to social media censoring innocent users.[82]

In addition to compliance with modified press laws, there are numerous technical changes that social media companies can make in order to play a more active role in combatting disinformation. A legislative and regulatory framework should include requirements for social media companies to update their interfaces with technical advancements with the aim of curbing disinformation. First and foremost, social media companies need to improve their algorithms to identify and demote obviously false content. Facebook has already had a great deal of success with identifying and deleting automated bot accounts. However, improving algorithms to delete or

[80] Ibid. Page 39.
[81] Ibid. Page 43.
[82] Ibid. Page 41.

demote all false content is understandably difficult. Many instances of disinformation are more insidious than bots and are not blatantly false in a way that can be easily detected by artificial intelligence.[83] To mitigate this challenge, social media companies can empower users to help detect and avoid disinformation. For example, social media platforms should start letting users customize their feed and search algorithms, allowing them to consciously select to see diverse political content, alternative views, or a larger amount of international content on their feeds.[84] This action will lessen the prevalence of filter bubbles and hopefully hinder the dissemination of disinformation within filter bubbles. Additionally, all social media platforms should have an option for users to report disinformation, and a system for investigating and acting on such reports.

Other technical changes that should be adopted by social media platforms to help combat disinformation include installing user-friendly fact checking and verification tools with the support of technology companies, such as image verification plug-ins.[85] This would allow users to actively ensure that they are consuming credible content. Social media companies should also require that shared content that has been proven false is flagged and reflects subsequent revisions so that disinformation does not continue to spread after it has been debunked.[86] If these technical alterations are implemented together, along with compliance to a modified set of existing press laws, social media companies would be enabled to take a more active role in combatting disinformation surrounding elections.

Regulating advertising networks

Regulating advertising networks is a crucial element of this model legislative and regulatory framework, because many disinformation producers are motivated solely by the money

[83] Information Society Project. “Fighting Fake News.” Page 10.

[84] Tucker, Joshua A. et al. “Social Media, Political Polarization, and Political Disinformation.” Page 59.

[85] Ibid. Page 59.

[86] Information Society Project. “Fighting Fake News.” Page 8.

they receive from advertising revenue. If advertising networks stopped allowing ads on proven disinformation sites, it would eliminate the financial incentive behind producing disinformation. The principle type of advertising that this framework addresses is programmatic advertising. Programmatic advertising is "advertising sold automatically on the basis not of which outlet or news brand it will appear in, but on the basis of how many 'clicks' or views it will receive from a target demographic," regardless of content.[87] Whereas individual advertisers have the ability to select where their ads will appear, programmatic advertising indicates that the advertisers do not decide where their content will appear, or which websites will make money off of their ad purchase. Instead, algorithms make these assessments based on web traffic, often without human review of the publishers or websites that are receiving revenue from the ad. This means entities that publish disinformation websites will receive advertising revenue from programmatic ads if their site receives enough web traffic. Therefore, it is essential to cut off programmatic advertising for sites that are suspected to be purveyors of disinformation.[88] Facebook's Audience Network and Google's AdSense are important advertising companies to target with this initiative, because they have a combined market share of 63.1% of the US digital ad market and a significant share of the global ad market. This demonstrates that these two advertising giants play an important role in deciding what type of content will and will not be monetized, and it is crucial that they are on board with cutting off programmatic advertising on disinformation sites.[89]

Education and training

Lastly, one of the most important aspects of this model framework for combatting disinformation surrounding elections is providing education and training to political parties,

[87] Caplan, Hanson, and Donovan. "Dead Reckoning." Page 19.

[88] Ibid. Page 19.

[89] Ibid. Page 19.

campaigns, and citizens. Everyone should receive some form of media literacy education; it should be adopted into school curriculums and made available for adult education. Online training modules and toolkits hosted on social media platforms or government-funded websites would be an excellent way to reach a wide population and provide equitable access to resources. Consumers need to be educated in how to recognize disinformation, how to diversify their news sources, how disinformation spreads throughout the internet, the stakeholders and actors in the disinformation landscape, and how to identify credible sources. Additionally, political parties and campaigns need to be trained about disinformation and political interference in order to protect the integrity of their campaigns. It is unrealistic to think that disinformation will ever completely disappear, because the digital landscape is always changing and there will always be entities that want to use it to undermine democratic integrity. Therefore, it is essential that a framework for combatting disinformation includes a comprehensive plan for educating citizens in media literacy, because that is the most foolproof way of avoiding disinformation and promoting high-quality information on an individual level.

Conclusion

This paper has shown how democratic elections can be influenced by disinformation, evaluated governmental initiatives combatting disinformation, and examined disinformation deterrence initiatives implemented by private organizations. These analyses have informed the creation of a model legislative and regulatory framework that can be adopted into the electoral policies of any country that hosts democratic elections. This model framework approaches the digital disinformation phenomenon by positive reinforcement of high-quality information and deterrence of untrustworthy information. Instead of simply sanctioning and criminalizing disinformation, this framework empowers citizens, political campaigns, and social media platforms to take an active role in promoting credible information and rejecting false information. It emphasizes public media literacy education, supporting democratic campaigns, weakening financial incentives for disinformation, and holding social media companies accountable for their role in the digital information landscape. This methodology places a focus on empowering civil society and adjusting information distribution so that it is more balanced and less prone to manipulation. Consequently, the framework does not specifically target and criminalize disinformation solely based on content, therefore there is little room for accidental encroachments on freedom of speech and freedom of expression.

In the social media age, it is critical that the disinformation phenomenon is adopted into the discourse surrounding international electoral standards. The information landscape is constantly changing and there are innumerable actors that have the ability to manipulate it for their own benefit. As long as there is an open internet and entities who are motivated by strong political ideologies or financial incentives, disinformation will be an issue with democratic elections. Therefore, it is crucial that the international community recognizes disinformation as a substantial threat to electoral integrity and develops a comprehensive, actionable framework that coordinates efforts to hinder the spread of disinformation and promote high-quality information surrounding elections.

Glossary

Astroturfing: Creating the illusion of widespread, grassroots support for a certain politician, policy, or ideology

Bots: Automated accounts on social media posing as humans that are utilized to amplify messages, drown out genuine voices, promote false claims, and create an artificial sense of popularity or relevance

Computational propaganda: The use of algorithms, automation, and human curation to purposefully distribute misleading information over the internet[90]

Cyber troops: Teams sponsored or controlled by the government or military committed to manipulating public opinion over social media, blogs, and message boards[91]

Disinformation: False information or decontextualized information that is purposefully produced and distributed in order to contribute to a larger ideological or financial agenda[92]

Eco-chamber: An online environment in which beliefs are amplified or reinforced by communication with others who share similar ideologies

Fact checking organizations: Independent organizations that check the veracity of online content and news stories. Several examples of fact checking organizations include First Draft, Bellingcat, FactCheck, Snopes, Truthorfiction, HopeNotHate, and Politifact.

Fake news: Broad term referring to intentionally misleading online content, including everything from incorrect news articles, hoaxes, rumors, manipulated images, fake accounts, and online abuse. This term has been politicized and appropriated by politicians who are looking to criticize the mainstream media when they are represented in an unflattering manner.

False amplification: Coordinated activity by inauthentic accounts with the intent of manipulating political discussions (e.g., by discouraging specific parties from participating in discussion, or amplifying sensationalistic voices over others)[93]

Filter bubble: Enclosed spaces of social media users that consumer, whether consciously or not, the same content and are not exposed to alternative information or opinions[94]

[90] Hwang. "Digital Disinformation: A Primer." Page 1.

[91] Bradshaw and Howard. "Troops, Trolls, and Troublemakers." Page 9.

[92] National Endowment for Democracy. "Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News."

[93] Weedon, Nuland, and Stamos. "Information Operations and Facebook." Page 5.

[94] Niklewicz. "Weeding Out Fake News." Page 17.

Hyperpartisan media: Media outlets that are either extremely far to the right or to the left of the political spectrum that manipulate readers by combining decontextualized truths, repeated falsehoods, and leaps of logic to create a fundamentally misleading view of the world[95]

Information Operations: Actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome[96]

International electoral standards: A values-based set of guidelines upon which election laws are constituted meant to ensure fair democratic processes and equitable access for all citizens

Internet trolls: Anonymous citizens on the internet who deliberately bait others with the objective of achieving an emotional response, often not motivated by a specific ideology, but interested in offending people with shocking material in order to disrupt electoral proceedings and cause confusion[97]

Misinformation: Inadvertent sharing of false information[98]

Programmatic advertising: Advertising sold automatically on the basis not of which outlet or news brand it will appear in, but on the basis of how many ‘clicks’ or views it will receive from a target demographic[99]

Selective censorship: Removing some pieces of content from a platform in order to decontextualize the content that remains

Targeted data collection: Stealing and often exposing non-public information that can provide unique opportunities for controlling public discourse[100]

[95] Tucker, Joshua A. et al. “Social Media, Political Polarization, and Political Disinformation.” Page 5.

[96] Weedon, Nuland, and Stamos. “Information Operations and Facebook.” Page 4.

[97] Marwick and Lewis. “Media Manipulation and Disinformation Online.” Page 4.

[98] National Endowment for Democracy. “Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News.”

[99] Caplan, Hanson, and Donovan. “Dead Reckoning.” Page 19.

[100] Weedon, Nuland, and Stamos. “Information Operations and Facebook.” Page 6.

Bibliography

Bradshaw, Samantha and Howard, Philip N. "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation." University of Oxford Computational Propaganda Research Project. Published December 2017. Accessed June 12, 2018. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Brattberg, Eric and Maurer, Tim. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace. Published May 23, 2018. Accessed July 14, 2018. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

Caplan, Robyn, Hanson, Lauren, and Donovan, Joan. "Dead Reckoning: Navigating Content Moderation after 'Fake News.'" Data&Society. Published February 2018. Accessed July 10, 2018. https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf

The Carter Center. "Election Obligations and Standards: A Carter Center Assessment Manual." Published 2010. Accessed July 9, 2018. https://www.cartercenter.org/resources/pdfs/peace/democracy/cc-oes-handbook-10172014.pdf

Etter, Lauren. "What Happens When the Government Uses Facebook as a Weapon?" Bloomberg Businessweek. Published December 7, 2017. Accessed July 16, 2018. https://www.bloomberg.com/news/features/2017-12-07/how-rodrigo-duterte-turned-facebook-into-a-weapon-with-a-little-help-from-facebook

European Union External Action Service. "Compendium of International Standards for Elections." Published 2016. Accessed July 8, 2018. https://eeas.europa.eu/sites/eeas/files/compendium-en-n-pdf_0.pdf

Freedom House. "Freedom On The Net 2017: Manipulating Social Media to Undermine Society." Published November 2017. Accessed June 20, 2018. https://freedomhouse.org/report/freedom-net/freedom-net-2017

Funke, Daniel. "A guide to anti-misinformation actions around the world." Poynter. Last modified July 2, 2018. Accessed July 9, 2018. https://www.poynter.org/news/guide-anti-misinformation-actions-around-world

Harding, Luke. "What we know about Russia's interference in the US election." The Guardian. Published December 16, 2016. Accessed July 23, 2018.

https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election

Hwang, Tim. “Digital Disinformation: A Primer.” Atlantic Council. Published September 2017. Accessed July 13, 2018. http://www.atlanticcouncil.org/images/Digital_Disinformation_Primer_web_0925.pdf

Information Society Project. “Fighting Fake News: Workshop Report.” Yale Law School. Published March 7, 2017. Accessed July 2, 2018. https://law.yale.edu/system/files/area/center/isp/documents/fighting_fake_news_-_workshop_report.pdf

International IDEA. “International Electoral Standards: Guidelines for reviewing the legal framework of elections.” Published 2002. Accessed July 9, 2018. https://www.idea.int/sites/default/files/publications/international-electoral-standards-guidelines-for-reviewing-the-legal-framework-of-elections.pdf

Marwick, Alice and Lewis, Rebecca. “Media Manipulation and Disinformation Online.” Data&Society. Published May 15, 2017. Accessed July 3, 2018. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

Morris, James and Nguyen, Son. “Thai Government warns about fake news online as political discourse picks up before elections.” Thai Examiner. Published June 21, 2018. Accessed July 17, 2018. http://www.thaiexaminer.com/thai-news-foreigners/2018/06/21/thailand-speech-online-news-commentary-fake-news-thai-government/

National Endowment for Democracy. “Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News.’” Published October 17, 2017. Accessed June 3, 2018. https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/

Niklewicz, Konrad. “Weeding Out Fake News: An Approach to Social Media Regulation.” Wilfried Martens Centre for European Studies. Published 2017. Accessed June 14, 2018. https://www.martenscentre.eu/sites/default/files/publication-files/mc-weeding_out_fake_news_v3_web.pdf

Picchee, Aimee. “Facebook: What is the Honest Ads Act?” CBS News. Published April 11, 2018. Accessed July 12, 2018. https://www.cbsnews.com/news/facebook-hearings-what-is-the-honest-ads-act/

Reuters Staff. “Danish national first to be convicted under Malaysia's fake news law.” Reuters. Published April 30, 2018. Accessed July 18, 2018.

https://www.reuters.com/article/us-malaysia-palestinian-fakenews/danish-national-first-to-be-convicted-under-malaysias-fake-news-law-idUSKBN1I10I9

Shearer, Elisa and Gottfried, Jeffrey. "News Use Across Social Media Platforms 2017." Pew Research Center. Published September 7, 2017. Accessed July 2, 2018. http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/

Thomas, Daniel. "Facebook to tackle fake news with educational campaign." Published April 6, 2017. Accessed June 27, 2018. https://www.bbc.com/news/technology-39517033

Timmons, Heather. "Honest Ads Act: Congress finally has a bill to regulate Facebook. Here's what it says." Published October 18, 2017. Accessed July 12, 2018. https://qz.com/1105987/congress-may-try-to-regulate-political-ads-in-the-internet-like-those-on-broadcast-television/

Tucker, Joshua A. et al. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." Hewlett Foundation. Published March 2018. Accessed June 28, 2018. https://hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf

Weedon, Jen, Nuland, William, and Stamos, Alex. "Information Operations and Facebook." Facebook. Published April 27, 2017. Accessed June 27, 2018. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

West, Darrell M. "How to combat fake news and disinformation." Brookings Institution. Published December 18, 2017. Accessed June 9, 2018. https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/