How are cybersecurity threats, in the form of disinformation campaigns, reflected on the security measures they inspire?

A case study of the responses to Russian election meddling in Mexico, Brazil and Spain

Ailyn Christiansen
Abstract
The contemporary topic and fear of information attacks making their way and altering the course of democratic elections is a common one for many nations at current times. New technologies, cyberspace, and the increasing risk of hybrid warfare, as well as the little and vague regulation present to manage these, pose an intimidating threat to nations trying to uphold their liberal democratic values; and the nations taking advantage of this new-found form of influence are well aware of this.
This thesis centres on the topic of disinformation campaigns by the Russian state in foreign elections, namely those of Spain, Brazil, and Mexico. Particularly, it analyses the response policies from these nations, along with coordinated institutions, as a means of addressing these threats. Taking inspiration from Constructivist theory, and making use of the tools of comparative research, this paper conducts a thorough but straightforward analysis, searching for answers to its research question, and ultimately arriving at logic-founded conclusions regarding the importance of context in policy analysis, and the study of global security, and more importantly how its role is explained on the cases at hand.

[13.115 words]
# Table of Contents:

1. Introduction.............................................................................................................. 1

2. Theoretical framework............................................................................................ 2
   2.1 Literature Review .......................................................... ................................ 3
   2.2 IR-specific literature .......................................................................................... 5
   2.3 Theory .................................................................................................................. 6

3. Research design....................................................................................................... 7
   3.1 Methodology ......................................................................................................... 8
   3.2 Research Process .................................................................................................. 9
   3.3 Limitations .......................................................................................................... 12

4. Analysis .................................................................................................................... 13
   4.1 Categories for analysis ......................................................................................... 16
      Box 1 - Categories as present in each case study ................................................. 16
   4.2 Measures encompassed by each category ......................................................... 18
      Box 2 - Measures by each state ............................................................................ 19
   4.3 Findings from the data ....................................................................................... 21
      4.3.1 Spanish Catalan-Independence referendum of 2017 .................................... 21
      4.3.2 Brazilian general elections of 2018 ............................................................... 23
      4.3.3 Mexican general elections of 2018 ............................................................... 24
   4.5 Three types of actors .......................................................................................... 25
      4.5.1 The international cooperator ......................................................................... 26
      4.5.2 The state-level actor ..................................................................................... 27
      4.5.3 The inactive spectator ................................................................................... 28

5. Conclusion ................................................................................................................. 29

6. Bibliography ............................................................................................................. 31

Appendix.......................................................................................................................... 37
1. Introduction

Disinformation, as a term, refers to false information being knowingly shared with negative intent, or with the intention of harm; which is in what it differs from the also popular term misinformation: when false information is shared without a direct means of harm (Nagasako, 2020: 127). When it comes to the democratic functioning of states, the spreading of information, and its accuracy, is a process that must be closely monitored and protected, to ensure that it is not abused or corrupted by individuals, groups, or even states.

In today’s globalised world, governments are not only involved in their own elections, but also affected by those abroad, which translates into an interest in their results. When the stakes are high, this can lead to attempts at influencing foreign democracies and their proper functioning. Disinformation campaigns are a major way in which actors, often states but occasionally other powerful entities as well, chose to target the public whose votes they aim to control. Research shows that a large majority of these types of attacks are carried out by large, powerful, and authoritarian states, such as Russia or China (Nagasako, 2020: 127). Threatening measures such as those of disinformation campaigns trickle down into defensive ones by their targets. These states may opt to approach the issue from a governmental perspective - through policies, political discourse, laws, and the like, or can benefit from institutional measures, coming from organisations, unions, or other institutions, within and beyond the state, that have an interest in countering these foreign threats.

This thesis centres its analysis on those states who have been victim to cyberattacks by Russia’s hybrid warfare methods, namely that of calculated disinformation campaigns. More specifically, it sets focus on the measures they choose to take in response to such a threat. This is an issue that fits within the frameworks of global governance and democracy, as it concerns transnational security in the areas of policy and counterterrorism, as well as affecting the democratic functioning of states. This research aim was to resolve the puzzle that the issue presents: How do states respond to cyberthreats coming from abroad? What circumstances play a role in guiding the approach taken? Can states’ actions be understood by their geopolitical and social context? And do these determine, in any way, the type and extent of measures taken?

While I did not set off from an already formed hypothesis in order to answer my research question, there were certain broad assumptions held beforehand about what the results would bear. It was my expectation that the unique aspects of the circumstances in the three nations at hand, Spain, Brazil, and Mexico, would play a role in dictating the approaches they selected, in lieu of the resources available, and the potential support or backlash they might face from the public. Furthermore, I considered - perhaps too sensibly - that states would be most successful in their fight against
disinformation, if they managed to locate, before taking action, the areas in which disinformation is most directly or efficiently reaching their citizens, and focused their efforts on said area(s).

The thesis is structured firstly by introducing the broad topic and puzzle within it. Afterwards, the consecutive section outlines a comprehensive research literature on the topic, both within IR and other related fields of academia, to then conclude on a clear theory statement, including its relevance and appropriateness to the research question. Following that section, the Research Design chapter gives a detailed description of the methodology to be taken, as well as explains and argues for its functionality and the reasoning behind its selection. This section does a thorough job of describing the process taken for the different steps in the method, and explains the justification for them, as well as making mention of the limitations faced with the method chosen, and how these were addressed.

The next and most imperative section is that of the analysis itself, which has been divided into four parts. It first introduces the case studies at hand, following this with a general description of the categories of approaches as found within each case, and then outlining their specific measures taken, within these same categories. While these two parts act as summarised outlines, a more in-depth look into each states’ measures can be found in the Appendix. Thereafter, the Analysis chapter introduces a critical analysis and its subsequent findings from the data, divided by country; as well as introducing these nations as examples of three different types of state-actors. In the succeeding section, the thesis ends its analysis with a Conclusion chapter, recollecting, as well as describing the findings, and delineating potential research answers.

The final section can be found after the conclusion chapter, and is the Appendix. This section provides a very in-depth overview of the full range of measures taken by the states being considered in the analysis. While it is not included within the analysis itself, or the word count for that matter, the Appendix is meant to provide the reader with the necessary information to better understand its findings, as well as the basis for any answers obtained from it.

2. Theoretical framework

Previous researchers within IR have approached the issues of fake news, social media, propaganda, leaks, AI, and others, when it comes to the topic of information warfare (Landon-Murray, Mujkic, and Nussbaum, 2019: 513; and Nagasako, 2020: 126), various of which are encompassed within the disinformation campaigns I have taken to investigate.

2.1 Literature Review

Since authors of previous works of relevance to the field have opted for various and differing approaches to their analyses, this literature review has been structured and divided according to three strands of thought, to make for a clearer summary: Realist, Liberal, and Poststructuralist perspectives. Those who view the issue through more of a Realist lens were recurring in their focus on state actors...
as their main interest, and made up the majority of the theoretical approaches. Alternative perspectives were also present, however. Various authors chose to set their focus on the role and importance of International Law - as well as providing criticism to it, which gave their work a leaning towards a Liberalist perspective. The third approach noted was that of authors who, in many different ways, led their analysis by looking into the central matter of discourse, and opting for a Poststructuralist point of view.

The first group, which I deem as the Realist one, sets out to analyse the issue in terms of security threats to the state. Tenove (2020: 518), for instance, highlights the threats to three aspects of democracy posed by disinformation: self-determination, accountable representation, and public deliberation, promoting opinion and will formation. Furthermore, Janda (2018: 182) highlights Russian-specific threats to Western democracies, by means of support for political extremism, offensive cyber-attacks and disinformation campaigns. Both their work opts to analyse policy and other responses, such as sanctions, from the nations affected by the attacks described (Tenove, 2020: 519-520; and Janda, 2018: 183-184). I took from their method in my own study, looking too at the measures taken in response to these threats, but focusing on that of disinformation specifically.

Other authors within this category divert from this approach. Landon-Murray, Mujkic and Nussbaum (2019: 512), select a single and clear case study of disinformation in a foreign election: the United States’ general election of 2016. Their article conducts its study by centering around US covert action and then discussing modalities for action taken by the government, as well as presenting alternative policy strategies (Landon-Murray, Mujkic and Nussbaum, 2019: 513). This is an imperative piece of my framework, because I was inspired by the structure of their work in mine, choosing to look at specific case studies, and their course of action. Despite not acting as a policy recommendation, their paper does aim to provide an outlook on the success of the different measures taken, something that this thesis has not intended to do.

Most of the above research has potential for utility in terms of policy recommendations and guidance, but fails to consider the international dimension of disinformation campaigns, and the role that multilateral institutions play or ought to play in dealing with them.

The second group or category is that which takes on a more Liberal approach, setting its focus mainly on the role of International Law. Focusing on state-sponsored disinformation campaigns, Isik, Bildik, and Molla (2022: 107) centre their analysis on the ways in which these breach international law. Namely, they highlight the principle of sovereignty, the principle of non-intervention, and the right to self-determination, and they conclude their study by stating the importance of consensus between the states, in order to implement the rules, norms, and principles encompassed by international law (Isik, Bildik, and Molla, 2022: 119-120). Suárez Serrano (2021: 1), as well, approaches the issue of disinformation campaigns by emphasising the idea of information warfare,
and the role that international law shall play in it. While he argues for international law, and namely the UN Security Council, as a key actor for dealing with these types of threats, he also reinstates the necessity there is for international bodies to categorise them as such in order to address them (Suárez Serrano, 2021: 8-10).

My study’s perspective differs from the authors’ in this case, since it does not follow or consider the role of international law, in its current state, as relevant within the issue of information warfare. However, I do take from these particular pieces of work when they highlight the role of consensus between states or entities. In order for a multilateral body to be able to face a threat, there needs to be a level of agreement in terms of what the threat is, what constitutes part of this threat, and what measures are reasonable and required to counter it, an idea which applies beyond the realm of international law.

Rather than providing recommendations, as the Realist researchers do, authors within this category highlight the shortcomings of International Law, urging for international institutions to be more proactive in their denouncement of cyber attacks on democracy. However, they fail to provide a clear outline for measures that would enable these bodies to do so.

The third and final group is that which introduces discourse as an important concept when it comes to disinformation, taking on a Poststructuralist approach. It encompasses work by authors such as Baumann (2020: 288), who opts to analyse the role of discourse in Russia-West relations and interactions. Focusing on interpretations that arise from discourse, the author employs a Comparative Discourse Analysis (Baumann, 2020: 289), defining four parameters for studying: ‘the specific issue a discourse evolves around’, ‘the number of Selves to be considered’, ‘the time frame(s) under study’, and ‘the scope of the discourse’ (Ibid. 292). Baumann’s method itself is of great relevance to mine, given the comparative nature of my study, and so is his framework. Russia-West relations, which I must highlight differ between the nations I chose to look into, play an immense role in the perception that the governments, and the public, have of this threat, and the measures they will be willing or likely to put in place against it.

Authors and studies within this group are helpful in their alternative perspectives of matters of power and discourse; their analyses serve as good groundwork for building an understanding of the topic on, but fail to act as basis for research itself, due to the broad-ness of their scope.

2.2 IR-specific literature

All of the authors above served the role of providing a basic framework for the topic of disinformation campaigns and the responses to them. Their works encompassed a large combination of fields within the social sciences, including but not limited to security studies, politics, international law, and policy analysis, a multidisciplinary approach which resembles that of International Relations itself. The following authors and their work, which is centred within IR specifically, will aid this
previous understanding, as well as set it in an IR context, highlighting its relevance and presence in the field.

Maschmeyer (2023: 79) incorporates the idea of an alternative perception of power, through the lens of a structural view of it: subversion, which targets social or sociotechnical structures. His ideas regarding alternative approaches to power are highly relevant to my research and will become useful shortly, when I discuss the relevance of ‘sharp power’ when it comes to disinformation campaigns. The author here chooses to highlight issues of interaction and capacities, as means of harm, guided by the example of the US Elections Interference Campaign (Maschmeyer, 2023: 81).

Machurishvili (2021: 131) takes on an Offensive Realist theoretical approach to his analysis of EU measures in response to the Russia-Georgian conflict of 2008, both in his understanding of the conflict itself, as well as in his focus on the EU’s military security approach. On top of aiming to research the Union’s responses to the invasion, the author also looks at Russian propaganda, and the effect it had on the perception of the societies surrounding the conflict (Machurishvili, 2021: 142). Their study is guided by a qualitative analysis of conflict resolution methods by the European Union’s CFSP and CSDP, a methodology that acts as a useful tool for my own qualitative analysis.

Livingston and Nassetta (2018: 101) highlight in their paper the role of language and ideas in international relations. They tackle the issue of how best to analyse Russian hybrid warfare, from the point of view of Constructivist theory, by studying the frames and counterframes spread by disinformation (Livingston and Nassetta, 2018: 106). This work is of utmost importance for my thesis’ framework because of its theoretical application, given that my analysis is too, guided by Constructivism throughout its different sections.

The last two subheadings have presented a variety of theories and methods previously used for studying this particular topic. Taking inspiration from certain of them, as well as visualising how others may not be fitting for this research study, it is my conclusion that a comparative and content analysis methods would be most beneficial, following in the footsteps of authors such as Baumann (2020) and Machurishvili (2021), as well as guiding my analysis with Constructivist theory, as Livingston and Nassetta (2018) have done.

2.3 Theory

While the main focus of previous authors has mostly been on either disinformation campaigns as security concerns, or cybersecurity policies, I look to incorporate the two in my work. The analysis by Tuukka Elonheiro (2021: 114) is carried out in a similar manner, analysing Western vulnerability to information cyberattacks, and examining the different security approaches in response to Russian hybrid warfare. It goes over different forms of hybrid warfare: threats or use of military forces, cyberwarfare, information warfare and non-military coercion and intimidation (Tuukka Elonheiro,
The analysis I have conducted is a more specific study, focusing solely on the issue of information warfare.

As previously mentioned, an alternative perception of power is a key part of this topic: sharp power. This is a concept, as popularised by the ‘National Endowment for Democracy’ (NET) and incorporated by Walker (2018: 11-12), that incorporates ideas of censorship and information manipulation into its understanding of power, in which these are used to pierce the political sphere, among others, of targeted countries. This phenomenon is often studied when looking at China or Russia, as this thesis does, and perceived as a tool that they employ for dissemination of information, images, and ideas, or CAMP - culture, academia, media, and publishing sectors (Walker, Kalathil, and Ludwig, 2020: 128; and Walker, 2018: 13). These countries are presented as “ill-equipped” for soft power, relating to public image, because of their authoritarian states; therefore leaning towards this ‘sharp’ one as the alternative to hard or military power (Walker, 2018: 18).

The concept of sharp power is highly relevant when discussing disinformation because of its close relation to discourse control as a means of influence. The mere idea of disinformation campaigns, implies that controlling a narrative, through information channels, translates directly into power and influence. If we looked at power from a more traditional perspective, as Realism does, we would find that the power to misinform only really fits within less classical theories of IR, such as Poststructuralism or Constructivism.

This research is encompassed within the framework of Constructivism, considering the aspects of historical, cultural, and social context to be of utmost relevance when looking at any empirical phenomenon (Dunne, Kurki, and Smith, 2016: 162-163), as well as matters of identity, norms, and knowledge (Baylis, Smith, and Owens, 2020: 193). I believe these factors are necessary to take into account if one is to analyse and understand the measures taken by a state or actor, at a particular time, and against a particular threat. When dealing with disinformation campaigns against a democratic nation, the country’s democratic legitimacy, as well as that of its electoral processes, their record of dealing with such attacks in the past, and their citizen’s perception of their state and its actions, are all going to greatly influence, if not completely dictate, the measures that are taken and/or deemed appropriate. This decision, guided by its context, may not always fit neatly into what would be most efficient in theory.

While certain authors may take on a very objective approach to policy analysis and recommendation, searching for the most efficient problem-solving measures, I consider it as important to take into account external matters other than the threat itself, such as the context of these decisions. After all, it is the social construction of reality that ‘nurture’ actors, in this case states, through their cultural environment (Baylis, Smith, and Owens, 2020: 195). From a constructivist perspective, the choices, as well as their success, of any policy under study can only be understood...
from a broader point of view than simply technical utility. In terms of government policies dealing with disinformation, there is a thin line for states to navigate between being proactive to keep their citizens safe, and being perceived as deflective, blaming 'fake news' of pushing rhetorics that do not serve their interest.

Within the Constructivist leaning of my analysis, the Copenhagen School, and its related Security Studies Theory, have also been deemed as an appropriate framework for understanding and studying the given issue of disinformation. Taking on a critical approach to security studies and with the help of its securitisation theory, the Copenhagen School provides the right tools for looking into contemporary threats to a states’ national security, as well as how these governments’ responses are operationalised, whether it be in a nonpolitical, or politicised manner (Romaniuk, 2018: 2).

When centering on Securitisation theory in particular, one could emphasise the role of the referent object as that ‘which is to be secured’ (Buzan and Wæver, 2003: 71), and relate this to the circumstance of countering disinformation. Whether states, as a securitising actor, opt to see their democracy or their citizens, as the referent object, will determine what type of measures they take to protect them. The context, as mentioned in the previous paragraph, of how and if a threat is perceived by the state, will in turn define the extent of the means it takes to ensure its safety. Governments can, in turn, be expected to act in a logic of appropriateness, taking actions that are rational given the particularities of the securitisation process, who they are as a state, and what the possibilities available to them are (Dunne, Kurki, and Smith, 2016: 164).

3. Research design

The data that this study collected for the purpose of its analysis is in the form of governmental and institutional documents: policies, strategy statements, and reports, among others, both from the states’ representative bodies, as well as from organisations that they are members of. This is the same type of data that others authors studying the subject have opted for, such as Tenove (2020: 519-520), Janda (2018: 183-184), and Landon-Murray, Mijkic, and Nussbaum (2019: 513), whose approaches I take inspiration from.

From these sources’ content I have drawn my data for analysis, looking particularly to mentions of cybersecurity strategy broadly, as well as any reference to disinformation campaigns, foreign threats to democratic elections, or any specific instances of these.

3.1 Methodology

My method selection is close to that of Baumann (2020: 289), who conducted a comparative discourse analysis for their study. While their approach places a lot of emphasis on the discourse aspect of disinformation, this research is instead focused on the outcomes of it rather than the phenomenon itself. For doing this, the specific method proposed is a small-N Comparative Analysis
(Halperin and Heath, 2020: 237), enabled by a simultaneous content analysis of the data gathered. As described by Halperin and Heath, I found this to be the most logical path because of its applicability or ‘contextualisation’, going beyond the scope of particular or individual cases, but without rolling into general ones (Ibid. 238). What is meant by this is that while the study does look at individual case studies, it is still possible to avoid the risk of fake universalism, while being able to consider specific, rather than general, contextual components.

This particular instance of comparison, as previously mentioned, has as its focus qualitative forms of data or content, namely textual documents of various sorts. Focusing on official sources such as government and institutional policies and reports allows for an unobtrusive form of data, where little to none human, be it politicians, journalists, or individuals, bias can be seen in the sources. Qualitative analyses are a prevalent method within International Relations, as well as in Political Science and other Social Sciences’ disciplines; and various authors within IR have argued for its value and relevance in the field, namely in regards to the case of content analysis.

Hermann (2008: 155), highlights the use of qualitative content analysis in regards to its focus on whether themes and targets are present or absent in the content, rather than the frequency with which they are, as quantitative content analysis does. She emphasises the importance of context and circumstances of a message, noting how previously common ideas disappearing, or novel ones coming up, as well as new conjunctions of previously separated ideas, may all be relevant factors for understanding a message and what its intentions are (Hermann, 2008: 156). I incorporate some of these ideas in my comparative design, given the interest placed on analysing what the content says about each case study in relation to each other.

Pashakhanlou (2017: 452) points to the criticisms of the traditionally quantitative content analysis present in IR, particularly in its failure to provide a contextualised understanding of its findings. Instead he argues for an integrated content analysis in the field, including aspects of both quantitative and qualitative approaches. He discusses as well the upsides of qualitative content analysis, in comparison to its relative quantitative one, in its incorporation of context, authors, and recipients, giving central focus to interpretation (Pashakhanlou, 2017: 449). In comparison to discourse analysis, on the other hand, he highlights its interpretative and systematic - rather than holistic - nature, which is specially useful for descriptive projects (Ibid. 452). His paper not only discusses the usefulness and place that content analysis has within the field of International Relations, but also makes an argument for its utility in the purpose of this research study.

Ide and Mello (2022: 4), thirdly, discuss Qualitative Comparative Analysis (QCA) specifically, and argue for its utility in identifying conditions, or combinations of them, that lead or are needed for a specific outcome. This method allows the researcher to recognise relations, as well as their dependence on contextual factors (Ide and Mello, 2022: 7-8). This phenomena is titled
conjectural causation, and is part of what enables QCAs to bridge various theoretical fields of IR (Ibid.). While the structure of QCAs and their truth tables is not adopted in this thesis, its guidance in terms of comparing and contrasting qualitative data are still highly relevant and useful.

3.2 Research Process
Before being able to begin the analysis, the issue of case selection was faced, which was influenced by the matter of language. Given that I wanted to make the sources at hand as largely accessible to myself as possible, countries were selected whose languages I speak and/or understand: Spain, Mexico, and Brazil. The particular events selected are that of the Catalan-independence referendum of 2017, the Mexican general elections of 2018, and the Brazilian general elections of 2018 as well. I find it important to make mention of the fact that I am a native Spanish speaker, which enables me to utilise all original documents for the cases of Spain and Mexico, as well as the large amount of Spanish-translations available from Brazil. Furthermore, I have an intermediate level of Portuguese, gained by four years of language classes taken as part of my secondary education curriculum. While my speaking abilities are somewhat out of practice, my reading comprehension, combined with the languages’ similarity, is certainly suited to be able to understand and translate the sources as needed.

In order to proceed with the data collection, the first step was to locate the right places for gathering it. These were found to be official government websites, where access to various official statements, policies, reports, and much more is available, as well as websites and databases of any regional institutions or cooperations that these nations are part of: the EU, NATO, Mercosur, and the USMCA (United States-Mexico-Canada Agreement, or former NAFTA). Rather than collecting equal amounts of data from each state, it was the goal to make the selection to be as accurately descriptive of the three countries as possible. This means that data could and has been very abundant for some cases, while highly limited for others; which is an indicator of the extent of action, concern, and context of each one. The equivalence of data, in this case, refers to being able to showcase a complete and precise framework of the individual nations’ plan of action.

For this reason, the data selection was one of the most imperative steps of the study, as it was of utmost importance to be able to select the most representative and comprehensive sources possible while browsing the previously mentioned platforms. The aim was to limit the selections to those released between the times at which the cyberattacks in question occurred and the elections following them. Within this range, the sources were then cut down to only those that made mention of any measures taken against disinformation. While the content of these documents was considered in its entirety, most of their information was not of direct relevance to my research, therefore only the
sections (paragraphs, articles, chapters) where these issues are addressed were selected for analysis, and are encompassed in the Appendix.

It is important to note that the states in question and the phenomena at hand do not exist in a vacuum. What this statement intends to communicate, is that these nations, like many others, are victims of many constant forms of mis-, as well as dis-, information, other than the one of focus for this study. Having growing amounts of fake information incoming, both nationally and internationally (regarding politics, COVID-19, elections and many more) means that the measures taken by these governments and their counterparts will, for the most part, not be exclusively tasked with dealing with a sole circumstance of this type of cyber attack. Because of this, all the policies, reports and other approaches mentioned will be taken as a response to the threat of disinformation broadly, including that of the selected instances, but not limited to it.

For the analysing part, the data previously selected was first categorised by identifying the common themes and topics mentioned by each source. This aided the organising of recurring approaches and ideas present in each country’s various levels of action. Throughout the process of reading the large selection of documents from each nation’s case, certain categories were selected for the different actions to be divided into, both throughout the countries, as well as certain country-specific ones that were considered relevant to highlight. These categories are as described in the following paragraphs.

I ought to point out that rather than selecting categories for analysis, the process started by conducting a thorough reading of all the documents selected. Only afterwards, did the common themes of the different measures emerge and were defined; these were then polished into titles to guide the structure of the analysis. These categorisations, or some of them, show up in the different data pertaining to each country, and speak to the origin and intent of the approach of each nation.

The first section of approaches is encompassed within the sphere of ‘Transparency and cooperation with other governments’. This includes all proposals whose aim is to increase and/or improve the transnational aspect of the fight against disinformation, ranging from multilateral agreements, to the institution of shared networks and resources, as well as bodies tasked with the sole purpose of focusing on countering this threat. This category looks for the mention of terms such as: international cooperation, international networks, mentions of specific actors such as the EU, Mercosur, NATO, or countries other than their own, as well as any proposition that looked to incorporate foreign nations into its functioning.

Within the realm of transparency but shifting the perspective slightly, is the second category, which focuses on ‘Open communication and cooperation within the government’. This section takes on similar actions to the previous, but rather focuses on the different bodies and institutions present
within a state. It deals with the means and measures to increase and improve the flow of communication between them, as well as ensuring that their actions are complementary with each other, rather than contradicting or repetitive. In order to categorise approaches within this category, mentions of ideas such as national networks between actors, researchers, and educational and governmental institutions, as well as explicit mention of specific bodies such as the national police, the electoral body and its members, political parties, and private institutions within media and other spheres, were selected.

The third category of approach has been titled as ‘Organisational measures’, and includes all of the propositions to found new institutions or bodies, as well as improve the present ones, for the purpose of fighting disinformation, though not with the explicit aim of international or national cooperation. Some examples of thoughts that would point and fit as organisational, would be ideas of introducing and implementing new institutions and organisations to fight disinformation, discussions of measures to provide resources and improve present ones, as well as any mention of specific projects for either of these purposes.

Taking on the arena of regulatory measures is the fourth category I have recognised: ‘Social media companies and online platforms’. This is a category that encompasses those measures taking the role of fighters against the very roots of disinformation. Including ideas such as guidelines for these companies and platforms to set their actions by, commitments with private companies on measures to target disinformation within their platforms, legal measures to regulate their functioning in regards to fact-checking, information spreading and fake accounts, as well as judicial means of punishing those that violate the legal frameworks. The central idea of the measures within this section is to act as a means of either guidance or regulation for the platforms through which disinformation starts and spreads.

Similarly to the focus on the root of the issue, nations have taken on the approach of the means by which disinformation spreads, which ultimately is through society. The fifth category is the section for these, the ‘Societal measures’. Within this spectrum, mentions of strategies aimed at increasing people's media and information literacy, educational efforts to increase the involvement of civil society with matters of cybersecurity, and tools for the general public to be able to access trust-worthy fact-checking for their news, were highlighted.

The sixth and final section is more specific, and limited to those measures that relate most closely to the cases under study. ‘Election-specific measures’ are those that have democratic processes and the context surrounding them as their central focus, as well as the threat posed by disinformation in these particular circumstances. To analyse this category, those points which made mention of various aspects of the democratic process were selected, from political advertising and transparency, to raising awareness within the sector on the issue of disinformation and the risks it
poses, and also any mention of specific measures or tactics to be taken specifically during election period to reduce, and potentially eliminate, the spread of disinformation.

After having settled the stated sections, the analysis of their contents, and its comparison was able to have a more sensible structure. With the guideline provided by them, the process went on to create visual charts to better display the information, being able to visualise the countries side by side. Furthermore, the study encompassed written analyses of this data, which took into account the contents selected and helped to answer the thesis’ research questions: Who/what are the threats present in these nations? Social media, fake accounts and bots, mass-firing of false messages, or other factors? What measures are governments taking and prioritising to address these threats? And at what level or sector of governance? And, last but not least, what do these answers, and their level of success, say about these countries’ security strategies?

3.3 Limitations
There were limitations in regards to the type of data collected, which ought to be pointed out. Within policy studies and analyses, it is not uncommon to run into classified or unavailable files, particularly when looking in the area of security, or when focusing on older policies rather than the latest ones. This is the reason why the scope of analysis was extended, from the original policies, to include other forms of source material, such as reports or strategy statements, as well as those pertaining to actors other than the government itself. Where the existence of classified or unavailable files of any kind is known, their mention shall still be made, if anything to acknowledge the presence of further actions.

The methodology of qualitative research, both in regards to comparative and content analysis, presents certain limitations, as do most research approaches. Halperin and Heath (2020: 387) highlight that of the researcher bias, which can affect the process at various stages, including but not limited to the case selection, the source material selection, and the data selection, as well as analysis or interpretation of the findings. Given that it is a qualitative analysis, done on a small scale with a single researcher, these concerns cannot be completely avoided but rather need to be addressed to the extent possible. For this purpose, it is imperative that I am aware and mindful of my own personal biases and preconceptions throughout each and every step of the study, as well as consider how and which of my choices may be affected by them.

4. Analysis
Instances of information warfare attacks by Russian forces have been publicly denounced by government officials, as well as by various news outlets, journalists, and academics, in numerous cases. The ones central to this research paper are that of the Spanish Catalan-independence
referendum in 2017, the Brazilian general elections in 2018, and the Mexican general elections in 2018. The following paragraphs give a brief context for each case and its response.

Regarding the illegitimate Catalan-Independence Referendum carried out in Spain in 2017, we can see a continuation of Russia’s support for Western separatist movements in their deployment of state and social media efforts to push these separatist narratives (Polyakova and Boyer, 2018: 8). EU’s EastStratcom noted, during the period of time the referendum was being discussed and carried out, an increase in disinformation being posted in both Spanish and Russian language, largely from Russian state-owned news agencies (Rankin, 2017). We can note the perception of these actions as being an attack, in the national security strategy, which calls disinformation campaigns “a great threat to the electoral processes” (BOE 314, 2021: 167812). The state document even goes as far as to describe the cognitive scope as an additional point of interest to the traditional land, air, and water, for exercising influence (Ibid.).

As for their action plan, governmentally, this is largely based on a state document titled: ‘Procedimiento de actuación contra la desinformación’ [translated to: ‘Action procedure/plan against disinformation’], published by the National Security Council in October of 2020 (BOE 292, 2020). The state also implemented the creation of a ‘Comisión Permanente contra la Desinformación’ [translated to: ‘Permanent Commission against Disinformation’] (BOE 292, 2020: 96680).

On top of this, we can observe institutional approaches such as the ‘Action Plan Against Disinformation’ by the European Commission and the European External Action Service (EEAS), established in December of 2018 (BOE 292, 2020: 96673-96674; and European Commission, 2019: 2), the ‘European Democracy Action Plan’ (BOE 292, 2020: 96674), the ‘Rapid Alert System’ (RAS) by the EU (BOE 292, 2020: 96677; and European Commission, 2019: 3), and the collaboration of the Strategic Communication task forces and the EU Hybrid Fusion Cell within the EEAS (European Commission, 2019: 2). The specific measures outlined in all of these documents will be mentioned in Box 2, as well as detailed and categorised in the Appendix.

In the case of the Brazilian general elections of 2018, Russian intervention was called out first in September of the same year by a cybersecurity company called ‘FireEye’ (Benevides, 2018). They found mostly evidence of the use of bots, with the aim to increase the reach of posts criticising the democratic model and questioning its legitimacy (Ibid.). Once again we can associate this act as a perceived threat to the state, given by the extensive amount of data that will be outlined shortly.

For their plan of action, mainly, we can observe their approach as outlined by the ‘Programa de Lucha Contra la Desinformación’ [translated to: Programme for the Fight Against Disinformation]. This document serves as a permanent plan for fighting disinformation on the topics of the Electoral Justice and its members, the electronic vote system, the electoral process in its different stages, and the actors involved in it (Peres Osorio et al, 2022: 26-27).
We can see more action taken by the government in the form of, for instance, the ‘Projeto de Lei No. 2630’ [translated and from here on referred to as: Bill (lit. Law Project) No. 2630], a bill aimed at targeting ‘liberty, responsibility, and transparency’ in the internet (Vieira, 2020: 1-2). This document proposes multiple ways and measures to take to regulate social media and digital platforms in order to fight the disinformation being spread through them.

The third main source outlining Brazilian efforts against disinformation is named ‘Decreto No. 10.222’ [translated to: Decree No. 10.222]. This document consists of a concise National Strategy for Cybersecurity, and includes in it a comprehensive approach to navigating and taking advantage of cyberspace and the opportunities it entails (Decreto No. 10.222, 2020: 1-2). Within the margin of disinformation, and the cybersecurity threat it presents, this decree offers insight into the topic of international cooperation, as well as that of the general public’s level of maturity in cybersecurity matters (Ibid. 7-8). All three of these documents and the points encompassed within them outlined in it will be mentioned in Box 2, and categorised and further explained in the Appendix.

In the third instance of interest: the Mexican elections of 2018, we can see statements from US National Security Adviser, Gen. H.R. McMaster, warning of signs pointing to Russian meddling in their southern neighbour’s elections already the year prior to the elections themselves (Woody, 2018; and Semple and Franco, 2018). However, we can see limited statements and measures on behalf of the government to indicate that they view an explicit threat to their democracy in his actions.

In a 2021 questionnaire filled out by the Human Rights Commission of Mexico City [translated], we can find certain mentions that point towards a reasoning against extensive action to fight disinformation. Early into the document, the Commission stated a concern that governmental, institutional, and communication media mechanisms may present a threat to the rights of free speech, or incite hate speech (in the case of social media), if they were to target disinformation in their policies (CDHCM, 2021: 3). Despite the statement being limited to Mexico City itself, it gives way for a potentially nation-wide argument to abstain from substantial action against disinformation in the name of free speech. The same document goes on to outline how the existing bills and legal proposals in the city congress do not directly address disinformation or the diffusion, creation, or promotion of fake news (Ibid. 4). The lack of legislative measures at the city-level, aligns with the one encountered at the state-level as well.

In spite of the passive nature that these measures - or lack thereof - may indicate, research on the Mexican nation may point toward another reasoning. Valenzuela et al (2022) conducted a study on disinformation based in Mexico during the period leading up to the midterm elections. The aim of their research was to uncover what factors were positively related with the belief in false or inaccurate information. What the study found was that there was no significant association between the use of social platforms (or any one in particular) and misinformed beliefs (Valenzuela et al, 2022: 1).
Furthermore, it listed certain factors that did relate to having increased false beliefs and, against the popular blaming of social media, they found that those who discuss politics more often in conversation, those with lower information literacy, and those with higher digital skills, are more prone to be disinfomed (Ibid. 3 and 13). Particularly, they highlight how social media use for news had no relation to belief accuracy (Ibid. 3).

Being that the two identified factors are frequent political communication and discussion, and poor media literacy (Ibid. 14), it seems sensible that the governments would opt to focus their efforts on that which they can address through policy: media and information literacy. And, considering that advanced digital skills also relate positively with factually incorrect beliefs (Ibid. 14), this approach ought to be focused on the critical and accurate perception of information online, rather than technological abilities broadly. Certainly, it cannot be claimed that this study has shaped the course of government action, but it can possibly point towards facts that align with their reasoning.

The extent of Mexican governmental action is fully encompassed within a single document: ‘Informe de Estratégia Nacional de Seguridad Pública’ [translated to: National Public Security Strategy Report], which in turn makes mention of their ‘Ciberguía’ [translated to: Cyber-guide] (Gobierno de México, 2022: 163). All other relevant measures are within the scope of civil society or private enterprises, primarily in terms of fact-checking tools. ‘Verificado-Notimex’, ‘Verificado 2018’, and ‘El Sabueso’, are the three notable instances of anti-disinformation action being taken in response to the threat posed in the past elections. All of these documents and measures within them will be outlined in Box 2, as well as given more background in the Appendix.

Despite being victims to the same circumstances, we can already begin to see discrepancies between these nations’ approaches, which we can only assume would become even more extensive if we were to consider a bigger amount of empirical cases. While media, public authorities and social platforms are generally the main actors responsible for dealing with and stopping the spread of fake news (BOE 292, 2020: 96673), this multilateral approach is not the one necessarily opted for by most nations when it comes to the threat of disinformation. The following sections go in-depth into each individual case study, and look into the different approaches opted for by the actors involved, in hopes of addressing the aforementioned disinformation campaigns they were victims of.

4.1 Categories for analysis

While the categories as previously explained in the Methodology section are present in multiple of the cases - or absent in some instances - they are not necessarily showcased in the same ways or through the same means. The following table (Box 1) will outline the specific point of view present in each country’s national approach when it comes to each section of analysis individually.
<table>
<thead>
<tr>
<th>Category headline</th>
<th>Catalan-Independence referendum 2017</th>
<th>Brazilian general elections 2018</th>
<th>Mexican general elections 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency and cooperation with other governments</td>
<td>International cooperation being discussed in terms of EU action and cooperation. Issues highlighted are that of joint networks, both institutional and national, for responses, and information sharing.</td>
<td>Brief mention of expansion of international cooperation in the field of cybersecurity.</td>
<td>No mention of international cooperation measures taken.</td>
</tr>
<tr>
<td>Open communication and cooperation within the government</td>
<td>No mention of national cooperation measures taken.</td>
<td>Integration of the Electoral Justice bodies (Superior Electoral Court and Electoral Courts) in their resources and efforts. Focus on open communication. Cooperation with national non-governmental entities. Support to electoral bodies and public institutions. Dialogue with Federal Police and Electoral Prosecutor's Office to increase collaboration.</td>
<td>No mention of national cooperation measures taken.</td>
</tr>
<tr>
<td>Organisational measures</td>
<td>Discussion of means to improve EU institutions’ and member states’ capacity to detect, analyse, and expose disinformation. Implementation of a new institution for media and source transparency.</td>
<td>Establishment of networks with technology and infrastructure companies. Setting of standard practices against disinformation.</td>
<td>No mention of organisational measures taken.</td>
</tr>
<tr>
<td>Social media companies and online platforms</td>
<td>Implementation of a voluntary guidance for private institutions. Highlighting of media plurality and diversity.</td>
<td>Discussion of a Bill proposal for regulation and punishment of social media companies, online platforms, and private messaging companies. Focus on fact-checking cooperation with institutions.</td>
<td>No mention of regulatory measures taken for social media companies and online platforms.</td>
</tr>
<tr>
<td>Implementation of channels for reporting disinformation.</td>
<td>Educational incorporation of cybersecurity matters (basic education).</td>
<td>Focus on the providing of information on fake news to the general public. Incorporation of fact-checking tools for news corroborating.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>Societal measures</strong></td>
<td>Carrying our social events for media literacy, and other means for its improvement. Support for researchers and fact-checkers, within the EU and abroad. More public measures for civic society. Providing institutional fact-checking.</td>
<td>Educational incorporation of cybersecurity matters (basic education). Promotion of cybersecurity programmes at the higher education level. Focus on networks to spread accurate information, and fact-checking tools. Media literacy training.</td>
<td></td>
</tr>
<tr>
<td><strong>Election-specific measures</strong></td>
<td>Focus on matters of political advertising and communication, sponsored political content, and political party financing.</td>
<td>Electoral transparency. Raising awareness on disinformation and its risks among politicians and political parties.</td>
<td>No mention of election-specific measures taken.</td>
</tr>
</tbody>
</table>

It can be seen in the category of international cooperation a very different perspective between Spanish and Brazilian action. The former has its focus set on organisational and inter-state measures of information-sharing collaboration (mainly through the EU), and the latter is rather focused on international cooperation to improve cybersecurity capacities. As for the category of national measures, only Brazil can be seen as encompassing these. Mexico is notably not active in either of these regards.

Organisational measures of the two states share more similarities, in their focus on improving the ability and networks in place to fight disinformation. But Spain builds further by also instating an institution for media and source transparency. In terms of media regulation, the two countries return to taking on contrasting approaches. While Spain opts for voluntary guidelines for companies, Brazil opts for more strict projects to regulate them by legal standards. In this case, the latter takes on larger measures by also incorporating collaborative action with private companies, as well as with civilians through them, by means of reporting. In these two categories, Mexico is once again inactive.

The societal measures section holds both resemblances and differences between the three states. All three make mention of media literacy events and/or sharing information for awareness, as well as highlight the importance of creating and supporting the use of fact-checking tools, be it institutional, governmental, or news media focused. Brazil adds on to those by incorporating educational measures, at basic and graduate levels (from school education to higher educations), focused on cybersecurity.
As for election-specific measures, both Spain and Brazil are centred on the issue of political transparency, including matters of advertisement and funding. Brazil takes further measures in relation to education of individuals involved in the political processes. Mexico is lastly, not active in this regard.

4.2 Measures encompassed by each category

After having made a careful selection of the categories that best reflect the full spectrum of action taken by Spanish, Brazilian, and Mexican representatives, and comparing how these are reflected in each state (see Section 4.1), a comprehensive outline of these was grafted. While the full extent of the measures taken and what means they encompass can be found in this thesis’ Appendix (see page 37), their brief headings and mention is also outlined in the following Box 2.

<table>
<thead>
<tr>
<th>Category headline</th>
<th>Catalan-Independence referendum 2017</th>
<th>Brazilian general elections 2018</th>
<th>Mexican general elections 2018</th>
</tr>
</thead>
</table>
| Transparency and cooperation with other governments | ‘Action Plan Against Disinformation’  
○ Pillar 2: Actions 3, 4, and 5 (European Commission, 2018: 6-8)  
○ Rapid Alert System (European Commission, 2019: 3; and European Union, 2019: 1) | ‘Decreto No. 10.222’  
○ Point 2.3.8 (2020: 7-8) | No mention of international cooperation measures taken. |
| | ‘European Democracy Action Plan’  
○ Section 2.3 (European Commission, 2020: 6 and 8) | | |
| Open communication and cooperation within the government | No mention of national cooperation measures taken. | ‘Programme for the Fight Against Disinformation’  
○ National Strategy Stage 1 (Peres Osorio et al, 2022: 34)  
○ National Strategy Stage 3 (Ibid.)  
○ Axis 2: Projects 5 and 7 (Ibid. 53-54) | No mention of national cooperation measures taken. |
<table>
<thead>
<tr>
<th>Category</th>
<th>Reference</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisational measures</strong></td>
<td>'Action Plan Against Disinformation'</td>
<td>Axis 3: Project 5 (Ibid. 59)</td>
</tr>
<tr>
<td></td>
<td>○ Pillar 1: Actions 1 and 2 (European Commission, 2018: 5-6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'European Democracy Action Plan'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section 4.1 (European Commission, 2020: 19-20)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Social Observatory for Disinformation and Social Media Analysis' (SOMA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Source Transparency Index (European Commission, 2022: 2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Programme for the Fight Against Disinformation'</td>
<td>No mention of organisational measures taken.</td>
</tr>
<tr>
<td></td>
<td>○ Axis 3: Projects 6 and 7 (Peres Osorio et al, 2022: 60-61)</td>
<td></td>
</tr>
<tr>
<td><strong>Social media companies and online platforms</strong></td>
<td>'Action Plan Against Disinformation'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Pillar 3 (European Commission, 2018: 8-9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Voluntary Code of Practice (European Commission (2), 2018: 4-8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'European Democracy Action Plan'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section 3.4 (European Commission, 2020: 16-17)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section 4.2 (Ibid. 21-24)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Bill No. 2.630'</td>
<td>No mention of regulatory measures taken for social media companies and online platforms.</td>
</tr>
<tr>
<td></td>
<td>○ Section III: Article 10 (Vieira, 2020: 6-7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section IV: Articles 14, 14, 15, and 16 (Ibid. 7-8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section V: Article 28 (Ibid. 10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Programme for the Fight Against Disinformation'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Axis 3: Projects 1, 2, and 3 (Peres Osorio et al, 2022: 56)</td>
<td></td>
</tr>
<tr>
<td><strong>Societal measures</strong></td>
<td>'European Media Literacy Week' (European Commission, 2019: 2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Action Plan Against Disinformation'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Pillar 4: Actions 7, 8, and 9 (European Commission, 2018: 9-11)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Decreto 10.222'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section 2.3.10 (2020: 8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Programme for the Fight Against Disinformation'</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Axis 1: Projects 1, 2, 3, and 5 (Peres Osorio et al, 2022: 42-43 and 47)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Axis 2: Projects 1, 3, and 4 (Ibid. 49 and 51-52)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>'National Public Security Strategy Report' (Gobierno de México, 2022: 163)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Cyberguía [translated to: Cyber-guide]: Point 6 (Gobierno de México (2), 2020: 33-34)</td>
<td>Verificado-Notimex</td>
</tr>
</tbody>
</table>
The table above aids in gaining an understanding of the extent and frequency of measures by each state, in each regard, as well as allowing one to see just how many - or how few - different documents or reports addressed these categories of the issue. These understandings will be referenced and guide the following section outlining the findings from the data collected.

### 4.3 Findings from the data

Being able to visualise the way in which the approaches were directed, aided by Box 1, enables an analysis of the path chosen by the different countries. Furthermore, taking the information these documents provide, as expressed in the Appendix, and looking at it critically, leads to an understanding of the geopolitical context of each of the nations at hand, and which role these played in their response to the threat of disinformation.

While this is not a quantitative analysis, in that it is not looking for frequencies of the themes present within the data, the visual aid of Box 1 does allow for an understanding in regards to presence, absence, and frequency of action in the different categories. These, in turn, add more evidence to our analysis of the three nations’ approaches, and lead to more rounded and based conclusions to be drawn from the data.

The following sub-headings, divided by country, go on to analyse and conclude on which findings the previous data leads to. Actions taken and in which sector of government, will point towards an understanding of national priorities or preoccupations. Furthermore, a constructivist emphasis on the role of context will help understand what circumstance led to the differing perspectives, as well as potentially utilise these cases as ‘examples of’ due to their contextual action. Within the theoretical framework, it is also possible to visualise the importance that norms within

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○ Section 2.2 (Ibid. 5-6)</td>
<td>○ Axis 2: Project 6 (Ibid. 53)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Section 4.3 (Ibid. 25)</td>
<td>○ Axis 3: Project 4 (Ibid. 57-58)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
these societies had in terms of their security strategies. While looking at countries’ past policies was not within the scope of this thesis, the complete overview of their national security reports has allowed us to point out trends in their tactics, which indicate a certain standard when it comes to their security policy. Finally, and taking from a more content-analysis approach to research, the absence or combination of ideas will also act as an indicator of states’ reasoning, as well as a probable reflection of their political and socio-economic atmospheres.

4.3.1 Spanish Catalan-Independence referendum of 2017

For the case of Spain, it can be highlighted that their social and geopolitical context, being part of the EU and having a relatively stable political environment, as compared with the other two nations at hand, is crucial in understanding the reasoning behind the measures prioritised, given that a states’ agency allows it to be influenced by the environment it is present in (Dunne, Kurki, and Smith, 2016: 165). These measures are not only expected to have success from a theoretical perspective, but are also likely to be understood and not opposed by the population. The data recollected, and the careful analysis of its content, help create a fuller picture of what the situation was in Spain, and how they chose to address it.

It is important to reiterate how it is not only the information at hand, but also the absence of topics within the national discussion, or the repetition of common themes, that aids the process of reaching answers for some of our research questions. Recurring subjects, or wordings, within and between documents, can point to whether their measures are cohesive with one another, indicating cooperation or similar perspectives, or whether they clash with each other, or are broad in their approaches. The following paragraphs will outline some of the findings reached based on the previous analyses.

Who/what are the threats? From the statements, reporting, and wording of the documents analysed, we can understand that, while addressing the issue of Russian disinformation at large, there is a focus put on the presence of bots on social media, as well as fake news coming from state-owned Russian media. This indicates a threat perception in terms of misleading news reaching the local audiences, as well as fake accounts amplifying the reach of these.

What measures is the government taking and prioritising to address these? At what level or sector? When taking a careful look at the multitude of measures listed by Spain within their ‘National Action Plan Against Disinformation’ (BOE 292, 2020) we can observe almost exclusively the mention of EU-level approaches. Ranging from cooperation, to election-specific measures, and passing through social media regulation and societal ones, we can see the great amount of institutional action taken by the European Union to tackle the threat of disinformation. It can be safely assumed that the threat perceived is more prominent at the regional or European level, than merely at the
national one. Particularly, within the measures mentioned by the Spanish government, a majority of focus is set to the areas of European cooperation, organisational, and societal methods.

What do these answers say about the country and its security strategy? From the large pool of data, as well as the answers above, it can be concluded that the level of trust and commitment from the Spanish government on the effectiveness of the European Union is undoubtedly large, and by extension that of its citizens. No public or news coverage at the state level shows any disdain or dissatisfaction from the public with the severity of measures taken. Furthermore, seeing the majority of actions being concentrated in the field of EU cooperation and transparency, organisational measures, and societal measures indicates a great effort on the institutional front to put in place the correct mechanisms to tackle disinformation, while also focusing on the citizen’s resources and ability to continue this fight against disinformation in individual circumstances.

The transparency and trust vis-a-vis the EU, at least in comparison to other multilateral organisms, means that a large focus on action at this level will not raise concern or suspicion within the Spanish people, who are rather accustomed to their state ‘conforming’ to EU legislation. In this instance, it can be argued that Spain chose to act in a ‘logic of appropriateness’, upholding norms and maintaining its legitimacy (Baylis, Smith, and Owens, 2020: 198). And, even to the lesser extent that distrust in the government or the European Union might be present, these are addressed by the emphasis on societal measures of increasing media literacy, and political transparency.

Overall, the findings point to the idea that Spain and Spaniards’ status as European plays a large role in explaining both why these were the measures opted for, and why they were thought of as the most likely to prove successful. Identity, as the theory of Constructivism dictates, cannot be detached from the social world, even in situations of conflict (Dunne, Kurki, and Smith, 2016: 165). This is an idea that can be related both to their European identity, as well as the formed-identity of Russia as a threat to Europe. Taking on a more national-level approach, as that of Brazil, would have entailed a more limited access to resources, as well as potentially lead to a rise in concern, within and beyond the nation, about the shying away from the great tool that the EU and European Commission often provide for dealing with foreign threats, particularly Russian ones.

4.3.2 Brazilian general elections of 2018

For the case of data from Brazil, we can once again highlight the importance of context. While the Brazilian approach appears as a straightforward answer to the issue at hand, we can perceive their social context taking an important role in dictating the measures taken. Observing the themes that keep coming up, as well as those never mentioned or addressed, insight can be gained into the country’s international standing, in terms of cooperation with other nations, as well as what their
specific focus or perception of disinformation consists of. These ideas help answer the research questions introduced by this study.

Who/what are these threats? The large amount of importance placed on the regulation of digital platforms, particularly social media and private messaging, align with the recurring theme in Brazilian news and official communications. These are known to place blame on fake accounts, bots, and mass content-sharing through WhatsApp message chains for the widespread beliefs in false information about the electoral process, the ‘controversial’ electronic vote system, and politicians. In this understanding, we can observe a perception of threat on the information itself being spread, the media channels it is spread through, and the gullible nature of those spreading it. Less emphasis is placed on the origin of the fake news themselves, but rather more on the tactics used to increase its reach, such as bots or mass-firing of content.

What measures is the government taking to address these threats? And at what level or sector? A large majority of measures can be noted within the category of societal measures, and social media companies and online platforms regulation, with open communication and cooperation within the government taking the third place. In the case of Brazil, and their response to disinformation, we can see a shift from the Spanish multilateral and regional approach, to strictly governmental and national measures, with collaboration being highlighted with bodies and even private companies within the state, urging these sectors of government, or those allied with it, to take action.

No information on measures taken by international or multilateral organisations in which the country participates, were available and I am not aware of any classified or non-publicly available ones either. This information might point to the dichotomy between an organisation such as Mercosur, and a union such as the EU. Brazil’s status, both in geographic and economic terms, within Latin America, means that it has little benefit to gain from its neighbours’ material, technological, and intellectual resources. Instead, it sets its focus on increasing and improving these aspects of its nation in order to address the issue internally. We can see in this answer, how Brazil also acted according to a ‘logic of appropriateness’, making use of the ‘best’ resources at their disposal to achieve a collective, rather than individual interest (Dunne, Kurki, and Smith, 2016: 164).

What do these answers say about the country and its security strategies? In a country with high rates of corruption and little trust in the government or its officials, the state has considered it imperative to focus its efforts on the societal aspect of the issue as well. Emphasising the importance of media literacy, education, and the resources for fact-checking, even through third parties that, while collaborating, will not be immediately associated with the government, has the goal of increasing civil society’s role in being armed to fight disinformation in their daily lives, even in spite of their potential distrust of the government.
4.3.3 Mexican general elections of 2018

For the case of Mexico, very limited action has been taken, and perhaps even less is that which is available and has been analysed. As mentioned before, however, the omission of information can also point towards answers when it comes to the analysis of texts and their content, and it is a large part of what has been looked at for answering the research questions posed.

Who/what are the threats? As indicated by their limited measures, and ‘corroborated’ by the research previously mentioned, we can see a limitation of threat perception to the act of fake news spreading, particularly through deceiving news articles. However, a threat perception could also be highlighted in their fear of free-speech violations, and its reflection on their largely absent regulatory measures. As mentioned by the Human Rights Commission of Mexico City (2021: 3), a risk of violating people’s freedom of speech is a recurring topic when discussing the extent of measures that can and/or ought to be taken by the government.

What measures is the government taking to address these threats? And at what level or sector? Emphasis can be seen as placed solely on the category of societal measures, an action which is in line with the political and institutional discourse highlighting the risk of interfering with free speech or addressing questions of censorship. Within the measures that are available for analysis, however, a focus can be seen on the brief attempt at media or cyber literacy, as well as various efforts at fact-checking tools for public use. These actions can be seen both at the government level, though briefly, and at the civil society level, which does not directly relate to the research at hand.

Despite being immediate neighbours, and often allies of the United States, no public measures have been taken in collaboration with their northern counterpart to fight the threat of disinformation that the US is so quick to call out. While an odd idea, considering the quickness to take action observed from other nations, this could be a reflection of the famously American idolisation of free-speech as a pillar of liberal democratic societies - though arguable when looking at their literary censorship measures, that is ever influencing media worldwide.

What do these answers say about the country and its security strategy? The most successful of the measures taken, ‘Verificado 2018’ and ‘El Sabueso’, are notably not government led or sponsored actions, but rather a collaboration of private media companies and the work of a single news outlet respectively. Their success can be claimed to be linked to the general public trust in their functioning and unbiased-ness. As for the governmental equivalent, ‘Verificado-Notimex’, we can see hesitancy and even negative responses towards its implementation, though it is hard to establish whether this is a result of its alleged plagiarism or of the general untrustworthy-ness of politicians in Mexico, if not a combination of the two.

The famously Latin American trends of corruption and distrust in public authority and politicians that was already highlighted in the case of Brazil, can be reconsidered for Mexico’s case.
Though, while the Brazilian government chose to attempt and legitimise their measures as much as possible, Mexico opted for refraining from action altogether. This can be perceived as an action in ‘logic of consequences’, where the risk of censoring free speech was weighted as a greater cost than the benefit of tackling disinformation through more extensive methods (Baylis, Smith, and Owens, 2020: 198)

4.5 Three types of actors

Without claiming that the three case studies selected act as accurate representatives of all states globally, it can still be seen how their individual and distinctives approaches to fighting disinformation makes them into representatives of different types of actors internationally. This a useful categorisation to have, if future work were to be done to extend the scope of this thesis’ research. Studying external case studies other than the ones at hand, may be aided by an already existing understanding of the possible types of measures taken by states, as well as the circumstances that may relate to their selection. Such a division is made possible in this work because of its comparative nature, which allows one to observe how the case studies differ from each other, and which characteristics are general or unique to each nation’s context.

In this study case in particular, I have found that Spain acts in this regard as an agent for international and multilateral cooperation, while Brazil takes on a more nationalist role of independent cooperation, and Mexico opts for a more Libertarian perspective on government action and regulation, meaning little to none. I will elaborate on these three ‘examples of’, as classified by myself, in the next subsections.

4.5.1 The international cooperator

Spain’s response to Russian disinformation during the 2017 Catalan-Independence referendum is hereby taken as a case example of an actor who takes on the role of international cooperator. What this entails is that their national security strategy heavily, if not exclusively, relies on the work of multilateral organisations, namely the European Union. As noted in Spain’s outline of measures, both in the Appendix and in the previous analysis boxes (Box 1 and 2), a strong reliance on European-wide action is present, and no independent national strategy is mentioned.

There are various characteristics from this nation that align with its security strategy. For once, a strong European identity is present, which points to the idea that regional homogeneity, to some extent, is necessary for this type of actors. One could also highlight the historical role that EU cooperation plays in dictating this collaboration: for a nation to continuously be supported by a union of this sort on a variety of different state issues means that their default route when new problems or threats arise would logically be to once again look towards this actor for help.
For an international-cooperation actor to be possible, a decent level of trust, on behalf of the population, must be placed on the body taking charge, but also on the government relaying the problem to them. Delegating a matter of security to an entity beyond the state showcases a recognition of its better position in terms of resources: technology, time, and experts; and doing so without push-back from the general public indicates their satisfaction with previous decisions and actions by said entity.

Overall, it is simple to see the benefits that may come from multilateral cooperation if the context is right; I find it reasonable that Spain would opt for this approach, given its geographical and political context as innately European. However, I can also see how other states, without such a strong regional alliance or shared identity, may not find this path ideal. Whether a state has nothing to gain from its neighbours in terms of capacities, as is the case of Brazil, or is in a weaker position that its neighbours, making it harder to establish collaboration when one has more needs from the other than what they can offer back, which is the case of Mexico (and its northern neighbour: the US), it can lead a nation towards other frameworks for decision-making and action-taking.

4.5.2 The state-level actor

The case of the 2018 Brazilian general elections, and the Russian disinformation campaigns that infiltrated it, acts as an example of an actor which chooses to maintain its measures at the state-level, contrary to the Spanish international approach. What this means is that the decisions are largely made by the government itself, and their focus is put to nation-wide efforts in the fields they perceive as most urgent or useful to address. For the case of Brazil, these can be noted to be: transparency and collaboration within different bodies in the state, societal measures, and regulatory ones.

Their election to opt for this type of approach can be explained, as previously, by a lack of membership in strong international institutions. Brazil is not currently part of any alliance taking on political or legislative roles, but rather only economic agreements, which translates into their action being, for the most part, at the national level. While a national approach may seem like a viable tactic for many states when it comes to security threats, Brazil faces the unique condition of having a politically divided population with a strong distrust for the government. This means that, while they do take on the role of state-level actor, they have a need to shape this strategy so as to be able to maintain legitimacy with the public, enabling their measures to reach and be effective with as many people as possible.

Within the measures taken by them and outlined previously, we can highlight some characteristics which correlate with their contextual sphere. Particularly, one can highlight their recurring emphasis on collaboration with private actors and companies. When measures and messages come from an actor other than the state, though perhaps in collaboration with, this gives them an
increased sense of credibility with the public, given that private entities having an interest in manipulating the political information people consume does not tend to be such a large concern.

Furthermore, taking regulatory measures in the form of laws and justice to assure the transparent working of digital platforms, is a way in which people can be less exposed to disinformation altogether, in spite of their political beliefs and affiliations. Finally, addressing the issue of media literacy, through educational programmes at various degrees, makes for a future generation that faces news and other informational messages more critically, allowing for work to take place both at the individual and the collective level.

While a state-level of action, combined with the necessary measures for success with a sceptical audience, may prove as a useful approach for a nation such as Brazil, other nations facing similar challenges of political distrust and infamously corrupt leaders chose to take on different routes, such as Mexico has.

4.5.3 The inactive spectator

The case of Russian election meddling in the 2018 Mexican general elections provides us with an example of an inactive actor, which despite the contradiction is an accurate descriptor. What this role, which I have also referred to as the spectator, entails, is that the state opts to refrain from action as their main security strategy. For one reason or another, the government considers that taking measures at a large scale, be it regulatory, organisational, or cooperative, has the potential to bring more harm than good to the situation at hand.

In this particular case, we have a clear indicator of where this concern lies, in various mentions of worries for violating free speech rights, as well as censorship of public opinion in media coverage. Subsequently, we can barely see action taken by the government against disinformation, but rather a focus on media literacy; instead of addressing the threat of disinformation, it seems that the Mexican aim is to arm its citizens against it, though the measures for this remain limited.

While certain nations and their population may appreciate the respect for liberty given by these types of government actors, there are certain indicators in my analysis that point against this. The mere fact that private news channels and media companies came together to create a publicly accessible tool for fact-checking already speaks loudly to the extent of the issue, as well as the need for more extensive action. On top of that, the positive response from the public, making use of and trusting these novel reliable sources, shows a general leaning towards awareness of the presence of disinformation, as well as a seeking of measures against it. Whether the same people would be willing to accept these measures, and more, if they were to stem from governmental action, is a harder question, which I am not willing to stipulate on without more data to base such predictions on.
While this type of actor is not necessarily the one to be expected in democratic states, where protecting said democracy and its legitimacy is an overarching goal, it can still be seen as a reasonable selection in certain cases. When representatives have a genuine belief and worry that strong or extreme action may push an already divided political spectrum further into their sphere of government distrust, which in turn makes them more liable to believing fake news that align with their beliefs, they might consider a moderate bystander position to be the safest to take.

5. Conclusion

There are many conclusions to be drawn from the previous analyses of data and content. The substance, wording, and approach of all the programmes and initiatives above, aided this study in forming educated and evidence-based assumptions about the research questions it looked to address: How do states respond to cyberthreats coming from abroad? Who/what are these threats? Social media, fake accounts and bots, mass-firing of false messages, or other factors? What measures are governments taking and prioritising to address these threats? At what level or sector of governance? What circumstances play a role in guiding the approach taken? And, last but not least, what do these answers, and their level of success, say about these countries and their security strategies?

Overall, what the individual indications from each nations’ response mechanisms and tactics, and their subsequent implications, have shown is that, as previously stipulated along the lines of Constructivist theory: matters of social, political, cultural, and even historical, context can play a huge role in determining the path chosen by a state. Reality, and any circumstances within it, cannot be understood as static, but rather need to be observed through the lens of the particular time, place, and actors involved in it. In confirmation of this idea, it can be seen how Brazil, Mexico, and Spain, while all facing a virtually identical threat to their democratic functioning through disinformation, took on various different approaches, at a multitude of levels.

Through the relevant securitisation theory, we can also observe the different referent objects as indirectly indicated by each nation’s policy: Spain opting to protect European democracy and its integrity, Brazil opting to protect its national democratic functioning, and the ability of their citizens to remain well-informed, and Mexico prioritising the protection of free-speech over taking any significant action against disinformation.

The method of comparative and content analysis has allowed for this study to be based on formal sources outlining the measures taken to battle disinformation, and also for their objective analysis, which has led to viable answers to the research questions presented, attained through logic and reasoning. Throughout the different sections of this thesis, a clear overview of the phenomenon
of disinformation is given, ranging from what and how previous research has addressed and approached the issue, to how different countries have come to do so themselves in recent years.

While the extent of success for each case study is hard to define, and will be probably facilitated once more time has passed since their most recent elections, it can also be noted that success in terms of fighting disinformation was not their only aim, but also that of maintaining a decent level of credibility and, legitimacy for the government, politicians, and overall democracy of their state.

I can confidently state that, throughout this thesis, a comprehensive analysis has been followed, and has led to answers relevant to the research question, as well as to the gap present in the previous work in the field. The research at hand, studying the responses to information warfare and its implications and context, can prove of great use in the field of International Relations, particularly when studying cyber threats, or conducting policy analysis and recommendations, but also as means of providing tools to improve the reliance of democratic systems, and their resistance to threats attempting to disrupt their order. More broadly, it is a field of study that can contribute to matters of global governance, conflict, and democracy. Lastly, I believe that a continuation of this line of study, particularly at a larger scale, would prove very effective in shining a light on the issue of disinformation, as well as educating individuals, governments, and institutions on how best to address it.

[13.115 words]
6. Bibliography


Others/Comision-de-Derechos-Humanos-de-la-Ciudad-de-Mexico.pdf (Accessed on: April 24th 2023)


Appendix

This section encompasses the following materials:

- ‘Procedimiento de actuación contra la desinformación’ [translated to: ‘Action procedure/plan against disinformation’] (BOE 292, 2020)
- ‘Action Plan Against Disinformation’ (European Commission, 2018)
- ‘EU Code of Practice on Disinformation’ (European Commission, 2018 (2))
- ‘Report on the implementation of the Action Plan Against Disinformation’ (European Commission, 2019)
- ‘European Democracy Action Plan’ (European Commission, 2020)
- ‘Social Observatory for Disinformation and Social Media Analysis’ (European Commission, 2022)
- ‘Rapid Alert System’ (European Union, 2019)
- ‘Programa de Lucha Contra la Desinformación’ [translated to: Programme for the Fight Against Disinformation] (Peres Osorio et al, 2022)
- ‘Projeto de Lei No. 2630’ [translated to: Bill (lit. Law Project) No. 2630] (Vieira, 2020)
- ‘Decreto No. 10.222’ [translated to: Decree No. 10.222] (Decreto No. 10.222, 2020)
- ‘Ciberguía’ [translated to: Cyber-guide] (Gobierno de México, 2022 (2))
- ‘Cuestionario de Consulta del Relator Especial de la ONU sobre Promoción y Protección del Derecho a la Libertad de Opinión y Expresión’ [translated to: UN’s Special Rapporteur’s Consult Questionnaire about the Promotion and Protection of the Right to Free Speech and Opinion’] (CDHCM, 2021)
- ‘Verificado 2018’ (Verificado 2018)

The following sub-headings provide a detailed outline of the full extent of measures taken by each state following the information attacks against their democratic elections. Being each sub-divided into the categories of action as previously stipulated in the Methodology section, this Appendix offers an extensive description of the approaches as summarised by Boxes 1 and 2 of my analysis.
6.1 Catalan-Independence Referendum of 2017

Following the Russian intervention in the “illegal” Catalan-Independence Referendum of 2017, various measures to defend themselves from the future threat of disinformation campaigns can be seen from the Spanish government, as well as the European Union it is a member of.

6.1.1 Transparency and cooperation with other (EU) governments

Certain measures taken by the above mentioned institutions were aimed at the enrichment of intra-European cooperation and transparency, with the belief that such actions would lead to a more well-rounded and cohesive defence mechanism against future disinformation.

The ‘Action Plan Against Disinformation’, as introduced by the European Commission and EEAS, encompasses a significant pillar in this regard: Pillar 2 (European Commission, 2018: 6-7). With the goal of “strengthening coordinated and joint responses to disinformation”, this point proposes the establishment of a ‘Rapid Alert System’, which will target disinformation campaigns by utilising present networks between NATO, G7’s Rapid Response Mechanism, and the European Parliament (Action 3); increasing and/or improving communications regarding Union values and policies (Action 4); and emphasising strategic communications with those neighbouring the EU (Action 5) (Ibid. 8). The ‘Rapid Alert System’, in particular, is meant as an open-source of information, sourcing from fact-checkers, academia, digital platforms, and other international partners, and meant for EU institutions and Member States to share insights and coordinate responses (European Commission, 2019: 3; and European Union, 2019: 1). Its intended outcomes include but are not limited to: i. Public information and awareness raising activities; ii. Flagging serious cases to online platforms; iii. Empowering researchers, fact-checkers and civil society; iv. Coordinated response; and v. Coordinated attribution (European Union, 2019: 1).

As for the ‘European Democracy Action Plan’, its measure 2.3: “Strengthened cooperation in the EU to ensure free and fair elections” also speaks to the same cooperative-centred approach (European Commission, 2020: 6). In terms of specific action it calls for certain measures relating to the EU, including the set of joint support mechanisms for cooperative work with the ‘European Cooperation Network on Elections’, regarding the election processes and infrastructure against cyberthreats, improved cooperation on the fair and even treatment of media coverage during elections, and the bettering of cooperation between networks, both from the European Union, and other partner countries and organisations, to share insight and create the highest possible standards for actions against electoral threats (Ibid. 8)

6.1.2 Organisational measures
Within the same documents as previously mentioned, some organisational actions are to be highlighted as well.

The ‘Action Plan Against Disinformation’s Pillar 1: “Improving the capabilities of Union institutions to detect, analyse and expose disinformation” is one instance of this (European Commission, 2018: 5). This pillar calls for action in respect to strengthening the Strategic Communication Task Forces, as well as Union Delegations, by incorporating an increase of staff, and tools, necessary to ‘detect, analyse, and expose’ disinformation activities (Action 1); and to review the mandates by the same forces for the Western Balkans and South regions, permitting them to approach the issue of disinformation more effectively (Action 2) (Ibid. 6).

The ‘European Democracy Action Plan’ takes on organisational measures of its own in the instance of paragraph 4.1: “Improving EU and Member State capacity to counter disinformation” calls for action regarding institutional capacity instead (European Commission, 2020: 19-20). They mention objectives along the lines of developing the EU’s abilities in terms of countering foreign influence operations, through a comprehensive toolbox, new protocols, a cohesive framework, and support for the different actors. They emphasise the importance of these measures for improving cooperation structures, collecting evidence, holding dialogue, and building the capacity of EU institutions, civil society, private industry actors and other relevant stakeholders, as well as those same sectors abroad (Ibid.).

The ‘Social Observatory for Disinformation and Social Media Analysis’ (SOMA) is a project that was carried out in the period between 2018 and 2021, with the aim of mapping European social media and developing a Source Transparency Index (European Commission, 2022, 2). It proposed the creation of an online content-verification platform offering fact-checking, as well as social media mapping and visualisation tools. It also intended to develop a process to assess the socio-economic impact of disinformation, and target this by creating strategies and action plans to increase aspects such as media literacy. Its utility goes beyond that of aiding civil society, but also extends to providing policy recommendations based on its collected information and analysis, creating a repository of disinformation-related knowledge, and developing further tools for community-mapping for a future hyper-connected society (Ibid.).

6.1.3 Social media companies and online platforms

Multiple plans of actions aim to take on the issue at its root, and given that a large part of disinformation is created and spread through social media and other online platforms, their regulation is a point of interest in fighting these threats.

The ‘Action Plan Against Disinformation’ briefly touches on this issue in its Pillar 3: “Mobilising the private sector to tackle disinformation” (European Commission, 2018: 8). In it, a
voluntary ‘Code of Practice’ on disinformation is presented, which states the Commission’s responsibility to monitor its implementation (Ibid. 9). The ‘Code of Practice’ lists multiple commitments from the signatories, in efforts of countering disinformation in their networks:

II.A. ‘Scrutiny of ad placements’ deals with the restriction, fact-checking, and verification of ads, as well as the user(s) and or companies paying for them
II.B. ‘Political advertising and issue-based advertising’ takes on matters of transparency and distinction of political and issue-based advertising
II.C. ‘Integrity of services’ tackles the question of fake accounts or bots and their regulation to ensure they cannot be mistaken for human users
II.D. ‘Empowering consumers’ outlines matters of freedom of speech and potential censorship of content, the facilitation of diverse news sources representing alternative perspectives, and accessible ways of reporting disinformation. On top of this, it discusses user transparency, in the means of open information regarding one’s targeting of political or issue-based advertisement
II.E. ‘Empowering the research community’ considers the ability of accessing data for fact-checking and research purposes, in a way that complies with privacy measures

III. ‘Measuring and monitoring the code’s effectiveness’ emphasises the need for annual reports and follow-ups from the signatories, in order to assess and maximise the utility of the Code

(European Commission (2), 2018: 4-8)

The ‘European Democracy Action Plan’, as well, addresses the topic of social media companies and online platforms in two instances. Its Paragraph 3.4: “Additional measures to support media pluralism” calls for action in the sphere of media transparency and diversity (European Commission, 2020: 16) by setting goals such as the creation of a ‘Media Ownership Monitor’ for greater transparency in the area, the implementation of transparent measures for the fair allocation of state advertising, and the brainstorming of viable action to take towards media diversity, among others (Ibid. 17).

Section 4.2: ‘More obligations and accountability for online platforms’ (European Commission, 2020: 21). In it, it calls for action on the sole matter of guiding and strengthening the previously mentioned ‘Code of Practice on Disinformation’ during the year 2021, pushing its signatories to do so as well, and setting up a more permanent framework for its monitoring (Ibid. 23-24).

6.1.4 Societal measures
On top of focusing on the issue of disinformation’s source, action is also taken in regards to its targets, who, as well as states largely, are mainly their citizens, whose votes are being sought to influence.

The EU has taken to this through different means, of which is worth mentioning the *European Media Literacy Week* (European Commission, 2019: 2). This event consisted of a combination of panels, lectures, and workshops, held physically as well as streamed online, and aimed at reinstating the importance of media literacy, as well as sharing the various professionals’ perspectives on it (Deutschland sicher im Netz, 2022: 2).

The ‘*Action Plan Against Disinformation*’ also takes on societal measures in its Pillar 4: ‘Raising Awareness and Improving Societal Resilience’ (European Commission, 2018: 9). In this final section, the plan calls for action within the matters of: the organisation of targeted public campaigns and media trainings in the EU and its ‘neighbourhood’ (Action 7); the support for researchers with knowledge on the topic, and teams to create independent and multi-disciplinary fact-checkers, to then be able to detect and expose disinformation campaigns in different media (Action 8); and the support of cross-border cooperation between media literacy professionals, and the launching of tools to promote this literacy to the public (Action 9) (Ibid. 11).

The ‘*European Democracy Action Plan*’ itself, also addresses the topic of society and its role in fighting disinformation. Paragraph 2.4: ‘Promoting democratic engagement and active participation beyond elections’ looks to foster involved citizens in the political process, beyond the interest of election periods (European Commission, 2020: 8). The section calls for action through its objectives, which include the use of EU funds for purposes of civil society, and the building of capacity and infrastructure to increase and promote their engagement and political participation. The section also calls for the use of EU funds towards efforts to create opportunities for the youth, citizenship education, and impulse the work of the Creative Europe Programme and the equality agenda, fostering access to participation in the democratic process, as well as trust in its institution (Ibid. 11)

Furthermore, paragraph 4.3: ‘Empowering citizens to make informed decisions’ touches on the topic by suggesting the support for new innovation looking to fight disinformation, through EU programmes such as those by civil society organisations and higher education institutions, as well as calling for increased support and funding of more diverse initiatives that aim to promote media literacy for citizens to be able to recognise disinformation, both in the EU and abroad (European Commission, 2020: 25).

The final actor to take on a societal measure in this regard was NATO. While not necessarily related to the issue of election meddling per se, the organisation took on the role of fact-checker to disprove disinformation about Russian hybrid threats, particularly relating to the Russia-Ukraine
conflict. For this purpose, it has introduced a programme titled “Setting the record straight”, where myth and false news or information are debunked for the general public to access (NATO, 2022).

6.1.5 Election-specific measures

The fifth and final line of approaches that the Spanish government has taken, itself or through the institutions it takes part in, are those that had elections specifically in mind, and the threat that disinformation poses on these.

The ‘European Democracy Action Plan’ references this idea on two occasions. Firstly, there is section 2.1: ‘Transparency of political advertising and communication’, where it proposes legislation for greater transparency in terms of sponsored political content or ‘political advertising’ to be implemented in 2021, as well as the measures of support and guidance for Member States and political parties within the Union (European Commission, 2020: 4-5). And secondly, section 2.2: ‘Clearer rules on the financing of European political parties’, in which the proposition is to revise Regulation No. 1141/2014 that deals with the statute and funding of European political parties and foundations, in the year 2021 (Ibid, 5-6).

6.2 Brazilian general elections of 2018

When it comes to the Brazilian line of action, in regards to the threat posed by foreign disinformation campaigns on their electoral system, we can see an exclusive leaning towards governmental level of action, rather than having input from other international or regional organisations.

6.2.1 Transparency and cooperation with other governments

While outside interaction or action is not a main focus point of Brazil’s tactics to counter disinformation, we can observe one instance in which this type of approach is mentioned. In ‘Decreto No. 10.222’ point 2.3.8, a mention is made of expanding Brazil’s international cooperation in cybersecurity (2020: 7-8). With emphasis on transparency, the state looks to establish itself as “constant seeker of peace and international security”, and doing so while cooperating with “as many countries as possible” (Ibid. 8). Among the measures it lists to do so, the decree includes stimulating international cooperation and participation of Brazil in matters of cybersecurity in international forums or groups, events and/or training exercises, agreements, international mechanisms, future initiatives, and commercial opportunities. It looks to push and promote international relations in Latin America and beyond, with a particular intent of sharing and gaining insight and support in its fight against disinformation and cybercrime (Ibid.).
6.2.2 Open communication and cooperation within the government

Similarly to the idea of international communication and cooperation, we have that of open communication at the national level. Given its size, and the large number of institutes and bodies that constitute the Brazilian government, it is no wonder that they require special and explicit measures to ensure open and successful communication and cooperation within itself.

The permanent ‘Programme for the Fight Against Disinformation’ tackles this question in multiple instances. For starters, two sections of its National Strategy make mention of approaches to address national communication efforts (Peres Osorio et al, 2022: 34). The first stage of national integration of the Electoral Justice: ‘Institución’ [translated to: Institution] states how the Tribunal Superior Eleitoral (TSE) [translated to: Superior Electoral Court] is to stimulate the Regional Electoral Courts (TREs) that are unable to face disinformation through their own means and structures (Ibid.). The third stage, as well, named ‘Diálogo y monitoreo continuo’ [translated to: ‘Continuous/Constant Dialogue and Monitoring’] talks about an open means of communication with the agents assigned by the TREs to guarantee fast and clear dialogue between the bodies in the Electoral Justice, including the holding of periodic meetings (Ibid.)

The same document references intra-governmental communication in other sections. Project 5 of Axis 2: ‘Cooperation and actions to increase the reach of media and informational literacy initiatives by collaborating entities’ [translated] has as its goals that of discussing, with media and information literacy institutions wishing to collaborate with the programme, strategies to expand the reach of initiatives, specially during the periods of elections; and implementation, with this same institutions, of said strategies to achieve this goal (Peres Osorio et al, 2022: 53).

Project 7, from the same Axis: ‘Support of other electoral bodies and public institutions to implement actions against disinformation’ [translated], sets its objective to coordinate the dialogue between courts and national bodies, through workshops, meetings, and other forms of communication, as well as the dialogue with electoral bodies in other countries, with the aim of fighting disinformation (Peres Osorio et al, 2022: 54).

Project 5 from Axis 3: ‘Partnership and dialogue with the Federal Police (PF) and the Electoral Prosecutor’s Office (MPE)’ [translated] looks to increase collaboration with the Police and Judicial sectors of government (Peres Osorio et al, 2022: 59). It proposes, to do so, measures including the allocation of fixed agents from the PF and the MPE to represent their bodies’ participation in the aforementioned programme. These agents are then intended to maintain fast and continuous virtual communication and dialogue with various other government sectors to facilitate and speed the referral of criminal cases received by the Electoral Justice (Ibid.)

6.2.3 Organisational measures
As with other states, we can expect Brazil to opt for some measures in terms of organisation in its effort to fight disinformation. The very same document that presents the ‘Programme for the Fight Against Disinformation’ takes on this approach within its scope.

Project 6 of Axis 3: ‘Strategic Committee of Cyber Intelligence’ [translated] sets as part of its goals the establishment of networks with companies in the field of technology and infrastructure, to contribute towards cyber intelligence strategies in election periods; developing operations with planned action to take in case of cyber attacks, and security systems, as well as trainings on data leaks, phishing, and other cyber-intelligence risks (Peres Osorio et al, 2022: 60).

Project 7, from the same Axis: ‘Revision and setting of standards that counter the practice of disinformation in matters of Electoral Justice, as a way of preventing the phenomena’ [translated], sets among its objectives that of following the processing of bills dealing with the threat of disinformation (such as Fake News Bill aka Bill No 2,630), and improving their proposals when possible, following the sentencings relating to the same issue and building recompilations of these, and making sure of the participation of those managing the programme in the work groups that relate to preparing resolution proposals (Peres Osorio et al, 2022: 61).

6.2.4 Social media companies and online platforms

Given that digital platforms make up a large sector where disinformation is started and spread, it is not surprising to say many of Brazil’s measures to fight disinformation are present within this sphere.

The ‘Bill No 2,630’ is the first document in which we can find these. Article 10 from Section III: ‘About the Measures against Disinformation’ [translated] lists a couple of practices relating to the good regulation of social media content: the use of verification from independent fact-checkers, disabling the option of sharing (disinformation) content to more than one user at a time, labelling disinformation or false content as such, and assuring the delivery of verified information to those users reached by the false content, among others (Vieira, 2020: 6-7).

Section IV of the same bill: ‘About the Private Messaging Services’ [translated], includes various articles of relevance (Vieira, 2020: 7). Article 13 urges providers of such services to limit the number of recipients of one same message to five users or groups, with each group having a maximum of 256 members, as well as dictates that during electoral periods, or situations of public emergency, this number be limited to one user or group (Ibid.). Article 14 states the need for a user to declare whether the account will be managed by an artificial user or bot, and delete the accounts that fail to do so (Ibid. 7-8). Article 15 incorporates the need for permission from a recipient to be requested before delivery of mass messages or communication, even through a group (Ibid. 8). And finally, Article 16 dictates that the providers of apps that provide messaging services, must utilise all
resources possible to limit the spread, as well as to the presence, of false content and/or disinformation (Ibid.).

Article 28 from Chapter V of the same bill: ‘About the Sanctions’ [translated] once again addresses the issue of social media companies and online platforms, dictating the sanctions in place for those that were to violate the Bill. These start from a warning, which includes an indication of the period of time allowed for adopting corrective measures, moving up to a fine, then to a temporary suspension of activity, and finally the full prohibition of activities in the country (Vieira, 2020: 10).

Axis 3 of the ‘Programme for the Fight Against Disinformation’: ‘Reponse: Identification and content of the disinformation’ [translated] deals with the topic of online media and companies in 3 of its projects.

Project 1: ‘Permanent Coalition for the Verification of facts’ [translated] sets among its objectives to reunite with fact-checking institutions to discuss the challenges of disinformation, and reach a permanent cooperation agreement, setting in place a shared network, and eventual supply of information on the election process. The intention is centred on promoting the dialogue between these institutions and internet app companies collaborating with the programme (Peres Osorio et al, 2022: 55).

Project 2 of the same Axis: ‘Commitment of the digital platforms and their technological resources to face the structural networks of disinformation and inauthentic behaviour’ [translated] deals with aims to regulate and improve the functioning of internet app companies allied to the programme, as well as those that are not (Peres Osorio et al, 2022: 56). It proposes to do so by promoting dialogue to invite more companies to support and potentially join in on the programme’s purpose, establishing specific initiatives and measures agreed upon, to aid during and beyond the electoral year. The project also suggests the improvement of civic integrity policies from these very companies, through content moderation rules, and a clear-cut protocol of action to fight inauthentic behaviour looking to post and spread coordinated deceiving information about the electoral process. It supports the adoption of an action protocol for urgent cases of disinformation, grave enough to compromise an election. The section emphasises the importance of transparency with the general public and researchers, in terms of the application of these different measures on their platforms, and with the government, in terms of sharing periodic statistical reports on disinformation cases (Ibid.)

Finally, there is Project 3 of the same Axis: ‘Channel for reports against mass-firing of content in collaboration with WhatsApp’ [translated]. This establishes the goals of creating an electronic form for citizens to report mass content-firing, and improving the functioning of the existing one with a ticket system, as well as ensuring that its use and message is spread in an extensive and anticipated manner so as to work as effectively as possible (Ibid.)
6.2.5 Societal Measures

Beyond focusing their efforts in government-limited measures, Brazil opts to take on approaches that emphasise the role of society in fighting disinformation. We can see this in multiple of the documents under analysis.

The ‘Decreto 10.222’, in its section 2.3.10: ‘Raise society’s level of maturity in cybersecurity’ [translated] aims to do this so as to teach the risks and threats present in the digital sphere (2020: 8). To do so, it considers the idea of including matters of cybersecurity in the basic education (infant, elementary and middle educations), including the ethical use of information, as well as proposals to stimulate graduate and post-graduate programmes on cybersecurity, promote research on the topic, create training programmes for both private and public sector professionals, and promote the country’s participation in national and international forums and events on cybersecurity. With these aims, it attempts to improve integration, collaboration, and incentive between universities, institutes, research centres, and the private sector in relation to cybersecurity (Ibid.)

The ‘Programme for the Fight Against Disinformation’ also tackles the issue of society. Namely, Axis 1: ‘To Inform - Spread quality information’ [translated] deals with the topic in five of its projects.

Project 1: ‘Network for the massive spreading of truthful and official information about the elections and electoral process’ [translated] lists among its goals ideas such as developing alliances with internet app companies, civil society entities, and other public personalities, while also creating new digital communication infrastructure, and a network for both citizens and public institutions (Peres Osorio et al, 2022: 42-43). These objectives are meant to aid in the establishment of new measures for the spreading of accurate and trust-worthy information regarding the election process, while warning about disinformation (Ibid.)

Project 2 of the same Axis: ‘Chatbot - Questions and Answers on electoral matters on WhatsApp’ [translated] takes on the task of informing and providing fact-checking tools to the general public (Peres Osorio et al, 2022: 43). Among its aims, it discusses the maintenance of a Chatbot (in collaboration with the private messaging platform WhatsApp) which was introduced during the 2020 midterm elections, and whose results proved to bear positive impact in the general public. The aim is for the tool to be active both during and outside of election periods. The project also discusses its improvement in terms of updated language processing abilities, expanding from information and services to include media literacy training, and finally work on the expansion of the audience it reaches (Ibid.)

Project 3 of the same Axis: ‘Access, diffusion, and empowerment of the reach of fact-checking on the electoral process’ [translated] once again brings about topics of societal measures. Among its objectives it argues for measures of improvement of the, already existing, ‘Fato ou Boato’ [translated
to: Fact or Rumor] page. Among potential measures they discuss the integration with the WhatsApp chatbot, a new system of tagging for better organisation and smoother searching of information, links for easier sharing through social media, and lastly, creating agreements with mobile phone companies to allow more users to access the fact-checking and information posted on the Court’s page, free-of-charge (Ibid.).

Project 5 of the same Axis: ‘Development and improvement of technological tools and digital channels to spread quality truthful information’ [translated] addresses the recurring topic of the spreading of the ‘right’ information, and the means to do so (Peres Osorio et al, 2022: 47). For this purpose, it considers ideas such as updating and maintaining an up-to-date status on official pages providing information on the various electoral processes, services, and any interruptions or instabilities of these, improving the analysis of the ‘Fato ou Boato’ page entries to better understand its practical use, and monitor aspects such as accessibility, user experience, and others, of these and more official portals (Ibid.).

Furthermore, Axis 2: ‘To train: Media Literacy Training’ [translated] touches on issues of societal measures in three of its projects.

Project 1: ‘Training of the internal public on desinformation’ [translated] lists objectives relating to the enrichment of public employees’ toolkit for dealing with disinformation (Peres Osorio et al, 2022: 49). It includes proposals that aim to promote events, training, and workshops, as well as physical pamphlets and other educational material that extends their knowledge on digital platforms, information circulating on them, and the optimal use of their services to avoid and fight the spread of disinformation (Ibid.). It furthered these efforts by mentioning other aspects of disinformation, such as inauthentic behaviour (bots), coordinated networks, and different techniques to investigate these. The project emphasises the relevance of dialogue with international organisations for the exchange of experiences and insight (Ibid.)

Project 3 of the same Axis: ‘Training for the internal and external public about the electoral process’ [translated] builds on the idea of training for preparing individuals to mistrust disinformation (Peres Osorio et al, 2022: 51). It considers measures to do so, such as promoting official speakers, as well as journalists and public agents to strengthen the institutional discourse on election processes and other legislative processes and/or changes, training them on disinformation and the tools to properly spread official factual information in its place. (Ibid.).

Finally, Project 4 of the same Axis: ‘Sensitization campaigns about disinformation and actions of media and informational education for the external public’ [translated] has the goal of raising awareness of disinformation among the external public through media and education measures (Peres Osorio et al, 2022: 52). For this, they mention their objectives to include, among others, to hold events, conferences, and campaigns on disinformation, as well as on media literacy, and democracy,
with experts on the subject (Ibid.). The project also pretends to train communicators and influencers to share content on the election process, as well as extend these contents to other means such as radio and television (Ibid.)

The last section of the Programme that targets the topic of society, and that I ought to mention is that of National Strategy point b. ‘To train’ [translated]. This presents the plan to create a workshops that deals with the past programme’s teachings (2020), as well as the planning and expectations for the current one (2022); furthermore it discusses the presentation of a playbook, on measures to fight disinformation, and alternative approaches to Elections Registries (Peres Osorio et al, 2022: 34)

6.2.6 Election-specific measures

In this final section of analysis for Brazilian policy against disinformation, we can see three final projects, whose aim is specific to the election process and the actors involved in it.

In the ‘Programme for the Fight Against Disinformation’, we have Project 4 from Axis 1: ‘Deepening of electoral transparency’ [translated], which looks to make the election process more transparent for the general public, so as to steer them away from potential disinformation (Peres Osorio et al, 2022: 46). In particular, it proposes to make use of networks, the press and other Programme collaborators, to begin an ‘election transparency cycle’ a year prior to elections, during which in is impertinent to diffuse correct and complete information on matters of urn integrity, the different election stages, and the electronic vote system. (Ibid.)

Project 6 from Axis 2: ‘Dialogue with the political parties, to sensitise them on their responsibility in the fight against disinformation’ [translated] (Peres Osorio et al, 2022: 53). In this section, I ought to highlight the mention of relevant aspects such as informing party body representatives on the topic of disinformation broadly, through organised meetings; working, along collaborating companies, to educate these representatives to be able to recognise, and prevent the spread of disinformation in these platforms; and setting a time period for the representatives’ commitment to attend the proposed events, as well as to take measures against disinformation (Ibid.).

In Project 4 from Axis 3: ‘Creation of a network to monitor the practices of disinformation against the electoral process’, we can note some further points of relevance. They describe this network as having the role of identifying and exposing election-related disinformation, as well as communicating with the TSE about its findings, proposing the adequate countermeasures (Peres Osorio et al, 2022: 57). Among its objectives, this project discusses collaboration with forensic laboratories, technology companies, and other external partners, as well as the creation of an internal ticket-system to collect findings and facilitate their report to the respective platforms (Ibid. 58). It furthers this idea into the general public, by proposing the establishment of reporting channels for citizens and other government bodies to be able to submit their own (Ibid.)
6.3 Mexican general elections of 2018

In the case of Mexico, the actions taken to counter disinformation in their democratic system is limited to societal measures, since further governmental and/or institutional approaches are not outlined. Even though this could simply be an indication of measures being kept confidential to the general public, certain statements and academic research seems to indicate otherwise.

6.3.1 Societal measures

In terms of societal measures, we can note both those taken by the government, as well as some collaborative ones by other actors.

In their ‘National Public Security Strategy Report’ [translated] the Mexican government mentions a sole disinformation-related measure of cybersecurity: the introduction of a ‘Ciberguía’ [translated to: Cyber-guide], which is meant as an informative material that, among its 14 points, addresses fake news (Gobierno de México, 2022: 163). In Point 6 of the guide: ‘Fake news’ [translated], the general public can be briefly educated on what constitutes fake news, what intentions may be behind the spread of these, and what problems can arise from their diffusion (Gobierno de México, 2022 (2): 33). Furthermore, different pieces of advice to identify this false information are provided, ranging from technical characteristics to look for, to their overall critical analysis (Ibid. 34).

The second government measure, as introduced by President López Obrador, is a fact-checking news outlet titled ‘Verificado-Notimex’, which was promptly accused of plagiarism and did not prove as useful or efficient as its predecessor.

‘Verificado 2018’, the earlier news fact-checking collaboration by Animal Político, a Mexican independent digital publisher, and other news outlets, which counted with the collaboration of various companies and social media platforms, including Twitter, Forbes México, Facebook Journalism Project, and many more, proved to be a much more well-received tool for citizens to fight disinformation and corroborate their news’ accuracy (Verificado 2018). In spite of the praise it received for its work, and the trust gained from the general public, the platform was only active during the period of election campaigns (CDHCM, 2021: 5).

Animal Político, the leading mind behind the ‘Verificado’ project, has gone on to incorporate its own news fact-checking section titled: ‘El Sabueso’ [translated to: The Hound] (CDHCM, 2021: 5). The tool allows people to submit statements made by public figures or news pieces, and then goes on to look into their veracity, to finally assign them a ranking out of eight different categories: ‘Ridiculous’, ‘False’, ‘Lying with the truth’ (truth put in a context that changes its meaning), ‘Deceiving’, ‘Cannot be proven’, ‘Debatable’, ‘Inaccurate’, and ‘Truthful’ [translated] (Animal
Politico, 2015). This project predates both ‘Verificado’ ones, and is online even outside of election periods.