Supporting Information Integrity and Civil Political Discourse

2018

Table of Contents

Overview

The purpose of this resource is to raise awareness about the threat of disinformation and how it is being used to undermine the functioning of democratic institutions and processes. The resource is intended to assist civic and political activists with an interest in protecting the space for informed dialogue and public deliberation. This includes ensuring the flow of accurate information and supporting the practice of civil political discourse.

Terms

Disinformation
False or inaccurate information that is deliberately created or disseminated with the explicit intent to mislead and cause harm

Misinformation
False or inaccurate information, but not intended to cause harm

Malinformation
Genuine information that is shared to cause harm, often by moving information designed to stay private into the public sphere, such as doxing

Algorithm
A fixed series of steps that a computer performs in order to solve a problem or complete a task. For example, social media platforms use algorithms to compile the content that users see. These algorithms in particular are designed to show users material that they will be interested in, based on each user's history of engagement on that platform.

Automation
The process of designing a 'machine' to complete a task with little or no human direction. It takes tasks that would be time-consuming for humans to complete and turns them into tasks that are completed quickly and almost effortlessly.

Bots
Social media accounts that are operated entirely by computer programs and are designed to generate posts and/or engage with content on a particular platform

Botnet
A collection or network of bots that act in coordination and are typically operated by one person or group

Deep Fakes
Describes fabricated media produced using artificial intelligence (AI). By synthesizing different elements of existing video or audio files, AI enables relatively easy methods for creating 'new' content, in which individuals appear to speak words and perform actions, which are not based on reality.

Fact-checking
The process of verifying the truthfulness and accuracy of official, published information such as politicians' statements and news reports

Manufactured Amplification
Occurs when the reach or spread of information is boosted through artificial means

Propaganda
True or false information spread to persuade an audience, but often has a political connotation and is often connected to information produced by governments

Trolling
The act of deliberately posting offensive or inflammatory content to an online community with the intent of provoking readers or disrupting conversation. The term **"troll"** is most often used to refer to any person harassing or insulting others online.

Troll Farm
A group of individuals engaging in trolling or bot-like promotion of narratives in a coordinated fashion

A Proliferating Global Threat to Democracy

Information is a source of power and democratic systems have the potential to distribute that power. In this respect, information is liberating when citizens can openly impart, receive and compare it as they exercise the fundamental freedoms of speech, assembly and association. Democracy also relies on the active engagement of citizens in public life. This includes participation in political processes, such as regular, competitive elections that decide the composition of government. Participation, in turn, depends on faith in institutions that work in the public interest. This relationship represents a social contract between citizens and the state that, in part, relies on the flow of accurate information that allows citizens to understand what the government is doing and to make choices about different courses of action that hold the government accountable.

The integrity of information is vital to a healthy democracy. When information is false or inaccurate, it can negatively impact citizens' discussions of issues and their political decisions, leading to a breakdown in civil discourse and inhibiting compromise. The ability of citizens to discuss ideas about politics and public affairs in an informed, respectful manner is integral to sustaining long-term democratic health and also includes dialogue and deliberations that happen within government and amongst politicians. Likewise, the work of the government needs to be understood by citizens and information needs to be made available so that citizens are able to hold government actors accountable for decisions.

Democracy is threatened when false and misleading information is propagated and purposefully used to weaken public trust, increase polarization, exclude certain voices, and limit the ability of citizens to act individually or collectively. Disinformation can be particularly acute during elections in which there are significant, preexisting divides over priorities and policies. During these periods, disinformation can sway voter preferences, disrupt the normal functioning of the election process and foster public frustration and disaffection. However, not every attempt at disinformation is linked to a specific event such as an election. Disinformation can also be used to alter the broader information space in which people discuss issues, form beliefs, and make political decisions. Disinformation is sometimes deployed to promote a larger narrative over time or to degrade civic discourse by promoting division or cynicism.

Authoritarian actors often take various steps to influence the flow of information. These may include cutting off access to independent sources of information and public debate; controlling media outlets and the content of information being provided; or deliberately spreading disinformation that is false to mislead the public. These actors find great value in any action that degrades public trust and disrupts the political participation of their democratic counterparts.

Technology has fundamentally altered the production and consumption of information in a number of ways.[1] As the internet is becoming more widely accessible, faster and less expensive, billions of people are able to share information with one another more easily than they could before. This technological shift includes the growth of social media, which has made the consumption of information shared through online networks public rather than private, and controlled by several large companies. The speed at which information is shared has also grown, as the number of mobile devices has increased and the news cycle has accelerated. With information being exchanged more rapidly and in real-time between peers, the accuracy of shared information, in some cases, is less likely to be contested. In other cases, the flood of information being shared is overwhelming and it becomes more challenging to decipher what is accurate and what is false. The lack of contestation is especially true with digital environments becoming more personalized through algorithms that match content with user tastes and preferences. These factors, which have characterized the digital revolution, have enhanced public vulnerability to manipulation by inaccurate information.

The digitization of the information space is complicated by the challenges people face in contending with the fast pace of technological change. Psychological factors and socio-cultural norms shape how people process information, with different types of information generating either rational or irrational responses. Digital media environments, especially social media platforms where information is rapidly shared, may promote an immediate, illogical processing of information rather than rational responses that rely on careful scrutiny.[2]

While the manipulation of information in democracies is not new, digital technology has increased the magnitude of this problem by allowing malicious actors to anonymously manipulate public opinion and threaten the integrity of information. Social media amplifies these effects due to the relatively low cost and speed of disseminating information to a large audience.[3] This is often augmented by automated systems such as bots that push content to users who can be targeted through data about their personal preferences and demographics.

> "Political actors have used disinformation for their benefit for millennia. However, the velocity and volume of disinformation in the contemporary information space seems to have amplified its effectiveness and left many members of the public increasingly angry, fearful, or disoriented. This, in turn, leaves publics even more vulnerable to future manipulation, resulting in a cycle of declining public trust in objective sources of information which some analysts call "truth decay."
>
> — NED Issue Brief: How Disinformation Impacts Politics And Publics

Explanation of Common Terms

Fake news is a term that has been used interchangeably with disinformation or other types of disorder within the information ecosystem and has become a broad term used to describe news that is inaccurate or fabricated. However, the term "fake news" does not accurately describe the complexity of disinformation, misinformation and malinformation, and is often used by authoritarians and others to degrade true speech they don't like, conflating it with false narratives.[4]

Disinformation is false information deliberately created to cause harm to a person, social group, organization or country. Disinformation is not always composed of outright lies. It can also be facts that have been separated from the original context, facts that are distorted by prejudicial or discriminatory rhetoric, or facts that are blended with false information.

Example
California-based cybersecurity company FireEye uncovered a years-long disinformation campaign targeting Latin America, the Middle East, the United Kingdom and United States.[5] The company found over 600 social media accounts based in Iran aiming to spread disinformation across the globe. FireEye shared this information with Facebook in 2018, leading to the removal of 652 fake accounts and pages for "coordinated inauthentic behavior."

Misinformation is false information, but created without the intent of causing harm.

Example
Following a bombing attack in Manchester, England in 2017, a local newspaper erroneously tweeted information about a gunman outside a local hospital. This information was later discovered to be false and the newspaper retracted their previous tweet.[6]

The role of intent in the dissemination of false information is key to understanding the difference between misinformation and disinformation. Disinformation is typically part of a deliberate effort to deceive, influence or manipulate, while misinformation may not be intended to deceive. Even with this distinction, the intentions behind the creation and sharing of information may not always be clear.

Malinformation refers to factual information that is deliberately used to inflict harm on a person, organization or country.

> **Example**
> During the 2016 U.S. presidential primary process, emails from the Democratic National Committee (DNC) were selectively leaked to the public to demonstrate the DNC's alleged bias during the campaign.[7]

Propaganda refers to campaigns that disseminate information designed to manipulate audiences by generating specific attitudes or provoking specific actions.[8]

> **Example**
> North Korea is well-known for propaganda campaigns to indoctrinate its population. Nearly all forms of media including music, art, and film are centered on national pride. Limited access to internet and censorship of social media contribute to the agenda-setting by the North Korean government.[9]

Public information campaigns refer to organized communicative activities that aim to reach large groups of people and shape public attitudes, values, or behavior in the hope of reaching some desirable social outcome. This term should be distinguished from propaganda which implies deliberate intent to manipulate or deceive.

> **Example**
> In 2016, the Greek island of Syros began a public information campaign to inform the population about the harmful effects of pollution. Research found that the campaign successfully changed public attitudes towards littering, leading to a reduction in plastic waste levels in the local marine environment.[10]

Common Types of Mis- and Disinformation

There are many forms of mis- and disinformation. Claire Wardle of First Draft News separated the types of mis- and disinformation into seven distinct categories to explain the spectrum of problematic content found online and in the media.

Misinformation

Type	Description	Example
Satire	No intention to cause harm, but has the potential to fool	A humorous television show or social commentary
False Connection	When headlines, visuals or captions don't support the content	"Clickbait" an online news article with shocking or controversial titles
Misleading Content	Misleading use of information to frame an issue or individual	A photo that leads audiences to believe a specific person was in a certain location and they weren't

Disinformation

Type	Description	Example
False Context	When genuine content is shared with false contextual information	Factual information and genuine photos are mispaired
Imposter Content	When genuine sources are impersonated	False information that is incorrectly attributed with a major, credible news source
Fabricated Content	Content that is 100% false and is designed to deceive or do harm	Photoshopped images or fabricated information presented as facts
Manipulated Content	When genuine information or imagery is manipulated to deceive	Genuine photo paired with fabricated text

Perpetrators and Motives

Intent is a key distinguishing feature between what constitutes as mis- or disinformation. The motives that drive actors to create, produce and share disinformation provide additional insight into the phenomenon and can be separated into four categories: financial, political, social and psychological. Both state and non-state political actors may use disinformation as a means of manipulating the opinions or views of their targets. Politicians may propagate disinformation about institutions or political opponents, both foreign and domestic, in order to suppress their voice and manipulate discourse.[11] These political actors may be affiliated with governments or may be private actors who coordinate with others to act in support of a shared ideological belief.

Other actors who spread disinformation may be driven by non-political motives, such as entertainment or increased profit. Advertising on the internet now provides a financial incentive to create disinformation that can be rapidly shared and attract online traffic towards a certain website. The manipulation of social networks internal mechanisms for providing content (algorithms), and the information itself to garner attention, can be driven by corporate or independent actors who may seek greater profits from redirected online traffic. Misleading online consumers may be incidental in pursuit of the primary goal of profit seeking, since entertainment and news exist alongside one another on social media sites.[12] Other independent actors may be driven by different motives such as an opportunity to promote personal issues, fame, or even simply to aggravate or "troll" people.

Dissemination of Information

Significant growth in the digital media landscape increases the number of ways disinformation can be disseminated. Social media platforms have become primary tools for disinformation campaigns due to their popularity worldwide and the ease of sharing through private groups and personal networks.[13] While social media tools have legitimate uses, they can also be exploited for other purposes.

Social media platforms through which mis- and disinformation have been shared:

- Facebook
- Twitter
- YouTube
- Blogs
- Message boards

In addition to the list above, mobile messaging applications have become increasingly popular vehicles for disinformation. These applications differ slightly from other social media platforms because mobile messaging applications are designed for private conversations between actors rather than acting as public fora for multiple actors.[14] Applications like WhatsApp, Viber, Telegram, and WeChat feature end-to-end message encryption that prevents anyone from examining the content of the message, including the company.

While social media has been a primary vehicle for disinformation, more conventional news media sources have also historically been used to spread disinformation, such as:

- Newspapers
- Television
- News websites
- Radio

The relationship between traditional media sources and social media in the information landscape reveals a complex dynamic. Social media may be used to distort and amplify stories that travel through different forms of traditional news media and traditional media sources often report on and reflect trends in social media. This creates a negative feedback loop of disinformation that magnifies inaccurate information. Often simply repeating information or fact-checking content online has the unintended consequence of further amplifying false information.

Common Instruments of Disinformation

Purveyors of disinformation have relied on a number of tactics to spread disinformation, especially through digital landscapes. Many of these strategies are considered **computational propaganda**, defined by the Oxford Internet Institute as "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks."[15] Computational propaganda is a method by which disinformation content may be shared. Some examples of tactics include:

- **Fake personae and trolls:** actors attempting to spread disinformation may rely on the creation of fake social media profiles under false names to provide cover and credibility for the information that is shared. Similarly to bots, trolls can amplify disinformation, however, trolls target specific actors and troll farms work efficiently to silence opposition during a disinformation campaign.
- **Algorithm manipulation:** a strategy of manipulating social media network trends to make disinformation more prevalent. Algorithm manipulation can be either employed to spread disinformation or counter its dissemination, but manipulating trends to fight disinformation represents a more aggressive strategy.
- **Social media bots:** automated accounts designed to quickly disseminate disinformation or communicate with people. While many bots are used to quickly share information of all types, they have also been adopted by actors to manipulate social media algorithms and change what information consumers see. A botnet network can be used to draw attention to misleading narratives and create the illusion of public discussion and support.
- **Visual imagery:** may be used to trick audiences through the manipulation of pictures or video. A new trend, known as "deepfakes", involves the creation of fake videos using images of real people, compiled from a variety of audio and visual sources that are designed to fool audiences and experts alike.[16]
- **Memes, or cultural content:** designed to be virally shared, these can take the form of text, images, or video.

- **Doxing:** a type of malinformation where someone researches, hacks and publishes private or identifiable information on the internet about an individual or an organization with malicious intent. This information can include names, addresses, phone numbers or credit card details and may be used to coerce, extort or harass the target.

Countermeasures to Deter Disinformation

Civil society, technology companies, political parties, governments and citizens have taken numerous measures to counter disinformation. Digital security is critical to preventing information from being manipulated or shared with actors who would use the information to cause harm, and can include strengthening passwords, utilizing virtual private networks (VPNs), and enabling two-factor authentication.

Technology companies have begun taking the following measures against disinformation:

- **Detecting automated bots:** While not all bots are designed for deceitful purposes, understanding the context in which automated accounts are being used to pollute the digital information space is crucial to identifying bots that spread disinformation and taking steps to stop their activities.[17] Detecting automated accounts can help counter the spread of disinformation, especially through social media platforms like Facebook and Twitter.
- **Network analysis:** Tracing the patterns of automated accounts is a key means of understanding of how disinformation campaigns operate and how actors coordinate with one another to increase the reach of certain pieces of disinformation.

Fact-checking of traditional media outlets and the information that is shared is another potential countermeasure against disinformation. Fact-checking should be part of a multi-pronged approach taken by different actors, such as civil society organizations, political parties, education ministries, legislators and technology companies. Gauging the accuracy and intent of information can be challenging, as fact-checkers cannot always respond as quickly as disinformation is spread. Fact-checking of traditional media outlets must also be matched by similar efforts from social media outlets to ensure that they do not recirculate false information.

> **Example**
> A company in Taiwan developed a fact-checking tool within the LINE messaging platform called CoFacts. This tool compiles a database of popular disinformation messages and relies on collaborative action from fact-checkers and users.[18]

> **Example**
> Automated fact-checking tools, such as Chequeabot in Argentina and Full Fact in the United Kingdom, have attempted to counter the problem of recirculating false information by automatically checking claims made in news media against official statistics and verified information.[19]

Another important component of countering disinformation is **restoring citizen trust in political institutions**, including the media. The growing lack of trust in the ability of institutions to provide accurate and impartial information has provided opportunities and space for actors seeking to promote disinformation. This further impacts the ability of citizens to trust the information they receive. Building trust in institutions requires healthy dialogue between actors, such as political parties and citizen rights organizations, in order to better understand the nature of how disinformation impacts democracy. This includes establishing guidelines for appropriate behavior in online campaigns, especially where disinformation may play a role in shaping campaign conduct. During election

periods, citizen election monitors can, and do, help mitigate the effects of disinformation based on their understanding of the local context and the media environment in which citizens consume information. Citizen election monitors can also help track online content and monitor traditional media outlets as part of their efforts to combat false narratives. Election monitors may need additional assistance to identify and understand the targets and impact of false narratives.

Civil society organizations (CSOs) have been involved in efforts to strengthen the integrity of information through education campaigns and their increasing involvement in improving media literacy among citizens. Media and information literacy campaigns and efforts to improve citizens' critical consumption of media, especially in digital spheres, have become a popular strategy for countering disinformation. Women, young people and older populations are groups targeted more frequently by these campaigns, especially regarding social media, as both populations have increased their digital engagement and use of online services and media platforms.[20] However, young women are disproportionately discouraged by disinformation and are more likely to face barriers to media literacy as compared to male counterparts, which restricts their participation online. Young people, if exposed to disinformation that creates or solidifies pre-existing doubt about the trustworthiness of institutions, may seek alternate sources of information that further undermines their ability to act as informed citizens. Populations with lower rates of information literacy, especially communities that have less access to formal education, may also be vulnerable. Targeted media and information literacy campaigns have the potential to increase certain populations' resilience to digital and traditional disinformation campaigns.

Factors Influencing the Prevalence of Disinformation

There are generally two sets of circumstances under which disinformation may be especially prevalent. One set of circumstances refers to sensitive temporal pressure points, which are times when the integrity of information is extremely vital and the quantity of information shared is higher. These pressure points include elections or referenda, during which crucial citizen-driven decisions shape political futures, such as the 2016 British referendum on membership in the European Union or the 2016 United States presidential elections. The second set of circumstances involves broader structural or circumstantial factors that have an impact on multiple facets of social, economic and political life. For example, sensitive contexts that impact political stability, such as war or prolonged conflict, can create incentives for actors to pollute the information space with disinformation and further undermine citizens' trust in their weakening institutions. High levels of polarization, too, can allow disinformation to flourish by further weakening social ties between people and groups who hold opposing ideological and political views.

Country Examples

Threats to information integrity often manifest differently depending on the context. The following examples illustrate cases of dis-, mis- or malinformation and the impact of these threats on the tenets of democracy.

France

During the 2017 presidential elections, the campaign of then-presidential candidate Emmanuel Macron experienced a cyberattack on its email system. Hackers leaked a large trove of emails belonging to Macron's party, En Marche!, just prior to the implementation of a mandatory media and campaign blackout that banned public discussion.[21] The data leak followed a series of fake stories spread through

social media about Macron's personal life and professional ethics that were designed to discredit his candidacy. The Macron campaign responded by denouncing the hack and casting doubt on the nature of the hack, noting that some of the documents were deliberately forged by the campaign to fool hackers. The leak of this information seemingly had limited impact on the final results of the election, as traditional media coverage was sparse, and media companies formed a network to vet information with the support of FirstDraft, resulting in Macron winning the election.[22]

Kenya

Large populations of young people, who primarily receive information from social media platforms, can experience increased targeting and vulnerability to disinformation shared through online fora. Disinformation campaigns in Kenya designed to stoke lingering ethnic and economic tensions are not new, but social media has made the scope and scale of these disinformation campaigns more acute.[23] During the 2017 presidential elections, young people in Kenya constituted over half of the registered electorate of the country. Many young people took to social media to follow political developments in the country, especially through WhatsApp, Facebook, and Twitter. These social media platforms supplanted traditional sources of information in the country - the government, mainstream media, and civil society - thereby removing the barriers that prevented accurate information and disinformation from freely spreading throughout the media landscape. Some of the disinformation that spread through social media, including false news about party defections, was designed to appear as if it came from credible sources, like CNN, BBC and NTV Kenya.[24] Stories were often designed to discredit specific politicians or create false narratives around certain political parties and actions. This was an attempt to further divide the heavily young electorate and influence their vote in what became a tightly contested and highly controversial race between incumbent President Uhuru Kenyatta and opposition leader Raila Odinga.

Mexico

Disinformation in Mexico is not a new phenomenon; it was historically used by ruling parties to maintain power against opposition parties. However, disinformation in recent contexts has been used to exploit weak trust in institutions, including the government and mainstream media, as a weapon against democracy in Mexico. This weak trust has enhanced vulnerability to disinformation, especially as social media platforms like Facebook and WhatsApp have become the primary source of political news for many citizens. Many disinformation campaigns were detected during the general elections held in July 2018. For example, a false story that was shared 8,000 times from a Facebook page called Amor a Mexico claiming that the wife of Andres Manuel Lopez Obrador, the then-frontrunner who went on to win the presidential election, was the granddaughter of a Nazi.Verificado, a consortium of civil society and media organizations funded by Facebook, Google, and AJ+[25] Español, debunked this story and many others. One of NDI's partner organizations, Animal Politico, participated in this collaborative project that crowdsourced fact-checking efforts from a number of journalists and experts on social media and in political debates.[26]

Myanmar

Disinformation in Myanmar has often been used to influence public opinion about the state of social relations in the country, especially the social status of religious and ethnic minorities. Entrenched discrimination can prevent marginalized communities from participating in civic space, and greater access to and use of technology can exacerbate this discrimination. Prior to the prevalence of internet access in the country, radical groups within Myanmar distributed leaflets and videos containing false information about Muslim communities to increase negative public opinion of these groups. Rapidly

growing access to the internet and social networks has expanded the reach of disinformation in the country and Facebook has become the key means of internet access although some users are unaware that an internet exists outside of the platform. As a result, for many people, Facebook has become the internet itself. In July 2014, false stories on Facebook of a Muslim shop owner raping one of his Buddhist employees led to two days of riots in Mandalay and resulted in the deaths of two people and increased tensions between Muslim and Buddhist communities.[27] A Myanmar court later convicted five people for spreading the false allegations that led to the riots, including a Buddhist woman who admitted that she was paid to file a false complaint with police claiming she had been raped.[28]

Nigeria

A lack of accurate information and transparency has led to a number of disinformation campaigns on social media platforms in Nigeria. Social media sites like Facebook are highly popular in Nigeria, aided by greater access to smartphone technology. These campaigns have been designed to fuel high inter-communal tensions between farmers and herders, which have led to hundreds of deaths. Most notably, in June 2018, graphic pictures circulated through social media platforms appeared to show recent victims of violence in the country. These pictures were later found to have been from other unrelated incidents.[29] News stories on social media have also falsely attributed violence along the Lago-Ibadan Expressway to herdsmen in an attempt to create chaos around the security situation in certain regions, including anonymously fabricating audio and security alerts. Police eventually denied these false reports, which had already spread through social media.[30] In response to disinformation campaigns across the country, the Information Ministry of Nigeria launched a campaign to promote media literacy, which would educate Nigerians about the effects of disinformation on democracy in the country.[31]

Serbia

Disinformation and information manipulation have become common strategies in the Western Balkans, especially targeting Balkan relations with the United States, European Union and the North Atlantic Treaty Organization (NATO). Concerted disinformation campaigns have taken hold in Serbia in recent years and these campaigns are attempting to manipulate public opinion against European peace and security institutions and fuel regional tensions. A report from the Center for Research, Transparency and Accountability (CRTA) in Belgrade found that within the span of one month, approximately one third of media reports about international actors in Serbia did not cite any external sources for their news. The majority of this content promoted pro-Russian and anti-U.S. views.[32] Concerns remain that disinformation campaigns may undermine EU accession efforts, especially if voters begin to turn against the European Union and their own government.

Syria

Civil unrest in Syria created opportunities for foreign and domestic actors to use disinformation to impact public opinion about the war. Notably, in 2016, Russian hackers targeted the White Helmets of Syrian Civil Defense, a non-profit search and rescue organization, accusing them of supporting terrorist organizations.[33] Although fact-checking organizations and investigative journalists found the claims to be false, US-based social media intelligence firm, Graphika, found that the troll accounts reached an estimated 56 million people in 2016 and 2017.[34] The White Helmets were presumably targeted not only for their work in helping save lives, but also for their efforts to document what was taking place in the country. Perpetrators of disinformation, particularly at times of conflict, aim to discredit non-profits and other civil society organizations with the goal of inciting more chaos and confusion.

Ukraine

Pro-Russian online actors have actively promoted disinformation in Ukraine through the use of state-sponsored social media actors. One of the aims of this strategy has been to create doubt around the nature of information and the stability of the state by flooding the public sphere with false content.[35] Operations against the Ukrainian government and media institutions also aim to undermine the country's unity and stability while amplifying growing citizen distrust of the state. During a series of anti-government protests in 2014, alternate narratives about the nature of the protests, fed by foreign actors pretending to be Ukrainian citizens online, spread throughout eastern Ukraine. Disinformation campaigns through social and traditional media outlets suggested that protesters in Kiev supported the persecution of ethnic Russians in the east; these messages were explicitly designed to exacerbate tensions between the ethnically Russian population in the eastern part of the country and the rest of the population. This information warfare has been coupled with crippling cyberattacks on government institutions and infrastructure in the country, which has contributed to citizen perceptions that the government is unable to provide security for its citizens.[36]

United Kingdom

The referendum on the United Kingdom's membership in the European Union (EU) revealed the threat that disinformation poses on democratic principles. Research from the University of Edinburgh found that over 400 Russian-run accounts that participated in discussions during the 2016 U.S. elections were also used to tweet about the vote. The troll accounts attempted to incite fears about Muslims and immigrants in hopes of driving Britons to the polls to vote in favor of leaving EU. In February 2018, Twitter confirmed at a US Senate Foreign Relations Committee hearing that Russian trolls were targeting the Brexit vote. Following foreign interference in the Brexit vote, the UK government created the National Security Communications Unit to combat disinformation by foreign and domestic actors.[37]

The National Democratic Institute is taking a number of actions to protect the integrity of information in democracies, including:

- Conducting research on countries' disinformation vulnerability and resilience.
- Integrating experts into election observation missions to assess the impact of compromised information on elections and working with election monitoring partners.
- Developing tools to detect, analyze, and counter threats to information integrity with partners and looking at ways to share their findings.
- Supporting dialogue between political parties regarding information integrity and strengthening cybersecurity measures.
- Partnering with social media companies and other democracy organizations to protect the integrity of information and promote democratic discourse through the Design for Democracy Coalition.
- Working with civic tech organizations as part of the INFO/tegrity Initiative to increase transparency and improve public trust in institutions.

Acknowledgements

This resource was developed by the National Democratic Institute and was made possible with funding from the National Endowment for Democracy (NED). The opinions expressed herein do not necessarily reflect the views of the NED.

The National Democratic Institute is a nonprofit, nonpartisan, nongovernmental organization working to support and strengthen democratic institutions worldwide through citizen participation, openness and accountability in government. Since its founding in 1983, NDI and its local partners have worked to support and strengthen democratic institutions and practices by strengthening political parties, civic organizations and parliaments, safeguarding elections, and promoting citizen participation, openness and accountability in government. NDI's multinational approach reinforces the message that while there is no single democratic model, certain core principles are shared by all democracies. For more information about NDI, please visit www.ndi.org.

National Democratic Institute
455 Massachusetts Ave, NW - 8th Floor
Washington, DC 20001
www.ndi.org

National Endowment for Democracy
Supporting freedom around the world

Endnotes

1 Claire Wardle and Hossein Derakhshan, "Information Disorder: Towards an Interdisciplinary Framework for Research and Policymaking," published September 27, 2017, https://rm.coe.int/information-disorder-report-november-2017/1680764666, pp. 11-12.

2 Natalie Jomini Stroud et al., "Making Sense of Information and Judging its Credibility," *Understanding and Addressing the Disinformation Ecosystem*, Annenberg School for Communication, published March 2018, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v2.pdf, p. 47.

3 Dean Jackson, "Issue Brief: How Disinformation Impacts Politics and Publics," published October 17, 2017, https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

4 Commission High Level Group on Fake News and Online Disinformation, "A Multi-Dimensional Approach to Disinformation: Report of the Independent High-Level Group on Fake News and Online Disinformation," published 2017, p. 12.

5 Christopher Porter,"FireEye exposed an Iranian disinformation campaign. Not from Silicon Valley but from N. Virginia.", published August 27, 2018. Washington Business Journal. https://www.bizjournals.com/washington/news/2018/08/27/fireeye-exposed-an-iranian-social-media.html.

6 Caroline Jack, *Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute, published August 9, 2017, https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf, p. 2.

7 Theodore Schleifer and Eugene Scott, *"What was in the DNC email leak?"* July 25, 2016. CNN Politics. https://www.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html

8 Dean Jackson, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,'" published October 17, 2017, https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

9 "Propaganda nation: how North Korea spreads its message", published December 20, 2011. The Journal Ireland. http://www.thejournal.ie/propaganda-nation-how-north-korea-spreads-its-message-309343-Dec2011/.

10 Kostas Bithas, Dionysis Latinopoulos, Charalampos Mentis,"The impact of a public information campaign on preferences for marine environmental protection. The case of plastic waste". Marine Pollution Bulletin, Elsevier Journal, 2018.

11 Tim Hwang, *Digital Disinformation: A Primer*, The Atlantic Council, published September 2017, http://www.atlanticcouncil.org/images/Digital_Disinformation_Primer_web_0925.pdf.

12 Caroline Jack, *Lexicon of Lies*, pp. 3-4.

13 Alice Marwick and Rebecca Lewis, *Media Manipulation and Disinformation Online*, Data & Society Research Institute, published May 5, 2017, https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf, p. 26.

14 Nic Dias, "The Era of WhatsApp Propaganda is Upon Us," *Foreign Policy*, published August 17, 2017, https://foreignpolicy.com/2017/08/17/the-era-of-whatsapp-propaganda-is-upon-us/.

15 Samuel C. Woodley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Computational Propaganda Research Project, University of Oxford, published July 11 2017, http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

16 Derek B. Johnson and Susan Miller, "The Dangers of 'Deep Fakes,'" GCN, published July 18, 2018, https://gcn.com/articles/2018/07/18/deep-fakes.aspx.

17 Chris Doten, "In Fight Against Online Disinformation, A Variety of Tools Are Needed," NDI DemocracyWorks, published June 22, 2018, https://www.demworks.org/fight-against-online-disinformation-variety-tools-are-needed.

18 Wu Min Hsuan, "TICTeC 2018: CoFacts, the chatbot that combats misinformation," published May

8, 2018, https://youtu.be/4V2dpdmf8I0.

19 Daniel Funke, "Automated fact-checking has come a long way. But it still faces significant challenges," *Poynter*, published April 4, 2018, https://www.poynter.org/news/automated-fact-checking-has-come-long-way-it-still-faces-significant-challenges.

20 *Mapping of Media Literacy Practices and Actions in EU-28*, European Audiovisual Observatory, p. 29.

21 Amanda Erickson, "Macron's emails got hacked. Here's why French voters won't hear much about them before Sunday's election," *Washington Post*, published May 6, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/05/06/macrons-emails-got-hacked-heres-why-french-voters-wont-hear-much-about-them-before-sundays-election/?utm_term=.be98b12ccd14.

22 Boris Toucas, "The Macron Leaks: The Defeat of Informational Warfare," *Center for Strategic International Studies*, published May 30, 2017, https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare.

23 Tara Susman-Peña and Bebe Santa-Wood, "Kenyans need more than fact-checking tips to resist misinformation," *Columbia Journalism Review*, published October 25, 2017, https://www.cjr.org/innovations/kenya-election-fake-news.php.

24 Nanjira Sambuli, "How Kenya became the latest victim of 'fake news,'" *AlJazeera*, published August 17, 2017, https://www.aljazeera.com/indepth/opinion/2017/08/kenya-latest-victim-fake-news-170816121455181.html.

25 Elizabeth Dwoskin, "Facebook's fight against fake news has gone global. In Mexico, just a handful of vetters are on the front lines," *The Washington Post*, published June 22, 2018, https://www.washingtonpost.com/business/economy/in-mexico-facebook-faces-challenges-as-it-seeks-to-keep-democracy-honest/2018/06/22/098d5f3a-7624-11e8-b4b7-308400242c2e_story.html?utm_term=.0683a7a965df.

26 Daniel Funke, "Journalists and tech companies are teaming up to fight fake news about the Mexican election," *Poynter*, published March 13, 2018, https://www.poynter.org/news/journalists-and-tech-companies-are-teaming-fight-fake-news-about-mexican-election.

27 Samantha Stanley, "Misinformation and Hate Speech in Myanmar," *First Draft News*, published May 16, 2017, https://firstdraftnews.org/misinformation-myanmar/.

28 "Myanmar convicts five over fake rape claim that sparked riots," *Reuters*, published March 20, 2015, https://uk.reuters.com/article/uk-myanmar-conviction-idUKKBN0MG11820150320.

29 "Fake news and Nigeria's herder crisis," *BBC News*, published June 29, 2018, https://www.bbc.com/news/world-africa-44655148.

30 Dimeji Kayode-Adedeji, "No herdsmen attack on Lagos-Ibadan expressway - Police," *Premium Times*, published February 7, 2018, https://www.premiumtimesng.com/news/more-news/257886-no-herdsmen-attack-lagos-ibadan-expressway-police.html.

31 Evelyn Okakwu, "Nigerian govt launches campaign against 'fake news,'" *Premium Times,* published July 11, 2018, https://www.premiumtimesng.com/news/more-news/275846-nigerian-govt-launches-campaign-against-fake-news.html.

32 "Disinformation Analysis on the Western Balkans: Lack of Sources Indicates Potential Disinformation," *EU vs. Disinfo,* published August 3, 2018, https://euvsdisinfo.eu/disinformation-analysis-on-the-western-balkans-lack-of-sources-indicates-potential-disinformation/.

33 Olivia Solon, "How Syria's White Helmets became victims of an online propaganda machine," *The Guardian*, published December 18, 2017, https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

34 "Killing the Truth: How Russia is fueling a disinformation campaign to cover up war crimes in Syria", The Syria Campaign. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf

35 Daniel Arnaudo, *A New Wave of Censorship: Distributed Attacks on Expression and Press Freedom*, Center for International Media Assistance, published May 2018, https://www.cima.ned.org/wp-content/uploads/2018/05/CIMA_A-New-Wave-of-Censorship_web_150ppi.pdf.

36 Julia Summers, "Countering Disinformation: Russia's Infowar in Ukraine," *University of Washington*, published October 25, 2017, https://jsis.washington.edu/news/russia-disinformation-ukraine/.
37 Matt Burgess, "Twitter has admitted Russian trolls targeted the Brexit vote (a little bit)", Wired UK, published February 8, 2018. https://www.wired.co.uk/article/twitter-russia-brexit-fake-news-facebook-russia.