# 2 Theoretical understanding of State-Sponsored Disinformation

*Petros Iosifidis*

## Introduction. Contextualising disinformation

Communication historians claim that the term disinformation dates back to the Cold War era. Discussing Soviet Union disinformation tactics, Shultz and Godson (1984, p. 41) defined disinformation as "false, incomplete or misleading information that is passed, fed, or confirmed to a targeted individual, group, or country". More recently, the European Commission (EC, 2018a, pp. 3–4) defined it as, "verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public and may cause public harm". Disinformation is distinct from propaganda because it is neither based on ideologies nor facts (Chatterjee & Krekó, 2020). One could argue that it is based on twisted facts and what makes it powerful is the mingling of fact with fiction (lies, basically an untruth spoken as if it were truth). Further, when disinformation is shared unintentionally and unsuspiciously, the process is known as misinformation (Fetzer, 2014). In other words, misinformation is the spread of false information, but it is sent or shared without harmful intent. Disinformation, originating from official or unofficial agents, is basically false or misleading information that is intentionally disseminated and can cause chaos, confusion, public harm, as well as serious societal problems when it comes to sensitive socio-political issues such as security, the environment, and health. The widespread conspiracy theories and rumours around vaccines in the midst of the Covid-19 pandemic are a good example of how false or misleading content is purposefully created with the intent to deceive and can therefore be damaging.

Lin et al. (2022) noted that the relationship between such disinformation campaigns and disease spread warrants investigation, particularly in the case of the Covid-19 outbreak. Some governments adopt authoritarian strategies, including disinformation and censorship, to protect against political accountability and criticism over the spread of epidemics. However, the effects of such activities are unclear. In their work, Lin et al. hypothesise that political disinformation may lead to worse public health outcomes. By examining comprehensive data on respiratory infections from 149 countries from 2001 to 2020, this study discovered that government-sponsored disinformation is positively associated with the spread of respiratory infections, including Covid-19. The findings imply that

DOI: 10.4324/9781032632940-3

governments may contain the damage associated with pandemics by ending their sponsorship of disinformation campaigns.

It has now been some time since the World Health Organization (WHO) announced that, together with the health pandemic, it was also addressing an "infodemic", that is, an "overabundance of information, both online and offline" (WHO Director General, 2020). Even in the present day, the "infodemic" continues to undermine trust in vaccination efforts aiming to bring an end to the pandemic. In addition, disinformation is as much a weapon of war as bombs are. Budgar (2022) reminds us that in the ongoing Ukraine-Russia war, disinformation is particularly widespread and provides the example of the circulation of a video by Russia claiming Ukrainian casualties were fake news—just a bunch of mannequins dressed up as corpses. The video, originating on a Russian TV set, was an attempt to cast doubt on Ukrainian losses. Budgar (2022) goes on to say that, as the war continues, new techniques are being developed, such as the rise of fact-checkers (see more details on this in the below section on measures to combat disinformation). In Russia, fact-checkers were reporting and debunking videos supposedly going viral in Ukraine, but the videos were never circulated in Ukraine, meaning that the fact-checking itself was another disinformation campaign.

Disinformation is not merely motivated by the desire to create confusion among the citizenry, but also by political power or influence. Bennett and Livingston (2018, p. 124) define disinformation as "intentional falsehoods spread as news stories or simulated documentary formats to advance political goals". This has become more apparent in the digital, information society era. Whereas in the past the activity of disinformation agents was restricted because of the limited potential of analogue, linear media technologies, Chadwick (2013) considers how social media have been incorporated into mainstream political communication strategies. In this context, disinformation for the purposes of creating confusion or political motivations in the social media era is notably easier to spread and undeniably more threatening. Several news media companies today rely on social media to drive traffic to their own websites by frequently sharing clickable news stories there. But while social media are ideal for agents to disseminate deviant content, they are consequently becoming the most prominent forerunners of our current epistemic crisis (Napoli, 2019). Deviant agents build websites that imitate trusted news media publishers in order to lure users via social media posts. The approach is an effective means for disinformation agents to influence the political perceptions of unaware users.

A striking example here is the 2016 Brexit referendum that was largely based on post-truth politics. In the 2016 UK referendum, social media became a vehicle for contested political arguments, and post-truth positions defined the Remain and Leave camps. For instance, it was claimed that the UK Independence Party former leader Nigel Farage's anti-migrant tweets influenced many voters. Also, in the 2016 US presidential election, the victorious celebrity property tycoon

Donald Trump maintained a controversial online presence. He posted tweets about his campaign and engaged in a blatantly hateful online discourse aimed at his political opponents (Iosifidis & Wheeler, 2018). Distrust in political information has forced people to look inwards, giving rise to new forms of nationalism and populism (Flew & Iosifidis, 2020).

Nationalism (the idea that nations are better off acting independently than collectively) and populism (a philosophy directed to the needs of the common people and advocating a more equitable distribution of wealth and power) have challenged the globalisation trend. The rise of both these doctrines has had a negative effect on citizens' trust in their governments and contributed to the weakening of representative democracy (Flew & Iosifidis, 2020). The above definition of populism mainly applies to certain left-wing forms of the phenomenon but contrasts sharply with right-wing forms like the Trump movement in the US and Brexit. Trump's campaign to further isolate America by blocking southern immigration, Brexiteers' xenophobic ideas, as well as the tendency for citizens to vote for extreme parties in EU countries like France, Germany, Denmark, Greece, Spain, and Finland, are illustrations of the rise of nationalism and populism in recent years.

## Growth of platforms and self-regulation

Many democratic states around the globe have imposed legal frameworks to prevent disinformation, with measures primarily addressed to technology companies. Digital platforms consist of applications and services that allow users to interact with each other. Together, they impact the commerce, communication, entertainment, and finance of billions of people. The rapid growth of Alphabet (Google), Amazon, Apple, Meta (which also owns Instagram and WhatsApp), and Microsoft platforms has prompted policymakers to rethink the governance and regulation of the digital economy sector. All these companies increased their profits during Covid-19 as most people were confined indoors and used their services to communicate and exchange information. Their combined market capitalisation is approximately 6 trillion US dollars, a figure larger than the Gross Domestic Product (GDP) of most global economies (Companies Market Cap, 2022). Despite a minor post-pandemic setback, all hold dominant positions within the economy (Aral, 2020; Waters, 2021). Economic concerns over market dominance and the elimination of competition, as well as socio-cultural concerns relating to harmful content and the spread of disinformation, have prompted governments to impose legal restrictions.

Digital platforms such as Facebook (renamed Meta) and Twitter have lately stepped in themselves to take down content that is false or misleading, including the setting up of the Facebook Oversight Board and the banning of the Twitter account of former US President Donald Trump following the Capitol Hill atrocities. The Oversight Board (OB) was created to help the giant online platform

assess questions relating to freedom of speech; in other words, to decide what content to take down, what to leave up, and why. The OB, whose decisions are binding, consists of 40 members from across the globe, empowered to select content cases for review and to uphold or reverse Meta's content decisions. Meta has been struggling to address moderation regarding issues of violations of the privacy of users, the dissemination of unlawful and harmful content, and the political manipulation of selected groups of users, particularly in non-English-speaking regions (Wijeratne, 2020), for instance, the regulation of Spanish-language disinformation concerning Covid-19 (Paul, 2021). These problems have also been experienced by other platforms as automated, algorithmic tools have proven unable to detect illegal, harmful or misleading content. Such problems provided the rationale for establishing the OB.

The initiative is certainly a positive step to deal with the above issues, but according to Neuvonen and Sirkkunen (2022), it falls short of becoming a real "supreme court" of the online platform, for it cannot process enough cases, relies on idiosyncratic standards instead of general rules and principles, and has problems deciding which human rights principles to follow. In another case of self-regulation, Twitter was among the first online platforms to ban former US President Donald Trump's account after the January 6, 2021 attack on the US Capitol by his supporters. The then-owners of the platform said that Twitter permanently suspended Trump because of the risk of further incitement following the storming of the Capitol in Washington. The former US President used Twitter, as well as other social network sites, to falsely claim there had been widespread voter fraud and had urged his supporters to march on the Capitol to protest. But in November 2022, Elon Musk, the richest man on earth and new owner of Twitter, announced the reactivation of Trump's account. Alongside the decision by Twitter, as of November 30, 2022, to no longer enforce its policy on Covid misinformation (a five-strike system that took action against accounts posting 'demonstrating false or misleading' content), Musk's announcement is certainly a step back. True, it is imperative to guarantee freedom of expression, independent global public spheres, and open civil society, but an individual's freedom of speech should stop at the point where it causes harm to another person or society (Iosifidis, 2022)

Social media platforms should continue proactively tackling disinformation aimed at undermining trusted and accurate content that can negatively influence democratic processes such as elections. This will help ease people's concerns about the threat that malicious state-linked fake news poses to society and democracy. Implementing rigorous self-regulation is also likely to prevent the state from intervening and legally enforcing digital platforms to take down harmful and misleading content. Further, taking proactive, preventative action to identify and minimise citizens' exposure to disinformation will increase people's trust in online platforms. As Chatterjee and Krekó (2020) claim, in the absence of reliable, clear information, people may revert to tribalism based on the narrative they agree with, thereby deepening cleavages.

## Legal measures in selected countries and the EU

Since disinformation concerns are not always sufficiently addressed by self-regulation, several states and regional bodies like the EU have stepped in and imposed policy provisions. The Online Safety Bill in the UK, introduced in 2021 and updated on January 18, 2023, applies new rules for firms that host user-generated content (those that allow users to post their own content online or interact with each other), and for search engines, which will have tailored duties focussed on minimising the presentation of harmful search results to users. All platforms in scope will need to tackle and remove illegal material online, particularly material relating to terrorism, child sexual exploitation and abuse, as well as disinformation. In France, the 1881 law from 2018 outlaws the dissemination of '"false news" and the spread of misinformation. The legislation is mainly designed to enact strict rules on the media during electoral campaigns and as such it gives authorities the power to remove fake content spread via social media and even block the sites that publish it. In the US, the Countering Foreign Propaganda and Disinformation Act, dated May 10, 2016, is the main legal measure to combat false information.

Turning to the EU initiatives, in December 2020 the EC proposed an *ex-ante* regulatory regime known as the Digital Services Act Package that specifically targets gatekeepers in the digital economy sector. The package is divided into the Digital Markets Act (DMA) whichcomplements and updates existing competition policy, and the Digital Services Act (DSA), revising the 2000 E-Commerce Directive. Disinformation and content moderation concerns require gatekeepers to do their due diligence in identifying it and taking it down. Ultimately, both democracy and free speech concerns (the DSA) and economic and consumer welfare concerns (DMA) are addressed. Alongside the DSA and DMA, there exists the 2022 Strengthened Code of Practice on Disinformation, building on the pioneering 2018 Code while setting more ambitious commitments and measures aimed at countering online disinformation. The new Code brings together a more diverse range of stakeholders than ever, empowering them to contribute to wide-ranging improvements by signing up to precise commitments relevant to their field. Such commitments include demonetising the dissemination of disinformation; guaranteeing transparency of political advertising; enhancing cooperation with fact-checkers; and facilitating researchers' access to data. It is important that both the DMA/DSA and the Code accomplish their goals in regulating digital platforms since as regulatory forerunners, other regions of the world will create copycat legislations.

## Use of new technologies in the fight against disinformation

### *Fact-checking*

The process of fact-checking is one of the most effective means of detecting digital disinformation (Guarino et al., 2020). Fact-checking concerns the

correctness of factual statements and can be divided into human-based and automated systems of artificial intelligence (AI) and machine learning (Nguyen & Kyumin, 2019). Journalistic fact-checking in the past century or so may have allowed news outlets to become trusted sources of information and, meanwhile, keep citizens objectively informed. It has to be said, though, that fact-checking has expanded at a time when trust in journalists, and especially social media, is declining, and it is not clear that it actually has the effect of reversing that decline. As news media have become more intertwined with digital tools and social media platforms, fact-checking processes have shifted toward a detection rather than a prevention mechanism. When it comes to online platforms, it is mainly the share option, introduced by Facebook/Meta a couple of years following its launch, as well as the retweet option on Twitter, that enabled agents to take digital disinformation to the next level since users could now unintentionally or intentionally spread deceitful news.

The meddling of the US elections and the Brexit referendum in 2016 demonstrated the dangers to democracy associated with the share option. Both the US presidential elections and the UK's decision to leave the EU through a voting referendum left many observers puzzled by the outcomes. Those 2016 shockwaves, combined with the 2018 Cambridge Analytica/SCL scandal, eventually prompted Facebook/Meta to increase its post-published digital fact-checking detection process. The social media giant began outsourcing the services of independent fact-checkers to flag and analyse disinformation, and today there are more than 80 fact-checking organisations working with Facebook. It should be noted, though, that the direct defence mechanism of fact-checking the huge digital ecosystem comes with numerous difficulties and there are doubts over its effectiveness as it might not be enough to undo the damage an untrue story has already done to democracy. Fact-checking may not be effective in changing pre-shaped perceptions, and it might not be shared back with all interpreters of the initial disinformation.

### *Artificial intelligence (AI)*

According to the European Parliamentary Research Service study on AI (EPRS, 2019, p. 12), "Artificial Intelligence refers to advanced forms of machine learning, generally classified as algorithmic processes powered by advanced computing techniques such as neural networks and including in particular Deep Learning". Platforms such as Facebook/Meta and Twitter have for several years now begun to adopt AI and machine learning to combat disinformation. Facebook, alongside hiring thousands to identify hateful or offensive content, has also invested heavily in AI and machine learning to identify disinformation (Iosifidis & Nicoli, 2020; Woolley, 2020). Tools that have been used by social media to detect bad content include Deeptext, a software that is a deep learning-based text understanding engine that can understand with near-human accuracy

the textual content of several thousand posts per second, spanning more than 20 languages (Abdulkader et al., 2016). Other companies such as Google have used similar AI tools to detect disinformation. Meanwhile, social media companies—driven by profits and shareholder pressures—will want to patent and protect their innovations rather than share them with others, so the advantage of disinformation agents seems destined to endure. This has also been the conclusive result of a large-scale European Parliament study on the use of AI in combating disinformation (EPRS, 2019).

***Blockchain***

Another promising technology in the fight against digital disinformation (one that essentially overlaps with AI) is blockchain. This technology enables the encryption and decentralisation of data that is timestamped and cannot be manipulated. The decentralised nature of the technology undoubtedly plays a major role in disrupting big industries, firms, institutions, and individuals. Tapscott and Tapscott (2016) claim that despite the promise of flatter organisations in the twenty-first century, most firms are still hierarchical in nature and that blockchain will disrupt organisational structures to the extent that many will become vastly flatter. Blockchain uses cryptographic techniques to create a secure, decentralised ledger that records transactions in a way that is transparent, verifiable, and resistant to tampering (https://fact.technology/learn/blockchain-technology-to-combat-fake-news/). The decentralised nature of blockchain can disrupt the information ecosystem, as a decentralised approach to news dissemination means that priority can be placed on the content. A blockchain news story travelling from one user to another will serve everyone's interest, as no single party can control it. Blockchain in news media, therefore, has the potential to be a game changer, since the content in the information ecosystem that works on a decentralised blockchain network can be officially verified (Dickson, 2017). As a tool for sales teams, blockchain-based registries can rank and filter trusted advertisers and ad content. But when the content is vague, divisive, or personal, for example, with political opinion pieces, the affordances of blockchain might not be enough to keep people from sharing content as their motivations might be a priori deceitful. If a supporter of a serving government wants to gather more support for that government, they might be more inclined to share a fake story despite knowing it is fake. And it is precisely in such occurrences that social media platforms can take more decisive action; once disinformation is identified from the source, they should be more inclined to take it down before it spreads.

***Media and news literacy***

In the context of a concerted and continuous effort to stifle disinformation and facilitate a digital democracy that supports the public interest, one can include media and news literacy across all ages and demographic standings. The

National Association of Media Literacy Education defines media literacy as "the ability to access, analyse, evaluate, create, and act using all forms of communication" (2019, para. 1). The EU regards digital literacy as one of the most crucial skills of the twenty-first century in fighting back against digital disinformation and has come up with several policy recommendations in support of digital literacy programmes. The HLEG report (EC, 2018b, p. 25) states that "media and information literacy is acquiring a strategic importance for digital citizenship as basic educational competences were for citizens of the industrial age". It recommends integrating media literacies within national schools, training teachers, and engaging with libraries and fact-checkers. It further supports such programmes for all ages, which again is imperative in covering ground on the digital divide. Within this context, the Audiovisual Media Services Directive (AVMSD) reiterates the value of acquiring knowledge to use and create media content responsibly and safely.

News literacy is currently the most significant subcategory of media literacy (Richter, 2019). It comprises three dimensions: access and use; critical understanding; and participation and production processes (ibid, p. 319). By increasing news literacy, citizens will eventually become more news literate, capable of identifying trustworthy news and information channels. Social science disciplines, such as communication studies, cultural studies, political economy of communication, film studies, journalism studies, etc. have several years of practice and understanding of news literacy to draw from, allowing us to acquire an understanding of the ways in which ideologies drive content, how production and distribution mechanisms work, and how we understand visual storytelling. The intersection of digital disinformation and news literacy, including updated digital literacy curricula, concerns identifying, detecting, and understanding dubious information, which is crucial to digital democracy. Therefore, efforts to defend ourselves against digital disinformation in the areas of digital use, safety, rights, security, and literacy need to be intensified.

### *National regulatory bodies and EU policies*

National political and regulatory actions play a key role in shaping responses to disinformation. Many governments have responded to disinformation by passing rulings or updating existing laws related to disinformation. Such legislation ranges from media and electoral laws to cybersecurity and penal codes (Bontcheva & Posetti, 2020). Measures to protect the integrity of electoral processes from online disinformation and to ensure the transparency of online political advertising are good examples of such legislation. These include the French law on false information and non-binding guidelines passed by the Italian government (EC, 2018a). France, for instance, introduced laws to improve tech platforms' transparency on political advertising, requiring social media companies to create ad repositories. The French legislation enables its broadcasting agency

to suspend or terminate broadcasters under the influence of foreign states if they spread false information likely to undermine electoral integrity.

At an EU level, the current thinking is that disinformation erodes trust in institutions and in digital and traditional media, and harms democracies by hampering the ability of citizens to make informed decisions. Disinformation also often supports radical and extremist ideas and activities. In that sense, it impairs freedom of expression, media freedom, and pluralism, as well as the right of citizens to hold impartial opinions. As the European Court of Human Rights has concluded, this is particularly important in relation to elections. The EU approach to addressing online disinformation includes: a. improving transparency regarding the origin of information and the way it is produced, sponsored, disseminated, and targeted in order to enable citizens to assess the content they access online and to reveal possible attempts to manipulate opinion; b. promoting diversity of information, in order to enable citizens to make informed decisions based on critical thinking; c. fostering credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers; and d. fashioning inclusive solutions that require awareness-raising and more media literacy (EC, 2018a). More recently, the EU's goal has been to encourage debate and offer concrete ideas about addressing the problem, particularly considering the updated EU Code of Practice on Disinformation and the Digital Services Act.

***Official disinformation in authoritarian regimes***

So far, discussion on disinformation from official actors has mainly focused on the information warfare effort from authoritarian regimes like China to manipulate users in other countries. Myers and Mozur (2019, p. 5) argued that China is employing techniques to paint Hong Kong's democracy advocates as violent radicals. More specifically, in late June 2019, there were popular demonstration movements in Hong Kong asking for the territory's independence from mainland China. Chinese officials, who have lately stirred up more aggressively nationalist and anti-Western sentiment using state media (whose history of propagandising stretches back to Mao Zedong's era) and social media outlets, have manipulated the context of images and videos to undermine the protesters and begun branding them as terrorists, consisting of small violent gangs lacking popular support. Myers and Mozur claim that the assertion was more than just a spin of fake news, for the Communist Party exerts overwhelming control over media content inside China's Great Firewall (the combination of legislative actions and technologies enforced by the People's Republic of China to regulate the Internet), and it is now using it as a cudgel in an information war over the protests that have convulsed Hong Kong for months. The result, according to the commentators, is the creation of an alternative version of what was clearly a

popular demonstration calling for Hong Kong's independence in both mainland China and abroad.

Lu (2022) examined the nuanced practices of Chinese state-sponsored disinformation campaigns as participatory digital warfare and proposed analysing disinformation beyond the framework of political communication. Through examples and cases, the author demonstrated that disinformation campaigns strategically utilise suggestive half-lies to mobilise alliances and silence enemies regardless of their nationalities. Depending on whether they conform to the Party agenda, some foreign actors can be enlisted as allies, while critical citizens are portrayed as enemies. Overall, the work argued that Chinese state-sponsored disinformation campaigns can stealthily recruit netizens to combat in an ongoing state-making project that potentially consolidates the authoritarian Party-state. Addressing the gap between Chinese traditional war philosophies and contemporary, technologically informed practices, the author pointed out the significance of participatory and cultural countermeasures.

This is also an illustration of how authoritarian governments that were once hailed as harbingers of democratic ideals have weaponised social media. One only has to recall the Arab Spring, namely a series of pro-democracy, anti-government protests and massive uprisings ignited by social media, that spread across much of the Arab world (including countries like Tunisia, Morocco, Syria, Libya, Egypt, and Bahrain) in the early 2010s and the spring of 2011. Regrettably, many of the countries that experienced uprisings have returned to authoritarian rule as the respective leaderships used social media to spread their disinformation campaigns.

Focusing on the Middle East, Kenney and Bernadaux (2021) note that disinformation, while a global phenomenon, is particularly prevalent in the region, and there has been a rich history of fake news wielded as an offensive weapon by a wide range of stakeholders. The authors go on to say that non-state armed groups have been prolific in disseminating disinformation and provide the case of Hezbollah, which has gone so far as to set up disinformation training camps, attracting Iran-based militias, especially from Iraq. Citing a May 2020 detailed report from Omelas on the first few months of the Covid-19 information operations, the authors claim that "national governments of Middle East states are no bystanders to the disinformation onslaught" and list the example of the Emirati government, which has quoted fictitious Middle East specialists to support their anti-Qatar propaganda. Fake news, according to the authors, has long contributed to creating tensions that endanger fragile internal balances and international relationships in the region. In Iran, the Islamic Revolutionary Guard regularly resorts to state-run media for disinformation campaigns. Platforms such as Fars News, the hardliner Tasnim News Agency (the semi-official news agency in Iran), and the English-speaking channel Press TV (Iranian news and documentary network) regularly spin American and European commentators as expressing support for Iran's policies.

The health pandemic provided an opportunity for other governments in the region to advance misleading information that could serve their interests. Fabricated news concerning Covid-19 was used both as a defensive and offensive weapon. Kenney and Bernadaux (2021) argue that, since the outbreak of coronavirus, some Middle Eastern states, often through state-run media outlets, have "dishonestly extolled the efficacy of their responses to the crisis". In Egypt, media falsehoods took the form of alleged praise from Italy thanking the generous Egyptian government for sending medical help. In Palestine, some news sites reported that Israeli TV had admitted that Gaza's health officials have better handled the epidemic than the Tel Aviv regime. In Syria, pro-government activists advanced the claim online that Bashar Al-Assad is personally searching for a cure to the virus in a Damascus laboratory. According to the authors, all this fake news promoted by media outlets, widely followed social media accounts, and government figures share the same objective, namely to mask their mismanagement of the crisis.

Turning to Russia, its authoritarian president, Vladimir Putin, has for a couple of decades been employing digital disinformation tactics to create disruption in liberal democracies of the Western world. Russian digital disinformation and its hybrid threat strategies are still not completely understood and therefore not all can be identified (Iosifidis & Nicoli, 2021). For instance, the Russian troll factory, the Internet Research Agency, is a well-known entity that has been assessed and monitored for several years. Yet others are only now being discovered. A report conducted by Graphika in 2020 identified a troll factory known as Secondary Infektion that began operations in 2014 and has posted over 2,500 pieces of content online (Nimmo et al., 2020), most of which did not manage to gain significant online traction (although the entity did obviously succeed in covering its tracks). In addition, the Russian military intelligence arm, the General Staff Main Intelligence Directorate (GRU), has also been identified as a major disinformation hub.

In Europe, Russia's objectives include destabilising the region, preserving close ties with the Balkan States, and impeding Ukrainian and EU relations. Russia, which has already been among the world's top ten most targeted countries with cyberattacks and disinformation campaigns following the annexation of Crimea and Eastern Ukraine in 2014, is currently targeting Ukrainian infrastructure with a massive disinformation campaign to shape the war narrative (Gavin, 2022). Between 2020 and 2021, Russia has initiated over 685,000 cyberattacks in Ukraine, and currently, as a result, Ukraine is defending itself on two fronts: territorially and the cyber sphere. Certainly, on the Russian side, as Gavin notes, a tightly controlled state-run media and the substantial use of disinformation, both from official state sources and online via bots, have helped the state exert narrative control over the conflict. This explains, in part, the low levels of opposition to the invasion within Russia (Gavin, 2022).

Across the Atlantic, an example of political and ideological motivations behind sophisticated and well-funded official agents includes the accusation

that the Russian government interference in the 2016 US presidential election boosted the candidacy of Donald Trump. An investigation known as the Report on the Investigation into Russian Interference in the 2016 Presidential Election was conducted and submitted into record in March 2019. The report, known for short as The Mueller Report, did not establish any criminal conspiracy between Moscow and the Trump campaign (BBC, 2019). Attorney General William Barr noted a lack of evidence regarding American and Russian connections in the interference. Nonetheless, the report did stress that Russian illegal interference did occur "in sweeping and systematic fashion" (Mueller, 2019, p. 1). Volume I of the report mentions Russia's involvement in interfering in Facebook and Twitter through the use of individualised accounts and botnet activities.

## Disinformation in Western democratic countries

Chatterjee and Krekó (2020) argue that, while democratic leaders have so far opposed authoritarians who deliberately deceived their citizens to create a virtual reality, "suddenly, state-sponsored disinformation is no longer reserved for authoritarians and dictators. It has infiltrated the Western democratic world, catching us all off guard". They go on to say that "state-sponsored disinformation in Western democracies is the elephant in the room" and that we must now recognise the painful truth that, even in a Western democracy, disinformation is difficult to stop, particularly when it comes from the political elite. In fact, democratically-elected leaders are increasingly accused of fuelling the spread of disinformation by confusing the public with multiple messages without clear and reliable information based on hard facts.

Since 2010, Hungarian Prime Minister Viktor Orbán has created a highly centralised media empire with most media outlets conveying similar political messages and narratives favourable to the governing elite (e.g., the blaming of George Soros for the devaluation of the Hungarian currency and the false argument that the primary source of the pandemic is illegal migration). Other Central European governments like Romania and Bulgaria, also EU member states like the Central European government of Hungary, are adopting disinformation tactics related to vaccination in the post-pandemic era that have resulted in extremely low vaccination rates in the respective countries and eventually many deaths. In Poland, state-owned media have been reporting that opposition mayors have implemented policies that are facilitating the spread of the virus (Chatterjee & Krekó, 2020). Obviously, these examples pertain to transitional democracies (or post-authoritarian or non-consolidated ones) with long-held traditions of disinformation in the Soviet era, which now resurface.

Yet, it is not merely Central European territories that have employed such tactics. In the 2019 general election campaign in the UK, the incumbent Tories deployed a flood of fake news regarding Brexit and their political opponents until tech giants had to step in and remove some of their misleading ads. Earlier,

the EU Referendum which led to the Brexit decision in 2016 was accompanied by a populist online narrative. The social media echo chamber tended to reinforce the anti-European rhetoric within the mainstream media, led by a chorus of Brexit-led newspapers and Leave campaigners. Across social media, anti-immigrant sentiment was fuelled by the view that a dysfunctional European elite was bent on undermining Britain's economy, sovereignty, and self-confidence. This led to xenophobic falsehoods claiming that a Vote Leave outcome would Canute-like turn back the "waves" of immigrants who were ready to pounce from Eastern Europe and the Syrian refugee crisis (Iosifidis & Wheeler, 2018).

As said above, in the US, the Republican Presidential victor Donald Trump utilised social media to reach out to a disaffected electoral base to win the 2016 Presidential election against Democratic nominee Hillary Clinton. The highly controversial Trump, who had established his media capital as a property tycoon and television celebrity on The Apprentice (from 2004 onwards), developed his online presence through Twitter, where he regularly posted comments about his campaign, other candidates, political views, and the "rigged" mainstream media coverage. Trump was notorious for his negative, aggressive, and sometimes blatantly hateful tweets, in which he routinely called his opponents, political and otherwise, "losers" and "haters". For many, the Trump campaign was accompanied by the rise of "fake news" via close advisor Steve Bannon's online Breitbart News, information provocateurs, and "post-truth" politics. It has been unfortunate that one of the greater democracies such as the US has been associated with the rise of fake news and disinformation campaigns.

## An afterword

It is clear then that state-backed disinformation is not exclusively confined to authoritarian and autocratic states, for it has exacerbated in Western liberal democracies. How can this new challenge be tackled? Because such extensive disinformation campaigns are a relatively new phenomenon in the West, there are no institutions ready to deal with domestic, homegrown, politically charged disinformation. We need to develop and test an analytical approach and assessment tool to monitor changes in the level of strategy-driven, state-sponsored disinformation activities. The pace of these issues has produced some excellent research work that is being undertaken, both through conventional academic routes, think tanks, and others. The sources cited throughout this chapter suggest that fact-checking and news literacy can be identified as the main detection mechanisms involved in combating digital disinformation. Responses toward digital disinformation involve communication strategies consisting mainly of debunking, rebuttals, and myth-busting but also of technologies used, such as AI and blockchain. Corporate voluntary actions to mitigate and counter disinformation, such as the employment of content moderators to detect and take down misleading content, are crucial. The initiative of Meta to set up the Oversight

Board to promote free expression by making independent decisions regarding content on Facebook and Instagram and by issuing recommendations on content policy should be applauded, despite its limitations.

I would stress here the key role of civil society in combating disinformation. Civic groups are more closely connected to citizens and are better placed to identify the negative disinformation impact on society, and, meanwhile, better equipped to build trust with local communities—a key factor in responding to specific information disorders—and are more likely to be perceived by all parties as relatively objective. More specifically, civic associations promote the cooperation of citizens from distinct interest and identity groups, such as females, ethnic minorities, and groups with protected characteristics like the disabled community. Civil organisations and coalitions are often best placed to identify disinformation campaigns that target marginalised groups and mobilise broad opposition and responses to these campaigns. (https://counteringdisinformation.org/topics/csos/complete-document-civil-society).

But more thinking is required to develop a workable analytical approach. Whereas there is certainly an international academic network interested in policy issues, platform overseeing, and disinformation, it is small relative to the size of the research community as a whole, and few of its members are in a position even minimally to affect debate. What I suggest is that potential fighting back mechanisms could be applied (and turn more impactful) by a combined effort by academics, journalists, technology platforms, taskforces, civil society, and regulatory bodies. This is a moment for research, but also for activism.

## References

Abdulkader, A., Lakshmiratan, A., & Zhang, J. (2016, June 1). Introducing deeptext: Facebook's text understanding engine. *Facebook Engineering*. https://enginee ring.fb.com/core-data/introducing-deeptext-facebook-s-text-understanding-en gine/

Aral, S. (2020). *The hype machine: How social media disrupts our elections, our economy, and our health – and how we must adapt*. Harper Collins.

BBC. (2019, October 25). Mueller report: Criminal probe into Russia inquiry begins. *BBC News*. https://www.bbc.com/news/world-us-canada-50178197

Bennett, L. W., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139.

Bontcheva, K., & Posetti, J. (Eds.). (2020). *Balancing act: Countering digital disinformation while respecting freedom of expression*. UNESCO Broadband Commission Report.

Budgar, L. (2022, November 8). Misinformation vs. disinformation: How to tell the difference. *Reader's Digest*. https://www.rd.com/article/misinformation-vs-disinformation/

Chadwick, A. (2013). *The hybrid media system: Power and politics*. Oxford University Press.

Chatterjee, S., & Krekó, P. (2020, July 10). State-sponsored disinformation in Western democracies is the elephant in the room. *Euronews.* https://www.euronews.com/2020/07/06/state-sponsored-disinformation-in-western-democracies-is-the-elephant-in-the-room-view

Companies Market Cap. (2022). Largest companies by market cap. *Companies Market Cap*. https://companiesmarketcap.com

Dickson, B. (2017, August 24). How blockchain helps fight fake news and filter bubbles. *The Next Web*. https://thenextweb.com/news/blockchain-helps-fight-fake-news-filter-bubbles/

EC. (2018a). *European commission, tackling online disinformation: A European approach.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

EC. (2018b). *European commission, a multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation*. European Commission.

EPRS. (2019, March). Automated tackling of disinformation. *European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

Fetzer, J. H. (2014). Disinformation: The use of false information. *Minds and Machines*, *14*(2), 231–240.

Flew, T., & Iosifidis, P. (2020). Populism, globalisation and social media. *International Communication Gazette*, *82*(1), 7–25. doi:10.1177/1748048519880721

Gavin, J. (2022). *Information and misinformation in the Russia Ukraine War*. https://www.visionofhumanity.org/information-and-misinformation-in-the-russia-ukraine-war/

Guarino, S., et al. (2020). Beyond fact-checking: Network analysis tools for monitoring disinformation in social media. In H. Cherifi et al. (Eds.), *Complex networks and their applications VIII. COMPLEX NETWORKS 2019. Studies in computational intelligence* (Vol. 881, pp. 436–447). Springer.

Iosifidis, P. (2022, December 1). Here's what Elon Musk's language teaches about his ambitions. *The Conversation*. https://theconversation.com/heres-what-elon-musks-language-teaches-us-about-his-ambitions-195144

Iosifidis, P., & Nicoli, N. (2020). The battle to end fake news: A qualitative content analysis of Facebook announcements on how it combats disinformation. *International Communication Gazette*, *82*(1), 60–81.

Iosifidis, P., & Nicoli, N. (2021). *Digital democracy social media and disinformation.* Routledge.

Iosifidis, P., & Wheeler, M. (2018). Modern political communication and web 2.0 in representative democracies. *Javnost - The Public*, *25*(1–2), 110–118. doi:10.1080/13183222.2018.1418962

Kenney, S., & Bernadaux, C. (2021, January 13). New ways of fighting state-sponsored Covid disinformation. *Mei@75 Piece, Prosperity, Partnership*. https://www.mei.edu/publications/new-ways-fighting-state-sponsored-covid-disinformation

Lin, T.-H., et al. (2022). Government-sponsored disinformation and the severity of respiratory infection epidemics including COVID-19: A global analysis, 2001–2020. *National Library of Medicine*. doi:10.1016/j.socscimed.2022.114744

Lu, I. F. (2022). To subdue the enemies without fighting: Chinese state-sponsored disinformation as digital warfare. *Digi War, 3*, 96–106. https://doi.org/10.1057/s42984-022-00052-7

Myers, S. L., & Mozur, P. (2019). *China is waging a disinformation war against Hong Kong protestors*. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html

Napoli, P. M. (2019). *Social media and the public interest: Media regulation in the disinformation age*. Columbia University Press.

National Association for Media Literacy Education. (2019). Media literacy defined. *NAMLE*. https://namle.net/resources/media-literacy-defined

Neuvonen, R., & Sirkkunen, E. (2022, October). Outsourced justice: The case of the Facebook oversight board. *Journal of Digital Media & Policy*, *12*. https://doi.org/10.1386/jdmp_00108_1

Nguyen, V., & Kyumin, L. (2019, July 21–25). Learning from fact-checkers: Analysis and generation of fact-checking language. *Sigir*.

Nimmo, B., et al. (2020, June 16). Secondary infektion. *Graphika*. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

Paul, K. (2021, March 16). Facebook must tackle 'Spanish-language disinformation crisis', lawmakers say. *The Guardian*. https://www.theguardian.com/technology/2021/mar/16/facebook-spanish-language-disinformation-congress

Richter, A. (2019). Accountability and media literacy mechanisms as counteraction to disinformation in Europe. *Journal of Digital Media & Policy*, *30*(3), 311–327.

Shultz, R., & Goodson, R. (1984). *Dezinformatsia: Active measures in soviet strategy*. Pergamon Press.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business and the world*. Random House.

Wijeratne, W. (2020, July 23). Facebook, language, and the difficulty of moderating hate speech. *LSE Blog*. https://blogs.lse.ac.uk/medialse/2020/07/23/facebook-language-and-the-difficulty-of-moderating-hate-speech

Waters, R. (2021, April 30). Big tech's surging growth stuns wall street. *The Financial Times*. https://www.ft.com/content/42c5f1d6-36e5-4117-b30e-635c85c6a55c

WHO Director General. (2020, February 15). *Munich security conference speech*. Retrieved February 15, 2020, from http://www.who.int/director-general/speeches/detail/munich-security-conference

Woolley, S. (2020). *The reality game: How the next wave of technology will break the truth and what we can do about it*. Endevour.