87
2020

Democracy vs. Disinformation

Proposals for Protecting Open Societies

Junta de Andalucía
Consejería de la Presidencia,
Administración Pública e Interior
CENTRO DE ESTUDIOS ANDALUCES

Andalucía
ORIGEN & DESTINO
Quinto Centenario de la Primera Vuelta al Mundo

CENTRE FOR ANDALUSIAN STUDIES FOUNDATION IS A NON-PROFIT SCIENTIFIC AND CULTURAL INSTITUTION ATTACHED TO THE REGIONAL MINISTRY OF THE PRESIDENCY, PUBLIC ADMINISTRATION AND THE INTERIOR OF ANDALUSIA. THE FOUNDATION WAS CREATED FOR THE PURPOSE OF PROMOTING SCIENTIFIC RESEARCH, GENERATING KNOWLEDGE ABOUT THE SOCIAL, ECONOMIC AND CULTURAL REALITY OF ANDALUSIA, AND SHARING ITS FINDINGS TO BENEFIT SOCIETY AS A WHOLE.

OUR COMMITMENT TO THE ADVANCEMENT OF ANDALUSIA INSPIRES US TO CREATE OPPORTUNITIES FOR SHARING KNOWLEDGE WITH THE SCIENTIFIC AND ACADEMIC COMMUNITY AND WITH ALL CITIZENS, AS WELL AS TO ACTIVELY SUPPORT AND WORK WITH PUBLIC AND PRIVATE INSTITUTIONS THAT CONTRIBUTE TO THE DEVELOPMENT OF OUR REGION.

THE *ACTUALIDAD* COLLECTION, PART OF THE FOUNDATION'S CATALOGUE OF SCIENTIFIC PUBLICATIONS, IS A SERIES THAT CATERS FOR EXPERT READERS AS WELL AS THE GENERAL PUBLIC. EACH ISSUE IS STRUCTURED AS A MONOGRAPHIC REPORT AND OFFERS A THOUGHT-PROVOKING ANALYSIS OF A TOPIC RELEVANT TO ANDALUSIAN SOCIETY IN THE TWENTY-FIRST CENTURY.

Bailén 50, 41001 Seville, Spain
Tel.: +34 955 055 210. Fax: +34 955 055 211
www.centrodeestudiosandaluces.es

Legal Deposit: SE-1688-05
I.S.S.N.: 1699-8294

Democracy vs. Disinformation

Proposals for Protecting Open Societies

Manuel R. Torres Soriano
Universidad Pablo de Olavide, Seville

TABLE OF CONTENTS

1. Introduction

Disinformation has become a serious threat to the viability of democratic systems. The deliberate circulation of false, biased or manipulated information with hostile intentions has the ability to erode the very foundations of open societies. Disinformation targets one of the basic requirements of the liberal political order: the superiority of facts over emotions. But it goes about this slowly and stealthily, which is far more dangerous than any frontal assault could be, as it makes it harder for society to react. When the authority of data is undermined, emotions step in to fill the void. Although these campaigns may have specific short-term goals, their effects are ultimately permanent because they damage the "trinity of trusts" (Ingram, 2020): trust in others, trust in authorities/expertise and trust in democracy. The more these bases deteriorate, the greater a society's tendency to legitimize non-democratic forms of government and even take part in violent political activism.

The digital revolution changed the nature of the disinformation game, increasing the number of players on the field and giving unprecedented power to a tactic that hitherto had only played a minor role in confrontations between states. Authoritarian regimes have used technology not only to control their population more effectively, but also to promote illiberal practices beyond their borders (Barma et al., 2020). For example, although China and Russia are pursuing different goals, the conjunction of their apparently uncoordinated actions is having a more corrosive effect on democracy than either country could have achieved on its own (see Table I).

The boom of online disinformation campaigns came at a time when the world was ripe for such manipulation. In 2006, a more than thirty-year cycle of continuous worldwide expansion of political systems based on freedom came to an end. Since then, there has been a steady decline, not only in the number of regimes qualified as democracies, but also in the level of freedom in most of those countries (Ogilvy, 2017). Although the failure of second and third-wave democracies in Africa and Asia may partially explain this trend, the most troubling development is undoubtedly the decay of freedom in established democracies (*The Economist*, 2020).

Disinformation campaigns are not just products of the spontaneous action of a handful of unscrupulous politicians and opinion leaders; in fact, historically, they have been the result of the methodical action of major bureaucracies (Rid, 2020). Disinformation was, and in many ways still is, the purview of intelligence organizations—professionally managed, continuously improved, and generally wielded against foreign adversaries (see Figure I). Yet the worst damage to the democratic cause has always been self-inflicted. In recent years, we have witnessed a convergence (Sipher, 2018) of domestic and foreign, state and non-state actors. One of democracy's biggest challenges is actually having to face the hostile actions of various groups that are doing the same things for different reasons, creating a unity of interests among actors with separate starting points. Convergence happens, not because opposing actors support the same electoral outcome, but because, in their pursuit of incompatible goals, they all resort to the same disinformation tactics to inflame domestic tensions and undermine social cohesion (Mazarr et al., 2019).

In 2006, a more than thirty-year cycle of continuous worldwide expansion of political systems based on freedom came to an end. Since then, there has been a steady decline, not only in the number of regimes qualified as democracies, but also in the level of freedom in most of those countries

Table 1. Comparison of the Chinese and Russian approaches to using influence operations

Tools	Similarities	Differences
Advertising campaigns	Both create disinformation and use advertising strategies to augment its spread and influence abroad. Both use advertising strategies to influence public opinion inside their own diaspora communities.	China uses advertising campaigns to reach as wide a group as possible, whereas Russia's strategy targets specific segments of the population. The content boosted through Chinese campaigns tends to be related to issues in which their government is directly involved, whereas in Russian campaigns ties to the government agenda are more obscure.
Astroturfing (creating false opinion trends)	Both use government-organized non-governmental organizations (GONGOs) to create a climate conducive to international regulatory change. Both use bot accounts and paid trolls to boost astroturfing campaigns.	China tries to promote narratives that portray it as a responsible, internationally engaged country. Russia tries to confuse the information environment in order to sow political instability abroad and undermine democratic institutions.
Propagating technology for political control and influence	Both actively facilitate democratic backsliding by exporting the oppressive technological tools of political control that they have honed domestically. Both directly train and advise foreign government agents to strengthen their control through effective digital influence campaigns.	China tries to establish a stable relationship with the recipients of this technology, providing the infrastructure and support necessary to sustain it in the long term. Russia's approach is to supply digital influence tools and training to those who will use them, but with little effort invested in long-term maintenance.
Coercion and censorship of platforms online	Both create laws that ban or make it difficult for foreign social media to operate in their territory. Both pressure foreign tech companies to remove content favourable to political dissidents. Both pressure Western social media companies to remove content that supports activists and political or social movements within their borders.	Russia unilaterally implements censorship measures to control the domestic flow of information, whereas the Chinese regime, in addition to these tools, pressures companies that want to do business in China to protect its international image.

Source: adapted from (Kliman, 2020, 15)

This tendency has only been exacerbated by the onset of a global pandemic, which has weakened the global economy and forced democratic systems to undertake the complicated task of imposing a barrage of draconian measures to halt the spread of COVID-19. Actors with an anti-democratic agenda will continue using disinformation campaigns to exploit the contradictions between democratic promises and the reality of governments which have had to restrict their citizens' freedom in order to survive the pandemic.

Disinformation campaigns also have a negative effect on the efficacy of laws that govern democratic election processes. In most cases, these regulations were designed at a historical moment when lawmakers could not foresee the risks posed by the convergence of information manipulation and technology that did not even exist at the time.

Recent experiences with disinformation have made us realize the urgent need to adapt the rules of play in election processes to the reality of the most important threats they now face. Some states have already taken steps in this direction, especially those that have been the targets of political interference campaigns in recent years. Since 2017, several legislative projects have been proposed that aim to make online election propaganda more transparent and prevent foreign funding of such cam-

paigns. Some countries have attempted to protect certain periods of time that are especially vulnerable to disinformation campaigns, such as the weeks or months leading up to an election (Siboni and Shuker, 2019).

This article proposes a series of actions for making democratic systems more resilient and better able to cope with the threat of disinformation. To that end, it reviews the abundant literature that has taken a prescriptive approach to this issue in recent years.

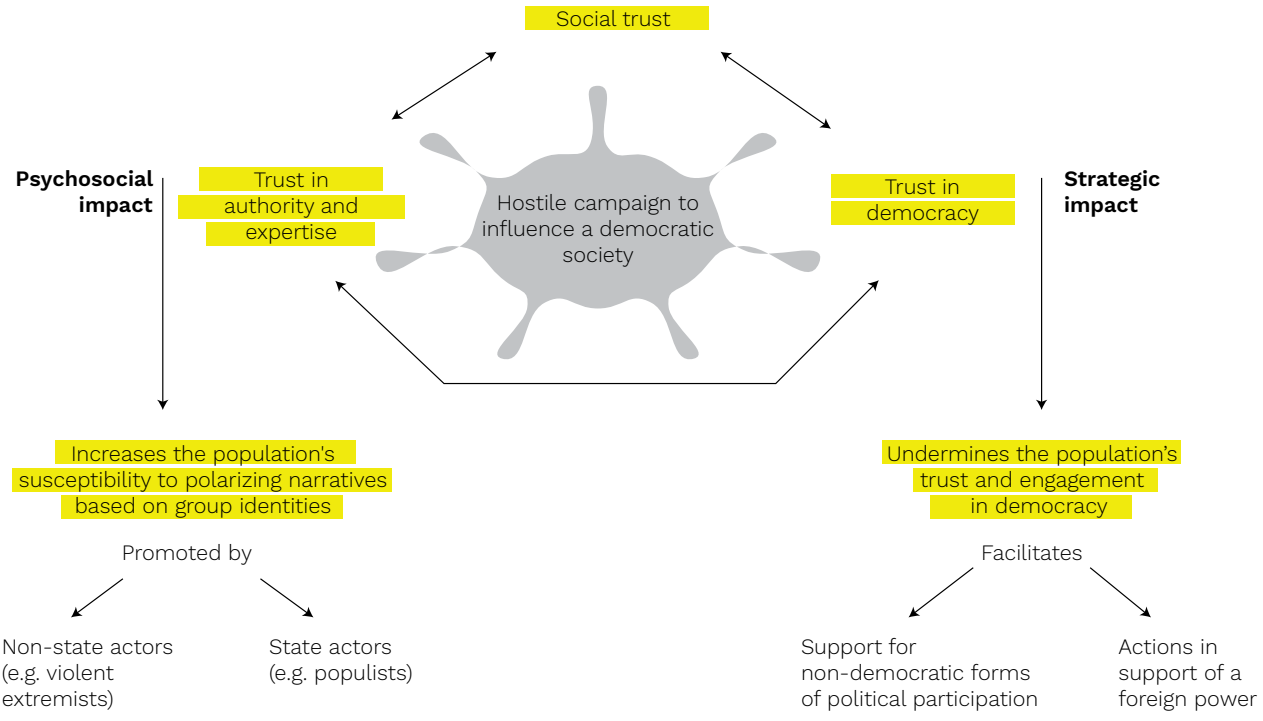
The goal is not to provide an exhaustive description of all implemented or recommended proposals, but rather to analyse the guiding principles that have proved most effective, thereby briefly outlining a plan of action for formulating effective policies to safeguard democratic systems.

2. What is Disinformation?

Any discussion of how to combat disinformation must begin by clarifying exactly what we mean by this term. Like so many other words that find their way into everyday speech, the term has been abused and misused, as its obviously negative connotations enhance its appeal as a means of discrediting adversaries or enemies. Conceptual accuracy has also been muddled by the fact that the word is used interchangeably or in conjunction with other traditional notions (influence, propaganda, active measures, information warfare, etc.) which have recently been joined by a variety of neologisms (fake news, post-truth, fact-checking, etc.).

To avoid getting bogged down in a conceptual debate, for our purposes, disinformation can be defined as the act of deliberately spreading false, manipulated or biased information with hostile intentions. As Nicolás de Pedro (2020) notes:

Figure 1. Strategic logic of anti-democratic disinformation campaigns



Source: adapted from (Ingram, 2020b)

> Intent is the key factor that distinguishes it [disinformation] from mistaken, inaccurate or even false information that is spread unwittingly. [...] Disinformation weaponizes information and communication. And this occurs in both domestic political disputes and wide-ranging geostrategic confrontations.

In addition to hostile intent, generally of a political nature, there are two other essential ingredients of disinformation: it contains false information that places the recipient in a vulnerable position, and it has the outward appearance of truth (Badillo, 2019).

This type of manipulation rarely aims to change the way people think. Instead, it attempts to corroborate what they already believe. And this is the secret behind the tremendous efficacy of disinformation: far from stating uncomfortable truths that force recipients to reconsider their opinions in light of the facts, disinformation places consumers in the comfortable position of confirming their biases (Torres, 2019). This is particularly gratifying when disinformation supports opinions that people are often reluctant to openly defend, believing them to be unpopular and liable to incur reproach from their peers.

Major online platforms have been instrumental in contributing to the virulence of disinformation; in fact, the business model of some of these companies has been described as “attention economics”

Disinformation needs to fuel social polarization, because when an issue is stripped of its nuances, people are inevitably forced to position themselves in binary terms: for or against. These manipulations do not have the power to create new rifts within society, but they can widen and deepen ones that already exist (Robinson et al., 2018).

Major online platforms have been instrumental in contributing to the virulence of disinformation; in fact, the interests of disinformers are aligned with those of the leading social media companies. The business model of some of these companies has been described as “attention economics” (Wu, 2016), where the ultimate goal is to increase the level of user engagement. To achieve this, these platforms incorporate gamification and attention-grabbing mechanisms that incite users to spend more time consuming, producing and interacting with the information they find on their pages. Most disinformation campaigns are perfectly synchronized with the operating logic of these services, which explains why they are able to spread beyond the control and knowledge of their own instigators. The principal online platforms are designed to make their inserted advertising useful to advertisers, giving them increasingly detailed information on user preferences and motivations so that they can target specific audiences with persuasive messages (Torres, 2018). The growing efficacy of automated market research tools has brought about a convergence of advertising technology and political propaganda, which rely on the same techniques: audience segmentation, micro-targeting and capitalizing on the prejudices, fears and aspirations of citizens/consumers.

The human brain has evolved so that its primitive, reflexive systems respond to information more rapidly than its reflective parts. Intuition precedes deliberation (Ahmad, 2020). Consequently, intuitive belief is less laborious than taking a sceptical view of all the informative input we receive throughout the day. Disinformation tends to use emotive language and evocative symbols to confirm our biases, eliciting reflexive responses that pre-empt reflective deliberation. It does not need to convey certainties; in fact, it is usually most effective when it spreads doubt. The strategy is to bury every inconvenient fact in an avalanche of competing interpretations, so that the truth becomes just another claim among many. The exploitation of doubt

aims not to foster legitimate scepticism but to relativize truth and encourage cynicism. In short, it is a spur to the cognitive bias that makes us demand a higher threshold of evidence for any claim that contradicts our intuitions.

In addition to feeding off our brain's most hard-wired biases, disinformation has also learned how to profit from the way our minds have adapted to the new information environment. Neuroplasticity is one of the most amazing features of the human brain, which has the inherent ability to form new neural pathways in response to different stimuli received over a lifetime. When digital devices burst into our lives, the brain quickly adapted to the characteristics of digital technology. Some authors (Miller, 2020) believe that this has resulted in the impairment of our cognitive abilities, or at least made it increasingly difficult for us to focus on one thing in a context rife with stimuli and distractions.

The ecosystem of digital media and networks has created an information overload, and citizens attempt to cope by taking cognitive shortcuts that make them particularly vulnerable to disinformation. Our ability to maintain focus is gradually diminishing, and this influences how content producers create and distribute information.

Headlines are designed to supposedly inform readers of a significant event in the most sensational way possible. Various studies (Alandete, 2019) have noted that the vast majority of online readers share news links on social media without reading the article first. Headlines are therefore the primary transmission vehicles of disinformation and the clearest indication of the intentions and priorities of their creators.

Another cognitive strategy is the way in which individuals attribute varying degrees of credibility to the information they process. Some statements are deemed more believable simply because we hear them repeated over and over again. This phenomenon, known as the "illusory truth effect" (Beasley, 2019), has become one of the clearest hallmarks of disinformation, which derives credibility from the reiteration of its claims.

In short, disinformation is a complex problem stemming from a variety of sources: human nature and its cognitive biases, social tensions, geostrategic rivalries, the crisis of the traditional media, our imperfect knowledge of how information technology affects society, etc. And this challenge demands a global response that simultaneously tackles the multiple roots of the problem. A few proposals for this response are offered in the following section.

The strategy is to bury every inconvenient fact in an avalanche of competing interpretations, so that the truth becomes just another claim among many. The exploitation of doubt aims not to foster legitimate scepticism but to relativize truth and encourage cynicism.

3. Principles of the Democratic Fight against Disinformation

3.1. Using transparency as an antidote

Democratic governments need to understand that transparency is one of the most effective weapons at their disposal and use it accordingly. Manipulative content thrives in situations where there is only partial access to information, turning the absence of hard facts into a pretext for all sorts of conspiracy theories. Many current restrictions on public access to information are hard to justify from the perspective of public safety or the protection of individual rights. Furthermore, in most cases there is no compelling reason why governments should not make their actions crystal clear. In fact, such restrictions are often merely a product of organizational indolence, a paralysing notion of how proprietary information should be protected, or a lack of internal incentives for government agencies to change their procedures and make transparency one of their primary objectives. Yet these barriers to freedom of information are often used by disinformation campaigns as the argument that justifies a wide variety of claims, based solely on speculation about why certain governments are "hiding something". This vicious circle can be broken by ensuring that public information does not circulate reactively, for when that happens, the manipulators have already contaminated public opinion and the damage is often irreversible.

3.2. Sharing information

In recent years, a number of national and multilateral initiatives have been launched to institutionalize the mission of detecting and denouncing foreign disinformation campaigns, such as the East StratCom Task Force (part of the External Action Service of the European Union), the European Centre of Excellence for Countering Hybrid Threats, the NATO StratCom Centre of Excellence in Riga, and the US Department of State's Global Engagement Center. These and other initiatives have done much to boost the institutional capacity for responding more rapidly to hostile campaigns. The next step must be to establish streamlined mechanisms for sharing information and best practices among all actors that aim to neutralize the effects of disinformation. For instance, this is one of the tasks that the European Commission assigned to the European External Action Service, which in addition to quickly detecting threats must also coordinate the response of the EU and its member-states (Badillo, 2019). In theory, this should not be a problem among actors who share the same values, but the reality is that, as in other spheres of public action, there are still organizational rivalries, national suspicions and political distortions that hinder the fluid exchange of information. An important aspect of combating such manipulations is taking organizational measures to ensure that the sincere desire to share helpful information is not strangled in a morass of bureaucratic regulations and red tape.

3.3. Enlisting the aid of civil society

Civil society has proved itself amazingly creative and genuinely committed to the fight against disinformation. In recent years, vibrant private initiatives have been steadily swelling the ranks of "digital Sherlocks": Ukraine's StopFake, Bellingcat, the Atlantic Council's Digital Forensic Research Lab, the Alliance for Security Democracy's Hamilton 68, EU DisinfoLab, the Baltic Elves, etc. In some cases, these actors are better equipped than governments to develop and update the tools needed to identify emerging disinformation techniques (Polyakova and Fried, 2019). Unlike their

public counterparts, these organizational structures are much less cumbersome and open to innovation, allowing them to remain effective in the face of dynamic, constantly changing disinformation tactics.

It is estimated that there are now at least 188 fact-checking entities in more than 60 countries, and fact-checking is a fast-growing field (Woolley and Joseff, 2020). Fact-checking can be an effective deterrent, as some actors may curb their impulses for fear that a negative report from such entities might damage their reputation.

The greatest weakness of these actors is their financial sustainability. Although they usually start out as altruistic initiatives that rely on a network of disinterested volunteers and contributors, over time they find that round-the-clock response capacity requires an increasing level of professionalism.

Governments, leading online service platforms, and philanthropic organizations should provide steady financial support that would enable these initiatives to consolidate and expand their range of action. The cost of this sponsorship is very low if we consider the potential of these actors to multiply the strength of all the counter-disinformation initiatives launched by government agencies.

3.4. Measuring impact

One of the problems associated with the fight against disinformation is the difficulty of measuring its effects (Hanson et al., 2019). Many of our perceptions about how these campaigns affect society are based on hunches rather than empirical evidence. There is no direct causal link between these campaigns and political and social behaviour; manipulative content is merely one of the countless variables that shape citizens' opinions and actions. It is especially hard to isolate the impact of these manipulations on pre-existing biases and prejudices, which are generally the *sine qua non* of effective disinformation. Moreover, the most effective disinformation campaigns tend to go unnoticed by message recipients, making it even more difficult to gauge the impact on the opinions and attitudes of people who do not even realize they have been targeted by these malign influences.

Metrics problems also affect the actors who promote such campaigns, though they have an incentive to use this lack of data for their own ends. It is not uncommon for such actors to exaggerate results and take credit for certain events to curry favour with their superiors (Rid, 2020).

The action of the media tends to further complicate the arduous task of measuring the impact of manipulations. At times, the journalistic coverage of these operations and their promoters becomes a kind of self-fulfilling prophecy, where messages with limited reach end up becoming widely popular thanks to media action. For example, the performance of the Internet Research Agency (the most notorious Russian troll farm) during the 2016 presidential elections in the United States was generally rather poor (Rid, 2000), but by republishing its posts and advertisements, the press turned it into a spectacular disinformation success story. The influential newspaper *The New York Times* published a front-page article (Kang et al., 2017) that reproduced an IRA-sponsored advertisement with an illustration of an arm-wrestling match between Satan (backing Hillary Clinton) and Jesus Christ (opposing her victory). Numerous national and international media used that illustration to report on any matter related to Russian interference in the American campaign. Yet the impact of that advertisement had been negligible until the media turned it into a news icon. The advertisement was posted on Facebook for a single day, on 19 October 2016, and only received 71 hits and 14 click-throughs. One year later, it was resurrected with the unwitting assistance of the traditional press.

Table 2. The five stages of election meddling

Stages	Actions
1	Using disinformation to amplify divisions and polarization within a society
2	Stealing sensitive and leakable data
3	Leaking the stolen data via "hacktivists" or whistleblowers
4	Whitewashing leaked data through the professional mass media
5	Certain candidates collude with the meddling foreign state or organization due to a convergence of interests

Source: adapted from (Aaltola, 2017).

Our blindness to the effects of these campaigns is worrying, not only because it means we may be wasting resources on ineffective measures, but primarily because of the risk that we will fail to detect the boomerang effect of our own anti-disinformation policies. However, our response to the structural metrics problem should not be resignation but an increase in funding to research new methods for gauging the impact of disinformation campaigns and policies to neutralize their effects. This is primarily a scientific challenge that can be overcome, at least in part, by stimulating and supporting the creativity of the research community. Only when we fill the gaps in our analytical capabilities will policymakers be able to determine the best way to tackle the problem.

3.5. Deterring aggressors

A key factor that explains the growth of hostile manipulation campaigns in recent years is the fact that new information technology has dramatically reduced the political and reputational cost to the actors who instigate them. The internet simplifies the process and makes it viable from the distance of a third country, but most importantly, it offers perpetrators a high degree of plausible deniability. The promoters of these campaigns are effectively shielded in cyberspace by the technical difficulties involved in determining authorship (see Table 2). As a result, some political regimes have decided that they have much to gain and little to lose from disinformation (Torres, 2019). Although the rewards of such campaigns are generally hypothetical, their perpetrators are convinced that they will not have to pay a price for their success or failure. This conviction is the true driving force behind disinformation campaigns, but it is also the primary obstacle that democratic states encounter when attempting to defend themselves. No matter how effective countermeasures may be, disinformation will continue to circulate as long as disinformers believe they can act with impunity.

The only way to substantially reduce the flow of disinformation is for democracies to increase the cost of such campaigns for their promoters. We need to alter the strategic calculations of manipulators so that, while the benefits remain hypothetical, the drawbacks are daunting and certain. In recent years, in an attempt to exercise this form of deterrence, the United States and certain European countries have resorted to the "name and shame" strategy (Carlin and Graff, 2018), specifically identifying and denouncing the Russian government as the party responsible for those campaigns. This is a considerable improvement on the deliberate ambiguity of responses up to this point, reporting the existence of such manipulations without explicitly naming the instigators to avoid damaging bilateral relations. Yet this tactic has only been moderately successful.

The goal is to make aggressors change their behaviour by denouncing their reprehensible actions before the court of international public opinion. But this

only works when the "shamed" party has a strong interest in maintaining good relations with the injured party and is consequently willing to abandon certain tactics when they become counterproductive. The United States "named and shamed" Russia, and later China, at a time when diplomatic relations were at their lowest point since the end of Cold War, so Putin's regime was able to use those accusations to fuel its rhetoric about constant American hostility towards Russia.

Democracies should consider the possibility of establishing joint, concerted measures at the global or regional level rather than focusing solely on their own problems. Disinformation has the ability to alter reality and seriously damage the societies it targets. Therefore, the range of potential retaliatory measures should be equally broad and not limited to the sphere of public diplomacy.

3.6. Strengthening the media ecosystem

Over a short period of time, the traditional media have been rocked by multiple waves of change, and they now find themselves at one of the most critical junctures in their entire history. The internet has usurped their role as a necessary intermediary for engaging with public opinion, and the industry's business model, still struggling to adjust to the loss of advertising revenue, is on shaky ground. This strategic disorientation was exacerbated by the onset of a global recession in 2008, which further complicated the already precarious financial situation of media companies. They began to downsize staff and rely on news stories that were not particularly difficult to obtain. As a result, the media not only lost their ability to detect and neutralize the disinformation that reached their editorial departments, but they also made themselves especially vulnerable to such manipulations because disinformation is free and drives up circulation and ratings (Torres, 2019). To make matters worse, the artificial intelligence boom radically transformed the industry (Manfredi and Ufarte, 2020), forcing it to adopt a micro-targeting strategy that leaves little room for stories with universal appeal. The journalism industry faces fierce competition from actors who are all too willing to exploit consumers' increasingly limited attention spans and automated tools that target individual emotional states to serve their own ends (Nadler, 2018). We have recently seen an increase in the number of non-journalistic actors on the information market with editorial interests (Manfredi and Ufarte, 2020). Think tanks, diplomatic representatives, NGOs, private companies and influencers are all vying for the elusive attention of readers and users. Some of these new participants openly act as "fake news entrepreneurs and political clickbait fabricators" (Benkler, 2018), given the traditional media's inability to contain this avalanche of increasingly atomized disinformation.

It is no coincidence that the media themselves have become one of the primary targets of disinformation campaigns and populist political discourse. However, the decline of the mainstream press or television media is not an unrelated phenomenon; it is one of the key factors that explain the growing influence of such manipulations. Any counter-disinformation strategy must bear in mind that a democratic society needs a strong media ecosystem committed to the challenging task of providing citizens with accurate information. In this sense, the journalism industry is not simply another economic actor whose survival depends on its ability to offer an attractive product or thrive in a competitive environment. Protecting and supporting this sector is one of democracy's most powerful weapons. This was one of the conclusions of the study (Jeangène et al., 2018) commissioned by the French government to analyse the lessons learned from the "Macron Leaks" incident: an unsuccessful attempt by Russian actors to influence the outcome of the 2017 presidential

election. According to this report, one of the main reasons why the calculated leaks of information stolen from Emmanuel Macron's campaign staff had such a limited impact on public opinion was the fact that France has a robust media ecosystem. Tabloids and "alternative" news websites are far less popular than in other countries, allowing serious journalism to check the incoming flow of manipulated information designed to illicitly meddle in the electoral process, with the aim of discrediting the centrist candidate and tipping the balance in favour of his pro-Russian, Europhobic rival.

If traditional media are protected, then democracies are also more protected against subtler and hence more dangerous attempts at interference. Sometimes fake news outlets and alternative news sites are merely a distraction, diverting attention from other long-term media manipulation strategies (Jeangène et al., 2018). Hostile intelligence services are eager to insert their messages and perspectives in mainstream media, and they work slowly and steadily to co-opt and influence professional journalists and contributors. Media companies under constant financial strain are easy prey for this kind of subterfuge.

Nevertheless, the solution is not to prop up these companies with a constant injection of public funds. That would only exacerbate the problem, turning media companies into fickle instruments of domestic political pressure. The least detrimental option would be to establish a wide variety of material and non-material incentives so that any serious journalism enterprise can prosper in today's challenging environment.

3.7. Using technology where it can be effective

When discussing the potential role of technological tools in the fight against disinformation, opinions tend to gravitate towards one of two extremes. At one end of the spectrum, we find authors who believe that neutralizing disinformation is a purely technical issue, and that the entire problem can be solved simply by using the right tools to detect and block malicious content. At the other end, we find those who believe that automated tools have nothing to offer, being unable to detect the subtle differences between intentional disinformation and false or inaccurate information distributed without hostile intentions. Moreover, these observers feel that the spread of automated processes can only exacerbate the problem, as their inevitable false positives will undermine freedom of speech.

In this debate, as with so many other issues, the solution lies in finding a happy medium. Although the internet does play a decisive role in spreading disinformation, it is not just a question of data analysis (as it was with the algorithms that eventually minimized the spam problem) (Roy and Duruk, 2018). The biggest problem with disinformation actually resides in how the human brain works and reacts to certain stimuli. And that problem is far too complex to be modelled and solved by writing algorithms to filter the information we consume and share. There is little hope that natural language processing will ever perfect the art of detecting content deliberately designed to deceive human beings. Yet we can-

Unlike "high-quality" disinformation, whose formal appearance is virtually indistinguishable from content generated by a legitimate actor, "junky" disinformation has many hallmarks that algorithms can easily detect: spelling errors, recycled material, template formats, etc.

not deny the technological component of this process, nor can we ignore the fact that intervention on this front is a very important part of a larger strategy.

Disinformation detection by algorithms is complicated and hard to scale, and it is unclear whether internet platforms have a real incentive to adopt such technology. However, it can bear fruit in the outer rings of disinformation distribution. Although these mechanisms have a very hard time spotting the sophisticated campaigns launched by state or corporate actors, this is not true of initiatives originating at the bottom of the food chain, where we find decentralized disinformation suppliers such as individual trolls, online forums and clickbait purveyors. Unlike "high-quality" disinformation, whose formal appearance is virtually indistinguishable from content generated by a legitimate actor, "junky" disinformation has many hallmarks that algorithms can easily detect (Schiffrin, 2019): spelling errors, recycled material, template formats, etc. Filtering out such content makes the problem more manageable by reducing the volume of information that needs to be individually assessed by human analysts.

4. Glossary

Astroturfing: the practice of masking the message of an actor or organization to make it appear as though it spontaneously originated from grassroots movements or civic groups. The term is derived from AstroTurf, a brand of synthetic carpeting designed to resemble natural grass.

Bots: software programs designed to engage with users by mimicking human behaviour. In disinformation campaigns, they are used to automate the process of spreading content and generate online interaction by disguising themselves as legitimate users.

Clickbait: a neologism used to describe the online phenomenon of misleading, sensationalized headlines and images whose sole purpose is to generate advertising revenue by tricking users into clicking on them.

Fact-checking: the process of verifying information to detect errors or false content. This is a specialized branch of investigative journalism that has become increasingly relevant and independent in recent years due to the mass proliferation of fraudulent online content.

Fake news: false information presented with the appearance of legitimacy and published by the media. Lately, this term has been popularized by numerous political actors who use it to discredit any information that reflects poorly on them.

Hacktivism: online political activism that uses hacking techniques. Opinions on the nature of this phenomenon vary: some see it as a new form of unconventional political engagement, while others regard it as a criminal practice intended to further the agendas of unlawful groups.

Trolls: in internet subculture, trolls are users who, hiding behind the shield of anonymity, post inflammatory and/or offensive messages with the intention of eliciting emotional responses.

Whistleblowers: individuals who publicly (and illegally) disclose confidential information about an organization for the purpose of denouncing unlawful or immoral practices before society. Whistleblowing is generally well perceived in the English-speaking world as a means of ending impunity for those guilty of wrongdoing.

5. References

AALTOLA, M. (2017):
"Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling", *FIIA Briefing Paper*, no. 226 <https://www.fiia.fi/wp-content/ uploads/2017/11/bp226_democracys_ele- venth_ hour.pdf>.

AHMAD, M. I. (2020):
"Friendly Sirens and Deadly Shores: How Disinformation Works", Center for Global Policy, 20 March <https://cgpolicy.org/articles/ friendly-sirens-and-deadly-shores-how-dis- information-works/>.

ALANDETE, D. (2019):
Fake News. La nueva arma de destrucción masiva. Madrid: Deusto.

BADILLO, A. (2019):
"La sociedad de la desinformación: propaganda, 'fake news' y la nueva geopolítica de la información", Real Instituto Elcano, DT 8/19 <http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/lengua+y+cultura/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news- y-nueva-geopolitica-de-informacion>.

BARMA, N., ET AL. (2020):
"Digital Authoritarianism: Finding Our Way Out of the Darkness", *War on the Rocks* <https://warontherocks.com/2020/02/digital- authoritarianism-finding-our-way-out-of-the- darkness/>.

BEASLEY, B. (2019):
"How Disinformation Hacks Your Brain", *Scientific American* <https://blogs. scientificamerican.com/observations/how-disinformation-hacks-your-brain/>.

BENKLER, Y. ET AL. (2018):
Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. New York: Oxford University Press.

BERTOLIN, G. ET AL. (2017):
Digital Hydra: Security Implications of False Information Online. Riga: NATO StratCom COE <https://www.stratcomcoe.org/digital-hydra-security-implications-false-information-online>.

CARLIN, J. P. AND GRAFF, G. M. (2018):
Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. New York: PublicAffairs.

DE PEDRO, N. (2020):
"Crisis del coronavirus: la desinformación del separatismo catalán como desafío estratégico para España", Instituto de Seguridad y Cultura <https://seguridadycultura.org/ wp-content/uploads/2020/04/ISC_Desinfo- CAT_AFF.pdf>.

GU, L. ET AL. (2017):
"The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public", *TrendLab Research Paper* <https:// documents.trendmicro.com/assets/white_ papers/wp-fake-news-machine-how-propa- gandists-abuse-the-internet.pdf>.

HANSON, F. ET AL. (2019):
Hacking democracies: Cataloguing cyber-enabled attacks on elections. SPI International Cyber Policy Centre <https://nla.gov.au/nla.obj-1388425475/view>.

INGRAM, H. J. (2020):
"The Strategic Logic of State and Non-State Malign 'Influence Activities'", *The RUSI Journal*, 165, 1, pp. 12–24.

INGRAM, H. J. (2020B):
"Pandemic Propaganda and the Global Democracy Crisis", *War on the Rocks*, 18 May <https://warontherocks.com/2020/05/pandemic-propaganda-and-the-global-democracy-crisis/>.

JEANGÈNE, J. B. ET AL. (2018):
Information Manipulation: A Challenge for Our Democracies. Paris: CAPS-IRSEM.

KANG, C. ET AL. (2017):
"Russia-Financed Ad Linked Clinton and Satan", *The New York Times*, 1 November <https://www.nytimes.com/2017/11/01/us/politics/facebook-goo- gle-twitter-russian-interference-hearings. html?smid=fb-nytimes&smtyp=cur>.

KLIMAN, D., ET AL. (2020):
"Dangerous Synergies: Countering Chinese and Russian Digital Influence Operations", 7 May <https://www.cnas.org/publications/ reports/ dangerous-synergies>.

MANFREDI, J. L. AND UFARTE, M.ª J. (2020):
"Inteligencia artificial y periodismo: una herramienta contra la desinformación", *Revista CIDOB d'Afers Internacionals*, no. 124, pp. 49–72.

MAZARR, M. ET AL. (2019):
The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment. Santa Monica, CA: Rand Corporation.

MILLER, M. N. (2020):
"Digital Threats to Democracy: The Online Brain", Center for a New American Security <https://www.cnas.org/publications/commentary/digital-threats-to-democracy-the-online-brain>.

NADLER, A. ET AL. (2018):
"Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech", Data & Society Research Institute <https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf>.

OGILVY, J. (2017):
"The Forces Driving Democratic Recession", *Forbes* <https://www.forbes.com/sites/stratfor/2017/05/25/the-forces-driving-democratic-recession/#775ad9494db2>.

POLYAKOVA, A. AND FRIED, D. (2019):
"Democratic Defense Against Disinformation 2.0", The Brookings Institution <https://www.brookings.edu/research/democratic-defense-against-disinformation-2-0/>.

RID, T. (2020):
Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus & Giroux.

ROBINSON, L. ET AL. (2018):
Modern Political Warfare: Current Practices and Possible Responses. Santa Monica, CA: Rand Corporation.

ROY, R. AND DURUK, C. (2018):
"Is Fake News spam?", *Margins*, 28 May <https://themargins.substack.com/p/is-fake-news-spam>.

SCHIFFRIN, A. (2019):
"AI Startups and the Fight Against Online Disinformation", *GMF Policy Paper* <https://www.gmfus.org/publications/ai-startups-and-fight-against-online-disinformation>.

SIPHER, J. (2018):
"Convergence Is Worse Than Collusion", *The Atlantic*, 13 August. <https://www.theatlantic.com/ideas/archive/2018/08/convergence-is-worse-than-collusion/567368/>.

SIBONI, G. AND SHUKER, P. (2019):
"Defending against Influence Operations: The Challenges Facing Liberal Democracies", in KUPERWASSER, Y. and SIMAN-TOV, D. (eds.): *The Cognitive Campaign: Strategic and Intelligence Perspectives*. Tel Aviv: INSS.

TETT, G. (2020):
"The uncomfortable truth about fake news", *Financial Times*, 19 February <https://www.ft.com/content/01622cd8-5303-11ea-90ad-25e377c0ee1f>.

THE ECONOMIST (2020):
"Global democracy has another bad year", *The Economist* <https://www.eco- nomist.com/graphic-detail/2020/01/22/global-democracy-has-another-bad-year>.

TORRES, M. R. (ED.) (2019):
#Desinformación. Poder y manipulación en la era digital. Granada: Comares.

TORRES, M. R. (2018):
"Operaciones de influencia e inteligencia artificial: una visión prospectiva", IEEE, 19 June <http://www.ieee.es/Galerias/fichero/ docs_opinion/2018/DIEEEO74-2018_Inteligen- ciaArtificial_ManuelRTorres.pdf>.

WOOLLEY, S. C. AND JOSEFF, K. (2020):
"Demand for Deceit: How the Way We Think Drives Disinformation", The National Endowment for Democracy <https://www.ned.org/wp-content/ uploads/2020/01/Demand-for-Deceit.pdf>.

WU, T. (2016):
The Attention Merchants: The Epic Scramble to Get Inside Our Heads, New York: Random House.

PAST ISSUES

...

53: Basic Traits of Demographic Ageing and the Elderly in Andalusia

54: Gender, Health and Social Order: The Case of the Clinical Model of Transsexualism

55: Managing Religious Diversity at the Regional and Local Level

56: Education as a Determining Factor of Intergenerational Mobility in Andalusia

57: Low-Cost Companies at Andalusian Airports

58: Construction of the Political Subject among At-Risk Youth

59: Willingness to Pay for the Environment: An Analysis with Data from Andalusia

60: Immigration in Andalusia: An Analysis with 2009 Social Security Statistics

61: The Perception of Inequality and the Demand for Redistribution Policies in Andalusia

62: Male Violence and Preventing Violence against Women

62: Male Violence and Preventing Violence against Women

63: Children and New Information Technology: A Look at the Reality of Andalusian Digital Natives

64: Contact between Citizens and Local Councils as a Form of Political Engagement in Andalusia

65: Towards a Sustainable Urban Mobility Model

66: Transitioning towards Employment for Andalusian Youth

67: The Organic Food Industry in Andalusia: Diagnosis, Challenges and Strategies

68: How Spaniards and Andalusians Perceive Poverty

69: Women in Local Government in Andalusia (1979–2011)

70: A Story about Identity and the Good Life in Andalusia

71: Wellbeing, Inequality and Poverty in Andalusia: A Comparative Study with the Rest of Spain Based on the 2006 and 2012 Living Conditions Surveys

72: Regional Responsibilities and Management of the Guadalquivir Basin

73: Legislative Reform, Violations of the European Social Charter and Appeals to the Charter in the Judicial System

74: Constitutional Reform and the New Paradigm of the Welfare State: From Contingent Legislation to Conscious Welfare Organization

75: Bullying, Cyberbullying and Dating Violence: A Study of How Primary and Secondary Students in Andalusia Manage Their Social Life

76: Do We Hate Politics?

77: Social Determinants of Health in Andalusia

78: Political Leaders and the Electoral Calendar: An Analysis of the Andalusian Population's Perception

79: Guaranteed Minimum Income in Andalusia: Scope and Limitations

80: Independent Publishing in Andalusia

81: Gender and Social Mobility: New Statistics for Andalusia

82: Changes in Electoral Behaviour in Andalusia: Analysis of the 2018–2019 Elections (Regional, National and Local)

83: Territorial Cohesion through National Identity: Wellbeing as a Unifying Factor in Spain

84: Gender Gaps and Biases in the Choice of STEM Studies: Why They Exist and How to Eliminate Them

85: The Challenge of Longevity in Andalusia: Causes, Evolution and Consequences

86: New Trends in the Structure of Andalusia: Territory, Population and Family in the 21st Century

87: Democracy vs. Disinformation: Proposals for Protecting Open Societies

ACTUALIDAD

ACTUALIDAD

ACTUALIDAD

Junta de Andalucía
Consejería de la Presidencia,
Administración Pública e Interior
CENTRO DE ESTUDIOS ANDALUCES

Andalucía
ORIGEN & DESTINO
Quinto Centenario de la Primera Vuelta al Mundo