LUISS

Sciences Po Bordeaux

Master's thesis

Department of Political Science
Course of International Relations
Double-degree Sciences Po Bordeaux (BIRD)/LUISS

Major : International Affairs

2020-2022

Social media: a backdoor for foreign interference in elections

A paired-comparison between 2016 presidential election in the United States and 2017 presidential election in France

Jeanne Maurin-Bonini
Matricola: 650182

Under the co-supervision of:

- Pr. Anthony AMICELLE (Sciences Po Bordeaux), Professor of International Relations, Director of BIRD.
- Pr. Michele SORICE (LUISS), Professor of Sociology of Communication at Luiss Guido Carli.
- Pr. Domenico BRUNI (LUISS), Associate Professor of History of Political Institutions at Luiss Guido Carli.

TABLE OF CONTENTS

APPRECIATIONS

First and foremost, I sincerely thank my two thesis co-supervisors Pr. Anthony Amicelle and Pr. Michele Sorice, that have both always been available for any interrogation, and that gave me great recommendations for the literature, as well as for the thesis structure and content.
I would also like to thank Pr. Matthew Hibberd for his precious reference suggestions. Finally, I have a special thought for Pr. Vincent Tiberj, my Bachelor's thesis supervisor and to our discussions that initiated the idea of this thesis.

ABSTRACT – KEY WORDS

Abstract:

The 2016 presidential election in the United States represented the tipping point in foreign interference in elections. For the first time, a foreign power (here, Russia), was considered responsible for a large-scale information manipulation campaign through social media, interfering in the American presidential elections. Shortly after, the French 2017 presidential elections also seemed to be the target of foreign interference and information manipulation on social media. These cases, along with others in the same period, raised huge debates about the protection of elections' integrity and the democratic process. This research, through the comparison between the American and the French case, aims at understanding social media's vulnerabilities, that are – partly – responsible for facilitating information manipulation, and the objectives of such operations, between favoring one candidate and disrupting democratic societies. It also presents the main responses undertaken by France, the U.S. and other non-state actors, along with potential measures that could help improve the response to this threat and deter foreign actors from undertaking this type of campaign. This research ultimately responds to interrogations regarding the utility or necessity of extended efforts, in emphasizing the scale of the threat and its potential risks for democracies.

Keywords:

Social media; cyberspace; foreign interference; electoral process; information manipulation; cyberattack; hybrid threat.

INTRODUCTION

Figure 1: Rewards for Justice – Reward Offer for Information on Russian Interference in U.S. Elections" (U.S. Department of State - Office of the Spokesperson, July 28, 2022)

Beginning of this summer (June 30th 2022), the United States' Department of State released in a press statement the following offer: up to ten million dollars will be granted by the DoS' Rewards for Justice program, in exchange for information on foreign interference in U.S. elections[1]. The offer relates to election interference activities including "*vote tampering, database intrusions, influence, disinformation, and bot farm campaigns or any type of related malicious cyber activity*", as well as information on the Internet Research Agency and its associates (listed by the FBI as most wanted individuals[2]), which activity was considered crucial in the 2016 presidential election. This reward shows first that this threat is taken very seriously by the American government, but also that information on this issue is valuable but difficult to find. Since the first accusations of Russia interfering in U.S. elections emerged in 2016, states have kept a close eye on foreign interference and feared information manipulation campaigns. Similar accusations followed regarding the French presidential elections of 2017, and in other countries. Discussions about this topic emerged in the academic sector as well as in the media or the political sphere, generating a general confusion about the terms used to describe different situations. Framing the debate with clear definitions is therefore necessary in order to avoid confusions and discuss the topic on the same grounds. In this respect, it is useful to remember that talking about fake news is not the same as disinformation, misinformation, information manipulation, and many other terms. Here we will provide elements of definition for a few essential notions of our research such as social media, and backdoor (as referring to the title), as

[1] "Rewards for Justice – Reward Offer for Information on Russian Interference in U.S. Elections" (U.S. Department of State - Office of the Spokesperson, July 28, 2022).

well as more complex and debated notions such as information manipulation and foreign interference in elections.

Although the first social media in the broad sense emerged at the end of the 1990s, such as SixDegrees.com in 1997, social media as we know them today started developing only in 2004 with the creation of Facebook. The use of these platforms has exploded since the introduction of Instagram in 2010 and Snapchat in 2011. The number of social media users is difficult to evaluate since not all platforms grant access to these data, however, diverse studies agree on the fact that more than half of the world population today are active social media users (4,7 billion in July 2022 according to Datareportal)[3], a number that is expected to grow. Social media can be defined as forms of Internet-based media that allow groups or individuals to communicate and share information in real time. Important features of social media are the instantaneity of the information, the lack of regulation and national boundaries, as well as possibility of access by every individual. The social dimension of social media is central, in the sense that it differentiates it from other traditional media such as television or radio. Not that traditional media does not have a social goal in interacting with society, but social media are defined by their sociality of a different magnitude. Several features can be highlighted in distinguishing social media from older traditional media, according to Axel Bruns[4]. First, social media are based on a many-to-many basis through a networked environment, whereas traditional media are built on a broadcast system of one-to-many basis. This type of broadcast leads to a selected, filtered content subject to control or censorship, while social media are generally free from editorial control, and filtering (removal of content can occur, but only after the publication). For him, there is a democratic aspect of social media versus elite traditional media, and social media's means of production are gathered in the hands of people versus in a few commercial and/or public service organizations for traditional media. These last claims are to be nuanced however, in the sense social media are largely owned by big private companies, which can question the democratic and 'owned by the people' aspects of social media. Christian Fuchs' position[5] is in line with Axel Bruns' in their social aspect, since for them it is essential to take into account the societal context and analyze social media in their interconnections with the society. Social media are based on individuals and their interactions, which are different from one society to another. In this respect, since our study focuses mainly on the U.S. and France, we will study the main social media platforms used in these societies, which are mainly Facebook, Twitter, YouTube and Instagram. One specific type of social media platforms is private messaging applications such as WhatsApp, Facebook Messenger, or Signal. However, conversations on these platforms are encrypted and are therefore difficult to analyze, as well as to infiltrate by foreign actors. We will thus exclude social media messaging platforms, as it is

[2] "2016 Election Interference. Most Wanted - Counterintelligence," Federal Bureau of Investigation, accessed September 19, 2022, https://www.fbi.gov/wanted/counterintelligence/2016-election-interference.
[3] Simon Kemp, "The Global State of Digital in July 2022" (DataReportal, We are social, Hootsuite, July 21, 2022).
[4] Axel Bruns, "Making Sense of Society Through Social Media," *Social Media + Society* 1, no. 1 (April 1, 2015).
[5] Christian Fuchs, *Social Media a Critical Introduction*, 2nd ed. (London: Sage, 2014).

usually done in academic research, although a separate analysis on these platforms would be valuable. On social media, as well as on most of the software applications and systems, backdoors can be identified. Backdoors in computer science can be defined as a means to access the computer system or the data of a program, through a security bias. This opening can be created purposefully by the developers or result from a conception error. These backdoors are usually meant for legitimate purposes such as maintenance operations carried out remotely, or to leave access for the government. However, when discovered and used by malicious actors, they can represent dangerous vulnerabilities through which malwares can be inserted. In our title, backdoor is used as a metaphor from the cybersecurity world to show how social media's legitimate uses can be deviated and become a window open for malicious actors to cause harm. Through social media, malicious foreign actors can interfere in the electoral process in several ways such as through cyberattacks or information manipulation.

The definition of foreign interference is not clear and has been attributed different meanings by scholars, governments, or private companies. In the United States, 'foreign interference' has been defined by the Department of Homeland Security (DHS) as "*malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies*."[6]. Social media companies also provide us with definitions, such as Facebook that defined 'foreign interference' as "*Coordinated Inauthentic Behavior conducted on behalf of a foreign or government actor*"[7].

Different scholars also addressed the issue of 'foreign interference' and their works provide us with some insights regarding this concept and its definition. By introducing the term 'soft-power', Joseph Nye[8] elaborated on the ability of an actor to *influence* others, and to make them do what they would not have done otherwise, through attraction and not coercive means. The notion of influence is important to consider. However, if foreign interference is meant to *influence* others in the sense that the means used are not coercive, several dimensions need to be added to better understand the concept and to distinguish foreign interference from foreign influence. While public diplomacy through open communication is considered as a legitimate aspect of influence, interference is characterized by a pejorative meaning and considered as neither legitimate nor acceptable according to Kristine Berzina and Etienne Soula[9]. They underline two major dimensions that they consider essential in order to grab the notion of 'foreign interference', which are *intent* and *transparency*. Several factors can help determine the *intent* of these actions such as timing, coordination of behaviors and scale of effect. *Transparency* relates to the covert and opaque nature of foreign interference.

---

[6] U.S. Department of Homeland Security, "Foreign Interference Taxonomy. Mis-, Dis-, and Malinformation Resource Library," Cybersecurity and Infrastructure Security Agency, July 2018, https://www.cisa.gov/mdm-resource-library.

[7] Kristine Berzina and Etienne Soula, "Conceptualizing Foreign Interference in Europe," *Alliance for Securing Democracy*, March 18, 2020, 14.

[8] Joseph S. Nye, "Soft Power," *Foreign Policy*, no. 80 (1990): 153–71, https://doi.org/10.2307/1148580.

[9] Berzina and Soula, "Conceptualizing Foreign Interference in Europe."

It is important to notice that when we talk about foreign interference in the electoral process, not only we refer to the vote itself but first and foremost to the whole political campaign taking place before, for a period of time more or less extended depending on the country. The political campaign, as we know, takes place everywhere: in private conversations, meetings, traditional media but also more and more on social media, which can allow foreign interference. Still, foreign interference is a wide term and encompasses different subcategories, including operations of information manipulation.

Several terms are used to explain this phenomenon. The expression 'fake news' has been extensively used in the public discourse and the media, which distorted its initial meaning of false information and gave it a political aspect, and is therefore rarely used in academic research. While many scholars refer to disinformation operations[10], others use information operations, such as Facebook experts that defined it as "*actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome*"[11].

To analyze this phenomenon, Samuel C. Woolley and Philip N. Howard use the expression 'computational propaganda' describing it as "*the use of algorithms, automation, and human curation to purposefully manage and distribute misleading information over social media networks*". For them, automation and anonymity represent two main aspects of computational propaganda.

James Pamment et al. use the expression 'information influence activities', that are defined as "*the targeting of opinion-formation in illegitimate, though not necessarily illegal ways, by foreign actors or their proxies*". For them, intention, ambiguity and legitimacy are three characteristics that define information influence activities. The illegitimate character of these activities differentiate them from public diplomacy, in the sense that they "*deceive people*", "*exploit vulnerabilities*" and "*break the rules*"[12]. We would argue however, that influence does not necessarily encompass a problematic aspect, which is why using the term manipulation is more satisfying.

We believe that referring to 'information manipulation' instead of 'disinformation' is more relevant in the sense that the latter omits some key aspects, including the fact that operations of information manipulation do not only spread false information, and that they are part of an intentional coordinated campaign, which is not necessarily the case for disinformation. A report conducted by French scholars[13] highlighted three main aspects of information manipulation: it represents a coordinated campaign (not isolated individual messages), which main tool is to spread false or consciously distorted information, with the political intention to cause harm. For the authors, manipulation is more satisfying than influence in the sense that they consider influence as too broad and not necessarily

[10] Steven Barela and Jérôme Duberry, "Understanding Disinformation Operations in the Twenty-First Century," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, 2021, 41–72; W. Lance Bennett and Steven Livingston, *The Disinformation Age*, Cambridge University Press (Cambridge University Press, 2020).

[11] Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook" (Facebook Security, 2017).

[12] James Pamment et al., "Countering Information Influence Activities: The State of the Art: Research Report." (Lund University, July 1, 2018).

problematic. Moreover, contrary to propaganda, information manipulation does not necessarily imply the defense of an alternative world view, but to disrupt and delegitimize other discourses. Information manipulation can therefore take different forms: spread of false or distorted information through bots or trolls, targeting individuals relying on personal information (micro-targeting), hack-and-leak operations against public personalities, and many others. Information manipulation operations therefore use the information environment on social media to manipulate opinions, using and exploiting digital tools and vulnerabilities to achieve their goals. The fact that these operations are launched by a government or non-state actors depends on the definition. However, we will focus here on state-sponsored interference on social media, although it is difficult to prove the role of the government and to distinguish it from actions taken at the individual level.

Moreover, if foreign interference in elections can take several forms such as financing foreign political parties or relying on traditional media (in our case, Russia media such as Sputnik and RT can have an important role) to manipulate information and interfere in the electoral process, our goal here is to focus on social media and we will therefore analyze essentially information manipulation on social media as one of the forms of foreign interference in elections. This threat is generally qualified as a 'hybrid threat', in the sense that it encompasses several dimensions of conventional and non-conventional warfare.

Foreign interference in elections is considered as a major threat for democracies, since it obstructs the democratic electoral process. As stated by the Executive Order number 13848: "*The ability of persons, as well as foreign powers, to interfere in or undermine public confidence in U.S. elections constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States*"[14]. According to Viginum in France, the agency in charge of fighting digital information manipulation operations, four characteristics must be included to be qualified as such: a potential prejudice to the fundamental interests of the Nation; manifestly inaccurate or misleading content; artificial or automated, massive and deliberate diffusion; and the direct or indirect involvement of a foreign actor (state, parastatal or non-state)[15]. Foreign actors interfering in elections thus represents a major threat for liberal democracies since it touches upon the electoral process which is the basis of democracy. The fact, for the people, to not believe in the integrity of their electoral process delegitimizes all the democratic institutions. By manipulating information, foreign actors can also divide the population and increase political tensions. This topic is therefore of great interest since only a thorough understanding can help assess and frame the threat to then propose adapted solutions.

---

[13] Jean-Baptiste Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies" (Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, August 2018).

[14] Donald J. Trump, "Executive Order 13848 - Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election," Pub. L. No. Executive Order 13848 (2018).

[15] "Viginum, Vigilance et Protection Contre Les Ingérences Numériques Étrangères," Secrétariat général de la défense et de la sécurité nationale, accessed September 6, 2022, http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangeres-viginum/.

Election interference and information manipulation largely predate social media. However, we saw with the 2016 American presidential elections, and later with the 2017 French presidential elections, that it took a different form, more difficult to apprehend, and larger in scale, which at the time generated huge debates and fears due to its unknown and unpredictable character. If today, research has permitted a better understanding of the threat, it is still evolving and solutions are still either not adapted or applied unequally. Throughout our research we will therefore try to respond to these questions: how have social media opened up potential opportunities for electoral interference by foreign actors and how can the cases of American presidential elections in 2016 and French presidential elections in 2017 bring insights on this phenomenon? How do states and other actors respond to such threats and to what extent is there room for improvement?

Our main hypotheses are first that social media's characteristics and vulnerabilities are used by foreign actors as new tools to interfere in elections and favor one candidate. Another sub-hypothesis is that the U.S. and France both took significant measures to respond to these threats. This work seeks to provide a detailed analysis tackling these hypotheses and the questions raised, through a multidisciplinary and comparatist approach, which will be detailed in the first chapter, along with a state of the art on the topic including the broader literature on cyberspace. The second chapter will study the mechanisms and objectives of foreign election interference through social media, while the third chapter will analyze the response, from the measures that are already undertaken to those potentially applicable.

CHAPTER 1: STUDYING EMERGING THREATS ON CYBERSPACE: VARIETY OF RESEARCH AND CONTRIBUTION OF THE COMPARATIVE METHOD

Interfering in elections through social media is considered as an emerging threat for democracies. The cyber dimension of the topic will be underlined since social media emerged as part of cyberspace, that represents a flourishing and constantly evolving literature. Other aspects of the topic will be analyzed emphasizing on the variety of research fields feeding this literature, leading to our final section on the value added by the comparative method.

Section 1 : A growing interest in cyberspace: from flourishing literature to states' implication

The emergence of cyberspace has rapidly fascinated or worried the world, from researchers, who have seized the opportunity to engage in numerous works providing tools for a better understanding, to states that have shown a significant interest in integrating the cyber domain to their policies.

1. The early acknowledgement of growing threats in the newborn cyberspace literature

If the birth of cyberspace was accompanied with fantasies and various interpretations of cyber threats, the development of cyberspace literature has progressively framed the topic for a better understanding.

a. The birth of 'cyberspace'

Cyberspace is a term that was first popularized by the writer William Gibson in his novel "Burning Chrome"[16], where he described it as a data sphere of "unthinkable complexity". It later became the object of numerous science-fiction works, often leading to a dramatic outcome. Starting from the 1990s, research works about cyberspace, mostly in the fields of social science and computer science, developed and their number have kept increasing since then.

As we can see with this Scopus search, the number of documents (mostly articles), including the term 'cyberspace' in their title, abstract or keywords rose from only two documents in 1990, to 818 in 2021[17].

[16] William Gibson, *Burning Chrome* (Gollancz, 1982).

[17] Table realized from Scopus data, Elsevier B.V., 2022, accessed on April 10th 2022.

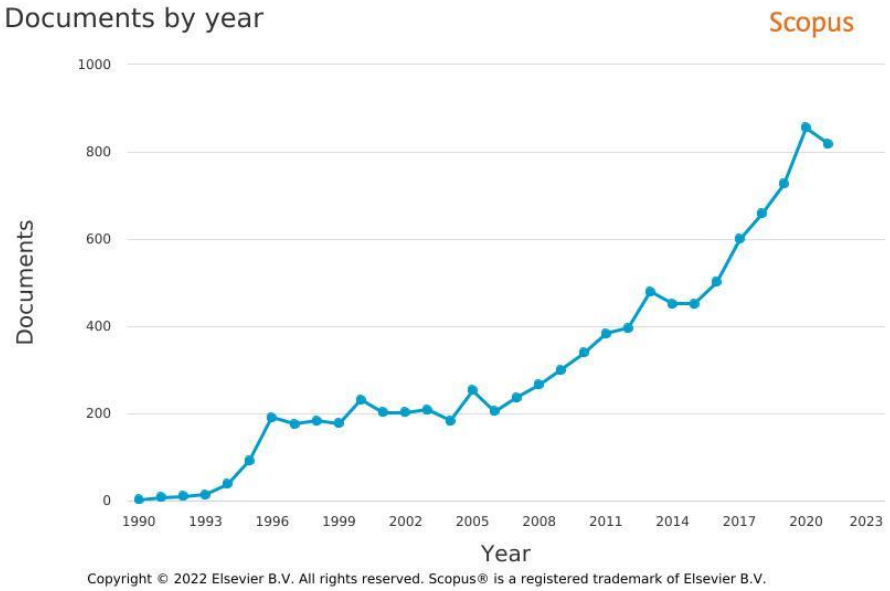

Figure 2: Documents including the term "cyberspace" in their title, abstract or keywords. Scopus data, Elsevier B.V., 2022.

Today, one widely used definition of cyberspace was coined by the U.S. government in 2009 when establishing a U.S. Cyber Command. It represents "*a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*"[18]. Joseph Nye later insisted on the human dimension of cyberspace that distinguishes it from other spaces: it is a 'manmade environment'[19]. Ronald Deibert highlights the fact cyberspace is an 'inherently political environment' in that its blurry limits in time and space are widely contested, especially from 2000 onwards when cyberspace emerged in political discourses[20]. According to scholars, we can distinguish diverse layers of cyberspace, Frédérick Douzet focuses on four of them[21]. The first represents its physical aspect, made of a network of physical components such as computers, submarine cables, or satellites. The second layer refers to the logical domain characterized by a common language to exchange data. The third one is composed of applications that plays a role of intermediate between individuals and the logical domain in that they can interact without understanding the common language. Finally, the fourth layer refers to individuals and their interactions and information. During a 2016 NATO summit, cyberspace is for the first time considered as a military domain along with air, land, maritime, and space. As we can see in this definition, the notion of cyberspace includes many aspects, and the Internet is only one of them. When studying social media, we are therefore studying a specific portion of cyberspace.

[18] U.S. Strategic Command, "The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities." (U.S. Strategic Command, January 5, 2009), National Security Archive, https://nsarchive.gwu.edu/document/21360-document-1.

[19] Joseph S. Nye, "Cyber Power," *Belfer Center for Science and International Affairs*, Harvard Kennedy School, May 2010.

[20] Ronald J. Deibert, "Trajectories for Future Cybersecurity Research," in *The Oxford Handbook of International Security*, ed. Alexandra Gheciu and William C. Wohlforth, 2018.

b. Between optimism and source of concern

Cyberspace, and social media in particular later, paved the way for a wave of opposite reactions between fear and optimism. In the domain of international relations, many saw in cyberspace a progress in technology that would facilitate economic interactions, communications or investments around the world, reinforce security and diplomacy, and spread free speech, as mentioned in the U.S. National Security Strategy in 2010[22].

Regarding the spread of free speech, social media were initially considered as a tool for communicating without censorship and boundaries, that would help democratization and promote political participation[23]. Just like Bill Clinton claimed that the Internet would liberalize Chinese politics[24], many authors showed how social media could represent a valuable tool for democratization, to overcome collective actions problems such as the rebel's dilemma[25], in helping individuals organize on platforms, bypassing the need for a political leader and central organization[26]. It was indeed the case during the Arab Spring in the early 2010s, where social media represented the driving force of uprisings against different oppressive political regimes or leaders and were largely used as a tool for political mobilization, facilitating the organization of large protests while avoiding censorship[27]. Actions ranging from naming their child 'Facebook' to investing in social media companies, showed that cyber and social media optimism was at its highest[28]. Similar famous rebellious movements organized on social media took place in Spain with the Indignados and in the U.S. with the Occupy Wall Street movement. Organized around public squares, these movements largely relied on the Internet and the social media to gather people through hashtags such as #Occupy, #SidiBouzid or #GeneraciónIndignada and the fact that they emanated directly from individuals on social media participated greatly in underlying the democratic aspect of the movements. If this was seen as a positive step for freedom of speech, not everyone considered it as a favorable progress, and political regimes in place often tried to shut down the Internet or some social media to control citizens, as it was the case in Egypt in 2011[29].

Going back to cyberspace more broadly, the potential risks linked to the development of cyberspace rapidly emerged and the growing literature on cyberspace was quickly tinged with an alarmist

---

[21] Frédérick Douzet, "Understanding Cyberspace with Geopolitics," *Hérodote* 152–153, no. 1–2 (2014).

[22] U.S. Department of Justice, "National Security Strategy" (2010), https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-security-strategy-may-2010.

[23] Anaïs Theviot, "Réseaux sociaux, la force du nombre," *Les Grands Dossiers,* Sciences Humaines, no. 62 (May 2021).

[24] Joseph S. Nye, "Protecting Democracy in an Era of Cyber Information War," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, Paper, February 2019.

[25] The rebel's dilemma refers to the rational reason of individuals in refraining from overthrowing a government, while having a common interest in doing so.

[26] Sarah Kreps, *Social Media and International Relations* (Cambridge University Press, 2020).

[27] Peter W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Mariner Books, 2018.

[28] Singer and Brooking. Ibid.

[29] Sarah Kreps, *Social Media and International Relations* (Cambridge University Press, 2020).

tendency as highlighted by Eriksson and Giacomello[30], underlying also the crucial role of science-fiction in projecting the scary side of cyberspace. As mentioned in uncountable works on cyberspace – more or less eloquently – the idea of an electronic Pearl Harbor, expression initially popularized by former deputy defense secretary of the United States John Hamre[31], shed light on the major risks that could occur on cyberspace and was largely used in the following literature to convey the idea that a cyberattack could paralyze crucial infrastructure and be almost as destructive as the attack on Pearl Harbor, representing an act of war in itself. As soon as 1991, a report by the U.S. National Security Agency warned about the potential risks of cyberspace, claiming that "*tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb*"[32]. Thus, around the world, as the literature on cyberspace grew, the novelty and unfamiliarity of this space contributed to contrasted feelings between enthusiasm and fear.

c. Framing cyber threats on the cyberspace

This topic quickly intrigued researchers and as literature grew, detailed and organized reasoning contributed to the establishment of a more understandable framework of cyberspace and its surrounding risks. The first difficulty in cyberspace resides in its delimitation, since it disrupts traditional boundaries. One specificity of cyberspace is that there are no geographical limits, interactions can occur on both ends of the planet, instantaneously[33]. Barriers of entry in one country's politics are significantly reduced, and state sovereignty is thus challenged. This phenomenon facilitates foreign interference insofar as every individual from every country can participate in another country's political debates on social media, our main focus here. When studying disinformation on social media for example, lines between domestic and foreign disinformation are extremely difficult to draw[34], although some techniques can be used to identify foreign actors (cf. chapter 3).

Cyberspace also challenges the classical realist view of states as the only relevant actors in international relations. Jan-Frederik Kremer and Benedikt Müller in their book *Cyberspace and International Relation*[35]*s*, invite us to think beyond the traditional approach of state to state relations and conflicts and consider other non-state actors. Individuals and private companies play a major role on cyberspace, and particularly on social media. Each voice can have an impact at the international

[30] Johan Eriksson and Giampiero Giacomello, *International Relations and Security in the Digital Age*, Routledge Advances in International Relations and Globl Politics (Routledge, 2007).
[31] John Hamre, "The 'Electronic Pearl Harbor,'" *Politico*, September 12, 2015.
[32] National Research Council, *Computers at Risk: Safe Computing in the Information Age* (National Academy of Science, 1991).
[33] Roxana Radu, "Power Technology and Powerful Technologies - Global Governmentality and Security in the Cyberspace," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, 2014.
[34] Claire Wardle and Hossein Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policy making" (Council of Europe, September 27, 2017).
[35] Jan-Frederik Kremer and Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, (Springer, 2016).

level and individuals can exchange on platforms that represent a wide public Agora, as Manuel Castells claimed, that replace the vertical political discourses[36]. The visibility of an individual's message depends more on the number of likes, comments or shares than on the professional and political position of that individual, as opposed to traditional media where opinions of experts and political leaders tend to prevail (for better or for worse). On social media, "*as the state fails, Homo digitalis rises to take its place*", as David Patrikarakos[37] put it, referring to the globally connected individuals. Individuals are not the only actors to challenge states' sovereignty on the international stage, private companies also play a major role in redefining the actors influencing international relations on cyberspace. The perspective of libertarian utopias of the Internet as a free and democratic space, escaping from all state control represented the dominant view when the Internet emerged in the United States in the 1990s[38]. In this respect, companies surfacing on this cyberspace were largely responsible for developing their business model, before states established a clear set of rules and practices to regulate this new space. The success of social media was so quick and huge that social media companies gained tremendous influence at the international level on cyberspace, becoming actors that could challenge states' sovereignty. The interconnectedness of the Internet, as Manuel Castells showed, has spawned networks that have broken down traditional state barriers, bringing together people and ideas around the world and building new transnational communities or political movements. Therefore, as Joseph Nye rightly predicted in 2010 in "Cyber power": "*States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control*"[39].

This new decentralized space that seems to escape states' control[40], generated new types of threats that were yet to be understood and defined. The work of researchers helped framing these threats in establishing some grounds for definition. John Arquilla and David Ronfeldt were already talking about cyber war in their 1993 article[41], which consists of "*conducting, and preparing to conduct, military operations according to information-related principles*". Cyber war allows states to get valuable information on others while protecting its own. This definition is interesting in that it refers to war due to the military aspect of the operations, but also for the place it gives to information as a key aspect of military operations. However, the authors write about another notion, that, notwithstanding its relative lack of success compared to cyber war, represents a key notion in this research: the netwar. Netwar refers to "*information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the*

[36] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford: Oxford University Press, 2003).
[37] David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*, Basic Books, 2017.
[38] Patrick Pharo, *Les data contre la liberté*, Presses Universitares de France PUF, 2022.
[39] Nye, "Cyber Power."
[40] Douzet, "Understanding Cyberspace with Geopolitics."
[41] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" (RAND Corporation, January 1, 1993).

world around it". In short, netwars are not directly related to military operations, but include a wide attack on a country's information environment, which is directly linked to what we defined in the introduction as information manipulation.

Definitions of cyber war largely evolved with the sophistication of threats in cyberspace, and emergence of new threats. There are different types of threats in cyberspace that go from infraction to war. Craig B. Greathouse[42] drawn up a typology of cyber operations on four different intensity levels: first, cyber vandalism refers to actions that are of low intensity, not meant to cause real damage but disturb (such as changing the URL of a website), followed by cyber espionage which represents the use of technologies to gather information, cybercrime (referring to criminal activities targeted at private or public actors for profit motives) comes at the third level before cyber war that includes denial of services, focused cyberattack on a specific infrastructure or massive cyber assaults.

If some use the term 'cyber war', this approach is not unanimous in the sense that it does not respond to traditional criteria usually characterizing war. While the use of the term 'war' in certain situations is eternally disputed, there are some defining elements that are commonly agreed upon and that allow us to differentiate between periods of war and peace. The presence of armed violence, the opposition between two political units, and the pursuit of a rational political objective are three key elements that characterize war. In cyberspace, these three compounding elements cannot be clearly established. The major problematic element in talking about cyber war is that attacks are generally not associated with physical violence and deaths, as in the definition of war. As a matter of facts, no cyberattack has generated deaths up to date, and it is unlikely to occur, as Ryan Maness and Brandon Valeriano pointed out, due to the "*general resistance to escalation dynamics of cyberspace*"[43].

However, Jan-Frederik Kremer and Benedikt Müller argue that due to conflicts being 'cybered', war is becoming "*difficult to bound, longer, more covert, more surprising in its scale, targets, and tempo, and ultimately more difficult to discern its beginning, end, adversaries, and motivations*"[44], redefining and complexifying war limits. We can say that a state of peace is rarely fully achieved in cyberspace, following the claim of military general Didier Tesseyre[45], commander of French Cyber Defense, that there was no such thing as peace in cyberspace. Therefore, limits between war and peace are blurred and qualifying different operations launched on cyberspace as "acts of war" can vary depending on the definition. Whether they qualify as war or not, these operations on cyberspace represent major risks that led this field to arouse great interest in the research sector but not only.

---

[42] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations*, by Alexandra Gheciu and William C. Wohlforth (Oxford University Press, 2018).

[43] Brandon Valeriano and Ryan Maness, "International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain," in *The Oxford Handbook of International Political Theory*, 2018, 259–72.

[44] Kremer and Müller, *Cyberspace and International Relations*.

[45] Maxime Tellier, "Mécaniques de la cybermenace. Épisode 1 : La guerre cyber," France culture, March 30, 2022. https://www.radiofrance.fr/franceculture/podcasts/mecanique-de-la-cybermenace/episode-1-la-guerre-cyber-3304112.

2. From research to states' implication: a greater attention to cyber threats

These emerging threats have generated a great deal of interest from states, as they understood that they could pose a crucial danger to their security. However, while the cyber world has received significant consideration, hybrid threats related to social media have often been left out of cyber issues, to be analyzed through a separate approach.

a. A growing interest towards cybersecurity

Recognition of the importance of threats on cyberspace have instigated interest of researchers but also governments in increasing their defense to guarantee their security. This led to works of international security scholars widening their vision of security to incorporate cybersecurity, and it is now common for handbooks of international security to include a chapter about cybersecurity. Cybersecurity is considered as a subfield of cyberspace. It refers to "*the threat opportunities from digital and computational technologies*". Back in 2010, when publishing their National Security Strategy, the U.S. government considered already cybersecurity threats as "*one of the most serious national security, public safety, and economic challenges we face as a nation*". Myriam Dunn Cavelty showed that countries have different threat perceptions, which makes cybersecurity a socially constructed concept. Therefore, cybersecurity largely depends on the context and its definition is constantly evolving. In liberal democracies, cybersecurity implies a need to find a balance between protecting information networks and databases while still allowing information to flow freely[46].

If cybersecurity gained interest in the research sector, its recognition as a crucial sector to improve mainly comes from states and their acknowledgement of cyber threats. In the last decade, states have increased dramatically their spending in cyberspace research and infrastructure, creating specific sections of government dedicated to this domain. Many countries started recognizing cyberspace as a warfighting domain[47], leading to what we call the 'cyberization of the military'[48]. This recognition consequently implies the establishment of a specific section in the military, starting with the United States that first set up a Cyber Command with the Department of Defense in 2009 (USCYBERCOM). The Army Cyber Command only, counts around 16,500 soldiers and employees, that is to add to additional forces for Cyber created in the Marine Corps, Air Force and the Navy[49]. As for France, it took until 2017 for a Cyber Command to be established with the creation of the COMCYBER that counts 3,200 cyber-soldiers today, projected to increase to 5,200 in 2025[50]. The wake-up call can be

[46] Deibert, "Trajectories for Future Cybersecurity Research."
[47] Rex Hughes, "A Treaty for Cyberspace," *Oxford University Press on Behalf of the Royal Institute of International Affairs*, International Affairs, 86, no. 2 (March 2010).
[48] Kremer and Müller, *Cyberspace and International Relations*.
[49] "Command History," United States Cyber Command, accessed August 12, 2022.
[50] "Le commandement de la cyberdéfense (COMCYBER)," Ministère des Armées, February 14, 2022.

considered as the recognition in 2016 by the North Atlantic Treaty Organization (NATO), of cyberspace as a domain of operations, along with air, sea and land[51]. Developing cyber military strategies and doctrines is not a new practice and while some countries are just joining the game[52], others regularly renew their strategy, such as the US with the latest update in 2018.

As for the civilian domain, states also took steps in increasing their cybersecurity, primarily with administrative agencies designed to secure information systems and cyber infrastructures. To that end, the U.S. established the National Protection and Programs Directorate (NPPD), as part of the Department of Homeland Security, in 2007. The NPPD was recently replaced by the Cybersecurity and Infrastructure Security Agency (CISA), through the Cybersecurity and Infrastructure Security Agency Act of 2018, expanding its prerogatives. France set up the National Authority for Securing Information Systems (autorité nationale de sécurité des systèmes d'information, ANSSI) in 2009, as part of the General Secretary on Defense and National Security (secrétariat général de la défense et de la sécurité nationale, SGDSN), that is directly linked to the French government. Still today, governments keep establishing agencies related to cyberspace, as evidenced by the creation, not later than April 4th, 2022, of the Bureau of Cyberspace and Digital Policy in the U.S. government[53].

b. Contrasting interpretations of cyber threats: how hybrid threats emerged as a separate topic

However, this deployment of resources by states is primarily a response to the need for cybersecurity in the face of cyberattacks. Much attention has been given by states and the research sector to cyberattacks, in the domain of international relations. Stuxnet, Wannacry or Solarwinds are all large-scale cyberattacks that reminded governments and the research sector that emphasis had to be made on this type of attack in cyberspace to increase cybersecurity. These attacks have a physical impact, generally on infrastructures. Due to the increase in sophistication and number of these attacks, the risk is real that some facilities could be paralyzed, putting a nation in danger. In 2021 only, ComCyber in France has identified more than 12,000 security incidents, including 14 of high risk reported to the Presidential Office[54].

Consequently, research has been focused on cybersecurity and cyberattacks in international relations. The role of states and non-state actors, attribution of these attacks, sanctions, deterrence and retaliation are issues that have been widely discussed in the literature, and that are still – rightly – getting more attention. Yet, if the information manipulation operations we are studying here occur on social media, which are themselves an integral part of cyberspace, they are not considered as

[51] NATO, "NATO Cyber Defence - NATO Factsheets," August 2020.
[52] Italy, for example, published its cybersecurity strategy this year following the creation of the National Cybersecurity Agency last summer.
[53] "Establishment of the Bureau of Cyberspace and Digital Policy (Press Release)" (U.S. Department of State - Office of the Spokesperson, April 4, 2022).
[54] Tellier, "Mécaniques de la cybermenace. Épisode 1 : La guerre cyber."

cyberattacks. These operations have a broader dimension that can mobilize means such as cyberattacks on specific targets (usually political parties or candidates) as part of a more general campaign of information manipulation. For example, a large campaign of information manipulation by an external actor, could include phishing activities[55] as part of the broader campaign. When studying potential disruptions in elections related to cyber, scholars might also put an emphasis on potential cyberattacks on electoral infrastructures, such as the disruption of electronic voting systems. Social media are therefore often excluded from cyberspace, although we consider that, according to their definition, they represent an integral part of it. Understanding the functioning of cyberspace is indeed essential to understand the functioning of social media. However, foreign interference on social media is not exclusively tied to cyberspace, in the sense that it involves less virtual dimensions such as information and society or politics, indicating a hybrid dimension. As stated in a NATO report, with the rise of social media platforms, "*the lines between cyber and information warfare are becoming increasingly blurred*"[56]. Risks of information manipulation on social media are consequently generally studied under the prism of 'hybrid threats', an area of focus that is difficult to classify in that it crosses many fields, as we will see later. The European Union has defined hybrid threats as a mix of conventional and unconventional methods used in a coordinated way by state or non-state actors, to achieve their objectives while remaining below the threshold of traditional warfare[57]. We can talk about hybrid threats in different fields including the use of economic or diplomatic tools, however, our main focus here will be on one particular characteristic which is the informational aspect.

Section 2 : A multifaceted topic: various arguments at the intersection of various fields of study

The difficulty of the topic resides in the fact that it is composed of three main subtopics (social media, foreign electoral interference, information manipulation), that can be analyzed through the prism of many research sectors, multiplying the possible approaches. If we tried to present the literature on cyberspace – the main concept encompassing our topic – with an eye of international relations scholars, it is equally crucial to provide an overview of all the different approaches of the topic, so as to widen our view for a more complete understanding. Particular attention will be given to information studies, which, while long established, are experiencing a revival with the emergence of social media.

[55] Sending a fraudulent link to the target that allows (through the victim's click) the author to obtain access to the desired data.
[56] Sanda Svetoka, "Social Media as a Tool of Hybrid Warfare" (Riga: NATO Strategic Communications Centre of Excellence, 2016).
[57] "Joint Framework on Countering Hybrid Threats a European Union Response" (2016).

1. Influencing opinions: a deeply embedded practice

While we chose to focus our study under the prism of cyberspace first, since information manipulation on social media takes place in an online environment, election interference through social media is also extensively analyzed as part of studies on information, reshaping an old strategy in international relations of influencing and controlling the information.

a. Interfering in elections: a long-standing phenomenon source of interest for researchers

Interfering in another state's elections to achieve a more favorable outcome for one state's interests is not a new phenomenon. In the post-World War II and Cold War eras, the United States and Russia (or USSR) regularly intervened in other countries' elections: not less than 117 times between 1946 and 2000, according to Dov H. Levin[58]. For him, we can consider it as a "*longstanding common phenomenon*", but not an insignificant one. In the same article, he exposes the perilous consequences of such interference in elections. With the collected data, he finds that interference in elections is significantly correlated with domestic unrest (and even domestic violence) afterward. Foreign interference in elections increased risks of a democratic breakdown from 2,5 to 8 times, in the next five years after the targeted country's elections. The main tools of foreign interference in elections can be divided into six categories. The intervening state can help favor one candidate/party's campaign in two main ways: through *campaign funding*, financing (directly or indirectly) the campaign, or *campaigning assistance* with non-monetary or non-material help to the campaigns (by training party locals for example). *Threats or promises* can be made by the intervening country's officials to guarantee a reward or threaten the targeted country, as well as promises of *giving or taking aid* that is currently in place (in changing trade agreements for example), or even guaranteeing *concessions* for the intervening state, such as on a disputed territory or prisoners. Finally, an intervening state can do *dirty tricks* to directly harm candidates/parties, through physical violence against the candidate/at the office/during political events, or by spreading disinformation. Campaigns of information manipulation on social media generally fall into this last category. Therefore, even though some claims of interference have been made about American and French presidential elections of 2016 and 2017 regarding in particular the financing of political parties' campaigns by foreign actors, we will focus our analysis mainly on non-financial interventions in the form of information manipulation on social media.

[58] Dov H. Levin, "Should We Worry about Partisan Electoral Interventions? The Nature, History, and Known Effects of Foreign Interference in Elections," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, Oxford University Press, 2021.

b. "Information is power", controlling information as a source of power

Information manipulation is not a new phenomenon either: "*the disruption of another country's public opinion and decision-making dates back decades, if not centuries*"[59]. Five centuries before Christ, in its famous *Art of War*, Sun Tzu already considered the military option as the last resort, after destroying the enemy from the inside through the devaluation of its values and the division of its population[60], which is tantamount to trying to influence information available to the population to control narratives and change opinions. That was essentially leaders' strategy during World War I, II, and the Cold War, in which the war of narratives was considered essential to "win hearts and minds" of the populations. Propaganda was used to control information and represented a precious tool in Nazi's strategy, with Joseph Goebbels, chief propagandist for the Party, developing on the concept of the "illusion of truth" through the multiplication of false information in the political discourse as a conscious destabilization strategy, claiming: "*repeat a lie often enough and it becomes the truth*"[61].

During the Cold War, controlling information and disinformation operations were a widely used tool by the Soviet KGB, following guidelines of *dezinformatsiya*. On the first page of one of these highly classified secret guides for *dezinformatsiya* was written in caps: "*IF YOU ARE GOOD AT DISINFORMATION, YOU CAN GET AWAY WITH ANYTHING*"[62]. Recent events that we will study later seem to show that lessons taught by the KBG to Vladimir Putin during his experience there were not forgotten. More generally, states' leaders have often followed Gramsci's statement that political victory was achievable only after an ideological victory. To win the cultural hegemony over the population of another state, influencing information therefore represented and still represents a key source of power for states. Joseph Nye argued in this direction when claiming that "*information becomes power*"[63], especially with the information revolution that occurs through the development of information and communication technologies (ICT), in the sense that information production, processing, and transmission now come at a substantially lower cost[64]. If controlling information is still considered as necessary to uphold national security and preserve sovereignty[65], ICTs have made it significantly more challenging for states to operate in interconnected networks of several flows and actors. This phenomenon has been reinforced with the emergence of social media.

[59] James Pamment et al., "Countering Information Influence Activities: The State of the Art: Research Report." (Lund University, July 1, 2018).
[60] In: David Chavalarias, *Toxic Data: Comment les réseaux manipulent nos opinions*, Illustrated édition (Paris: Flammarion, 2022).
[61] In: Kreps, *Social Media and International Relations*.
[62] Steven Barela and Jérôme Duberry, "Understanding Disinformation Operations in the Twenty-First Century," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, 2021, 41–72.
[63] Joseph S. Nye, "Soft Power," *Foreign Policy*, no. 80 (1990).
[64] Nye, "Cyber Power."
[65] Eriksson and Giacomello, *International Relations and Security in the Digital Age*.

c. Controlling information in the social media era, an extension of public diplomacy?

Social media also participated in this information revolution, by generating new opportunities for information to spread. Through the use of automation or Big Data, social media technologies shaped the way information is transmitted significantly, in its scale, scope, and precision, especially for disinformation[66].

Here is an infographic that summarizes the quantity of information being produced at an unprecedented scale every minute on the Internet, and on social media in particular. While 575,000 tweets are posted every minute, 176 million people watch videos on Tik-Tok and 240,000 pictures are shared on Facebook[67].

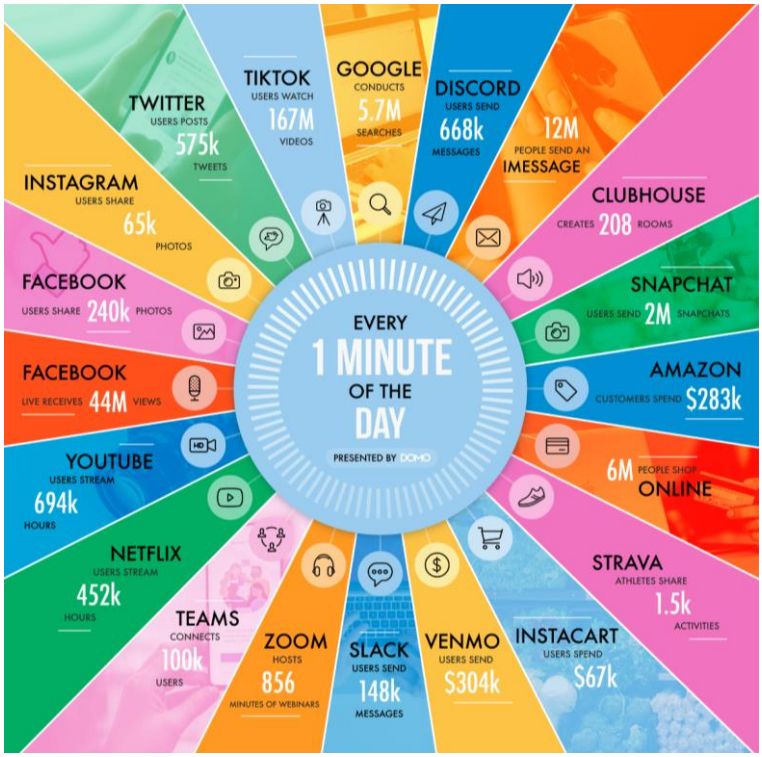

Figure 3: "Data Never Sleeps 9.0". *Domo*. 2021.

Moreover, social media's scope is huge, reaching an impressive range of people all over the world, from different ages, countries and social backgrounds. Precision on social media can be attained through microtargeting techniques that will be developed later (cf. Chapter 2), using users' available data. Social media shape the informational environment in building an online informational system, in which time and space are redefined through the instantaneity and global reach of the messages. Therefore, they have opened a myriad of new possibilities for different actors to influence information, while making it difficult for one state to control its own information environment, if not through a strict censorship (cf. Chapter 2).

[66] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," Computational Propaganda Research Project (Oxford Internet Institute - University of Oxford, September 26, 2019).

[67] "Data Never Sleeps 9.0," Domo, 2021, https://www.domo.com/learn/infographic/data-never-sleeps-9.

One way to control and influence information for states has been with public diplomacy through traditional media, in order to reach other populations and spread a message to influence their opinion. Social media substantially shaped public diplomacy practices, and emerged as a way to directly reach populations. Sometimes referred to as "Twiplomacy", the diplomacy on Twitter and other social media allows for immediacy and transparency, elements that redefine traditional diplomacy. Most embassies, diplomats and statesmen now have social media accounts, to interact directly with populations, as well as enhancing the image of their nation. China extensively used social media channels all over the world for their public diplomacy during the Covid-19 pandemic to restore a positive image, in order to counter "Chinese virus" discourse and show the country's efficiency in fighting the pandemic[68]. However, the line between public diplomacy and information manipulation or disinformation is thin. While public diplomacy is overt and usually claims to be truthful, disinformation is more opaque[69]. For Pamment et al.[70], the main difference refers to the legitimacy: foreign disinformation or information manipulation campaigns are illegitimate in that "*they deceive people*," "*they exploit vulnerabilities*," and "*they break the rules that govern constructive open and free debate*". Therefore, throughout this research, we will focus on information manipulation operations essentially, purposefully leaving behind other strategies of influence such as the use of state-sponsored media abroad and on social media, as Russia does with Sputnik and RT[71].

Campaigns of information manipulation on social media are therefore at the crossroads between cyberattacks – as seen earlier in the Chapter – that can be used for disinformation but also for other purposes, and public diplomacy, that can use disinformation but can also be honest, summarized schematically in a RAND report[72].

[68] Marc Julienne and Sophie Hanck, "Diplomatie chinoise : de l'« esprit combattant » au « loup guerrier »:," *Politique étrangère* (February 15, 2021).
[69] Raphael S. Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions* (Santa Monica, CA: RAND Corporation, 2021).
[70] Pamment et al., "Countering Information Influence Activities.".
[71] Kévin Limonier and Maxime Audinet, "La stratégie d'influence informationnelle et numérique de la Russie en Europe," *Herodote* 164, no. 1 (May 10, 2017).
[72] Raphael S. Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*..

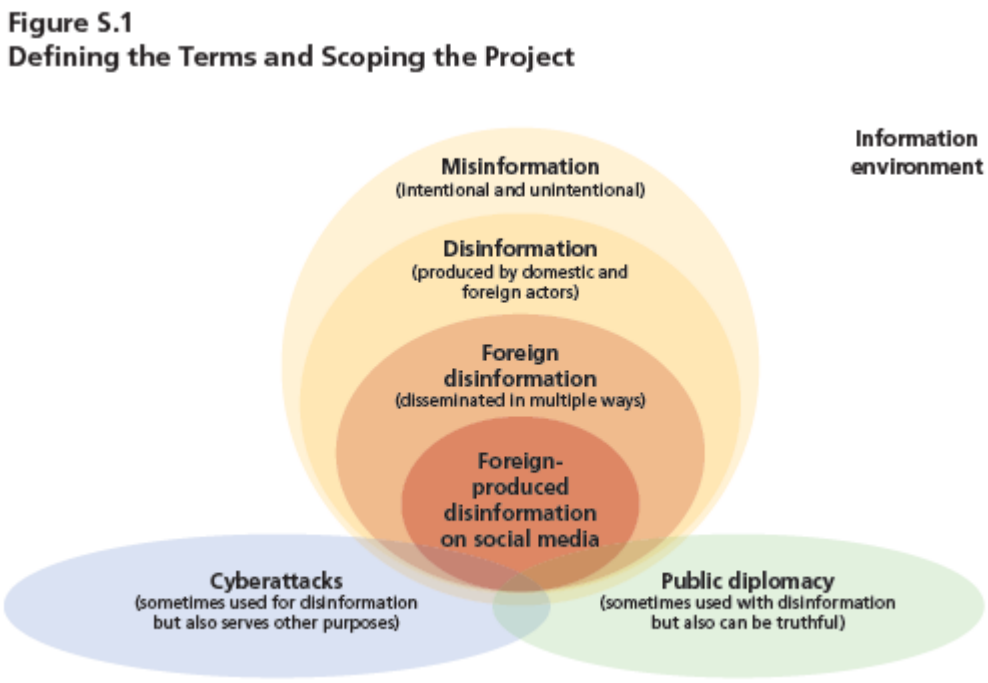

Figure 4: Defining the Terms and Scoping the Project. RAND Corporation. 2021

Information manipulation on social media therefore seems a relatively new field of study, that we saw stems from the whole literature on cyberspace, but is also of interest to researchers working on information. We will now see that this subject is at the crossroads of a large number of research sectors, which contributes to its richness.

2. Uncountable research fields at stake

Depending on the concept at hand, diverse analyses and fields of study will appear to be of primary importance. The multidisciplinary aspect of this subject represents a precious strength that it is essential to take into account to understand all its implications.

a. From psychology to computer science, through philosophy and political science

This paragraph, while not meant to be exhaustive, aims at presenting the main approaches to cyberspace and social media in diverse fields of study. Social media, election interference, and information manipulation represent the main concept of this research, and can be analyzed in many ways. First, social media has been a major source of interest for human and social sciences in general, from international relations to political science, history, philosophy or sociology, and has triggered many research works in order to try to understand this relatively new phenomenon. Information

manipulation is also at "*crossroads between international relations, war studies, intelligence studies, media studies, sociology and social psychology*"[73], just like election interference that has been widely studied in various research sectors.

This Scopus search helps us understand the variety of disciplines linked to this topic.

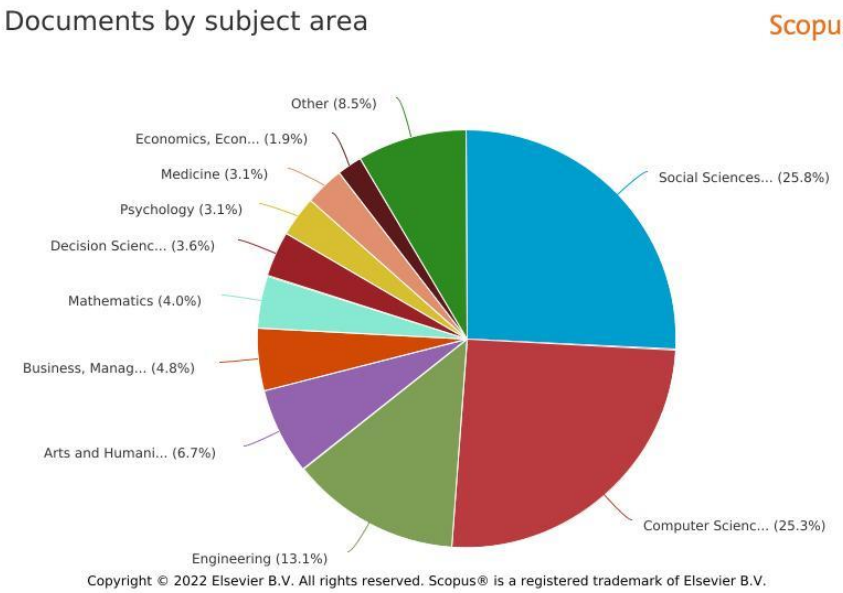

Figure 5: Scopus search on "cyberspace", by subject area. Scopus data, Elsevier B.V., 2022

When analyzing scientific research on cyberspace, we can see that the results are divided among many different categories, from medicine to engineering, along with business and management or social sciences. The two main disciplines that represent half of the research combined are social sciences and computer science. However, even within these categories of subject area, we can find many sub-disciplines that can form a considerably diverse literature.

Throughout this thesis, we will try to provide insights from different backgrounds, so as to better grasp the complexity of the issue. While political science will help characterize the different electoral systems and the impact of social media in democratic elections, sociology will be used to analyze social media use in diverse countries and the impact of information manipulation on populations, and philosophy will provide insights on the dilemmas related to the measures that should be taken in order to counter information manipulation on social media. Cyberspace and social media have triggered many debates in the field of law, so as to clarify which laws are applicable on cyberspace, and how to improve regulation to better protect the population, which proves to be essential when trying to counter these threats. Insightful remarks will also be found in the psychology literature in order to try to understand how individuals are manipulated on social media, and the mechanisms at play. Communication and media studies also help us understand the place and functioning of social media in the information system, and to what extent traditional media play a role in relaying information

[73] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."

found on social media. Social media also raised interest in sciences such as mathematics or computer science, especially with the study of algorithms used by social media to present content to their users.

b. The necessity to adopt an interdisciplinary approach, often lacking

The various approaches previously described not only represent a valuable input to our research, but are also considered as essential although often lacking. Scholars have emphasized the fact that interdisciplinarity is key to understanding the diversity of aspects of this topic. Claire Wardle and Hossein Derakhshan, in a report for the Council of Europe called "Information disorder: Toward an interdisciplinary framework for research and policy making"[74], underline the necessity to build an analysis based on a variety of disciplines, that all represent valuable inputs. For them, it is only in building common general definitions, accepted by the extremely diverse research community, that potential solutions can be found. A report presented in the European Parliament by the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, underlined this by claiming that "*there is a need for an EU definition and methodology to improve the common threat analysis*"[75].

Designing solutions also begins with finding the causes of the problem. However, this phenomenon is a "multifaceted problem"[76], and the causes are as diverse as they are numerous. From psychological predispositions, to algorithmic specificities and issues of trust in the media or institutions, foreign disinformation through social media can only be addressed through multiple but not totally independent measures, necessarily designed by a variety of actors working together.

For Alexandra Gheciu and William C. Wohlforth[77], the incorporation of methods that are not common to social sciences, such as techniques used in mathematics or data analysis, are crucial to understand cyberspace and social media functioning and would bring valuable insights to social science research, although they recognize that this could take generations to overcome the divide between the two types of science and the different methods. If this is a long process, social science research using data extracted from social media is developing, and has been the source of valuable works on social media[78].Nevertheless, they encounter a major problem developed further in our analysis (cf Chapter 3), that is the non-availability of most of social media data. All in all, this state of the art shows that there is increasing and extensive literature on cyberspace and the emerging hybrid threat of electoral interference through information manipulation on social media. However, this literature sometimes

[74] Wardle and Derakhshan, "Information disorder."
[75] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation" (European Parliament, February 8, 2022).
[76] Directorate-General for Communications Networks, Content and Technology, "A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation" (LU: European Commission, 2018).
[77] Alexandra Gheciu and William C. Wohlforth, *The Oxford Handbook of International Security*, Oxford Handbooks of International Relations (Oxford University Press, 2018).
[78] See the works of Sarah Kreps in *Social Media and International Relations*., and David Chavalarias (mathematician) in *Toxic Data, Comment les réseaux manipulent nos opinions* (in French, not translated).

lacks a multidisciplinary approach and might tend towards generalities and methodological nationalism. By responding to the following question, we want to insist on the inputs that this multidisciplinary, comparatist approach can bring. How have social media opened up potential opportunities for electoral interference by foreign actors and how can the cases of American presidential elections in 2016 and French presidential elections in 2022 bring insights on this phenomenon? This last part will explain how the comparative approach using extensive, diversified literature in this comparison, might provide insights to fill a void in the existing literature.

Section 3 : A multidisciplinary and comparatist approach: bringing new insights to the existing literature

The comparative method provides some insights on the phenomenon of foreign interference in elections on social media and will represent the core of our analysis, while incorporating multidisciplinary sources. The construction of the thesis will be explained through a quick methodological review of how the research was built, and through a more deepened analysis on the relevance of the French-American comparison.

1. Contributions and methodology of a comparative and multidisciplinary approach

First, it is important to present the methodology used in undertaking this research work, from the reason why it was adopted to the tools and methodology employed.

a. The comparative method: why?

The initial idea was to study foreign interference in elections through social media in general, studying varied examples along the thesis. However, during the research, one particular case appeared to come back often in the diverse works on the topic: the 2016 American presidential elections. If extended literature could be found on this specific case, it appeared quite challenging to resituate this case in a broader context of election interference through social media. Works of research were either presenting varied examples all over the world, which made the drawing of a detailed picture difficult in some cases, or were focused on one case (usually the United States), which generally obscured the global tendency of the phenomenon. A comparison with another country appeared as an excellent way to first, replace this phenomenon under a global approach to understand its scope, second, to study the different mechanisms at play in both countries and look at similarities and differences in order to grasp the intensity of the phenomenon. Finally, if this comparison is mainly explicative, it also has an interventionist dimension in that it is somewhat policy-oriented when studying the response of the states and potential solutions that could be adopted to try to counter this threat.

b. The comparative method: how?

The methodology for comparison was acquired mainly through academic courses of comparative politics, but also with two main handbooks for comparative method that are those of Cécile Vigour[79] and Leonardo Morlino[80].

First, regarding the material of the research, it is based mainly on literature and primary sources such as official reports and news articles, from diverse research fields, studied under a qualitative perspective. As David Chavalarias pointed out[81], potential foreign interference in elections is more a matter of intelligence services than academic research, especially on social media, due to its hidden character and the specific rules of social media, that engenders low accessibility to documents and data. The lack of access to social media data – that will be the object of further development in Chapter 3 – also represented a challenge and refrained from adopting a quantitative approach. As a matter of fact, only Twitter provides access to some data, and extensive quantitative work has already been realized on Twitter. Sensitive content was thus found mainly in official reports, drawn up thanks to the resources of the intelligence services, or by certain private companies specialized in intelligence and cyber. An added-value was found in using sources coming from as many research fields as possible and the comparison therefore encompassed a multidisciplinary approach, that helps understand this multifaceted phenomenon.

As for the methodology, the choice of a paired-comparison allowed for in-depth research on both countries, while not being too time-consuming since the available amount of time for this Masters' thesis was relatively short. The choice of the 2016 American presidential election appeared as a textbook case in terms of foreign interference in elections in that it is considered as the first case of large-scale interference in elections through social media, in a democratic country and is widely documented. The choice of the election to compare with was more difficult since the first idea was to study the most recent French presidential election of 2022. However, taking place in April 2022, the time frame appeared as too short to be able to gather any valuable information on potential interference. A delay is in fact necessary to study these interferences and reveal them (if they exist), as highlighted by the dates of main reports on 2016 American elections which rarely predate 2017. The focus on the French presidential elections of 2017 appeared not only more satisfying in that more material was available, but also in the sense that 2016 and 2017 being a closer time period, comparison was more relevant, and finally because it appeared that a major case of foreign interference in French elections of 2017, similar to the case of the United States, was highlighted by several newspapers and reports. While keeping in mind a certain necessary distance, personal interests

[79] Cécile Vigour, *La comparaison dans les sciences sociales. Pratiques et méthodes*, Repères (Paris: La Découverte, 2005).

[80] Leonardo Morlino, *Comparison: A Methodological Introduction for the Social Sciences* (Verlag Barbara Budrich, 2018).

[81] Chavalarias, *Toxic Data*.

and experiences played a role in the choice of the comparison, in the sense that, being French and having studied one year in the United States, the author developed particular knowledge and interest for both of these countries.

2. Relevance of the French-American comparison

France and the United States, if they differ in size since the U.S. is 18 times bigger than France, are relatively similar in that they both are well-established democracies and are considered as influential countries at the international level (although France to a lesser extent). Studying their democratic elections is consequently relevant, all the more so since both are presidential elections. Their use of social media is also similar in the sense that they use more or less the same social media and that the social media environment is generally open.

a. States' influence at the international level

Both France and the United States are privileged targets for foreign interference in the sense that they are – at a different scale – considered as influential countries at the international level. It seems obvious that it is more profitable for a country to succeed in favoring one candidate which shares the same interests in the United States than in a smaller country such as Liechtenstein, due to their weight and power to influence international relations. The major role of the United States at the international level is uncontested. Largest economy in the world with a Gross Domestic Product (GDP) nearly reaching 21 trillion dollars[82], the United States also has the biggest army by far (spending more in its military than the next ten countries combined), and a significant power of influence and decision in international institutions, negotiations and alliances. Historically, the United States has long played a role of leadership and if its hegemony can be disputed, it remains the most influential country in the world in the long-term. The role of the President of the United States is therefore crucial at the international level and American elections are followed closely by the entire world. Consequently, interfering in American presidential elections in favoring one candidate can significantly shape international politics and one country's interests. To a lesser extent, France is also an important actor at the international level and appears as an interesting target for electoral interference. At the international level, France benefits from overseas territories that rises the country to second place in terms of maritime power. It is also part of a restricted circle of economic powers in the G7, and political powers with its permanent seat at the U.N. Security Council, along with the restricted circle of countries in possession of the nuclear weapon. French is a widely spoken language – especially in international institutions – and France can benefit from the third diplomatic network behind the U.S. and China[83]. The role of France is particularly pregnant at the European level, with a role of leader in

[82] "Gross Domestic Product," U.S. Bureau of Economic Analysis (BEA), 2022.
[83] Frédéric Charillon, *La France dans le monde* (Paris: Cnrs, 2021).

the European Union (EU). For historical, economic and political reasons, France plays a crucial role in the EU and the decision-making. France accounts for 17.2% of the EU's GDP and contributes by 26.9 billion euros to the EU budget (representing the second largest contributor after Germany). Emmanuel Macron, as head of France, has initiated several proposals at the European level to reinforce the Alliance's strategic autonomy, or more broadly its integration and sovereignty. In this sense, trying to interfere in elections for a pro or anti-European Union leader could have a significant impact on European policies and decisions. All in all, France and the United States are both countries that can be understandably targeted by foreign actors in election interference, and the outcome of both elections can have an impact on future policies.

b. Presidential elections and political systems

Studying American and French elections is also interesting because the two are presidential elections. While the U.S. is a presidential system, France is generally qualified as a semi-presidential system. However, in both countries, the role of the President as head of State is extremely important. Presidential elections take place every four years in the U.S. and five years in France. An important aspect to highlight is that both systems are winner-takes all elections, which means that it is a majoritarian system in which there is no proportional representation of the other parties in the executive branch. The President appoints its Prime Minister and its Cabinet (government in France). Historically, the role of the President both in the U.S. and France has been put forward and the President is generally considered as the central figure of the Nation. Regarding the election, the main difference is that the French President is directly elected. France has a first-past-the-post system with two rounds, which means that the two candidates that have the most votes during the first round go to the second one, and the candidate that gets the most votes during the second round is elected. The American electorate, however, do not directly vote for their President but for an Electoral College that obtains a number of seats at the state level depending on the size of the state. This explains why, if Hillary Clinton obtained more popular votes than Donald Trump in the 2016 elections, Donald Trump was eventually elected as President of the United States. Both in the United States and France, the outcome of the election can be extremely tight and is widely awaited. Influencing hundreds of thousands of voters in this respect can therefore have a crucial impact. Due to many factors such as the extended powers granted to the President, representing a highly influential and charismatic figure, both internally and at the international level, or the fact that electors vote for one person instead of a list, the election of the President has been deeply personalized. The development of social media reinforced this phenomenon and many people today tend to vote more for the person than the political party. Consequently, political campaigns for the presidential elections in France and in the U.S. tend to rely heavily on their candidate and be built against the other candidates. This facilitates foreign interference on social media in that it is easier to support or downgrade a person (through impactful

messages, pictures or videos) than a political party. Some differences in the U.S. and French political systems are also interesting to mention in that they can represent explanatory factors of differences in states' responses. The fact that the U.S. political system is bipartisan, while the French one is more multipartite, along with the federal system characterizing the U.S. compared to the French centralized system, are differences that can have a significant impact on their approaches in combating these hybrid threats, studied in Chapter 3.

c. Electoral process and campaigns

France and the U.S. have similar political campaigns, although some rules differ, which can have a meaningful impact. France's rules regarding political campaigns are considered stricter than those in the U.S., especially with respect to campaign finance. In France, the official political campaign of the presidential election starts on the second Monday before the first round and stops the day before at midnight[84] (a crucial detail as we will see in Chapter 2). If the end of the campaign with the necessary media and candidates' silence is clear, the start of the campaign is rarely the official date, and an unofficial campaign can start as soon as someone declares themselves candidate for the election. Consequently, the political campaign usually begins when a few have made their candidacies official, around Autumn before the election that takes place in April. In comparison, there is no official regulation in the U.S. and the electoral campaign starts when the first candidate is declared. In 2016, Ted Cruz was the first to run for President, declaring himself candidate 596 days before the election[85]. The results of the primaries within the Democratic and Republican parties usually launch the final and most important part of the electoral campaign, opposing the two main candidates, although other candidates can still run for President. The electoral campaign in the U.S. is therefore considered as long and huge amounts of money are spent on both sides during the whole period. As a matter of facts, $6.5 billion were spent in the 2016 electoral campaign by candidates, their parties, and independent campaign groups, a considerable amount that is comparable to the GDPs of Monaco or Liechtenstein. In comparison, France's regulation[86] sets the maximum amount of money per candidate to 16,851,000€ and 22,509,000€ for those who made it to the second round. The amount of both Emmanuel Macron and Marine Le Pen – the two candidates in the second round – spending in the 2017 presidential electoral campaign reached only less than 30 million euros (29,114,887€)[87]. Furthermore, campaign finances are strictly controlled by the National Commission on Campaign Accounts and Political Financing (Commission nationale des comptes de campagne et des financements politiques, CNCCFP), that can impose sanctions to candidates and political parties if the

[84] "Décret N°2001-213 Du 8 Mars 2001 Portant Application de La Loi N° 62-1292 Du 6 Novembre 1962 Relative à l'élection Du Président de La République Au Suffrage Universel," 2001-213 § (2001).
[85] John Haltiwanger, "Americans Are Already Exhausted with the 2020 Election, and It's Just Getting Started. Other Countries Have Laws Limiting the Length of Campaigns.," *Business Insider*, February 10, 2020.
[86] "Comment est financée la campagne électorale de l'élection présidentielle ?," vie-publique.fr, September 13, 2021.

amount is exceeded, as it was the case in the 2012 presidential campaign of Nicolas Sarkozy. Donations and benefits from private companies are strictly forbidden, and donations from individuals are limited to 4,600€ per donor. Similar rules apply in the United States with limited public money to candidates and individuals being able to give up to $2,900 per each candidate. However, one specific rule is implemented in the U.S. since the Citizens United decision of the Supreme Court in 2010, and generates huge amounts of money in political campaigns. Due to that decision, independent groups can be formed as Super Pacs, that we often refer to as "shadow parties", in the name of the constitutional right of free speech, that can receive unlimited money from corporate and unions or anonymous sources[88]. This enables the financing of political advertising on social media at a big scale. In the 2016 American presidential election, $1,4 billion was spent on social media advertising[89]. As we will see later, social media are still legal loopholes in many aspects, both in the U.S. and in France. Regarding political advertising however, France has a strict legislation and paid political advertising in the press or online is not allowed during the six months preceding the election, according to Article 52 of the French Electoral Code. However, in the U.S., social media companies are free to choose their own policy. While Twitter, LinkedIn and other social media platforms banned political advertising before the 2020 elections, Facebook and Google chose not to, in the name of freedom of speech. This leads us to our last part regarding the use of social media in the United States and France.

d. The use of social media

When studying foreign interference on social media, it is crucial to analyze the use of social media in each country, to highlight major differences and how they could have an impact on the phenomenon studied. In order to understand and compare the use of social media in the U.S. and France, it is first essential to look at its evolution over time, and compare it to the use of traditional media. France and the U.S. are characterized by a "*hybrid media system*", as underlined by Andrew Chadwick, that are building in a "*chaotic transition period induced by the rise of digital media*"[90]. Today, in both countries, social media are being used increasingly, and represent a privileged way to follow the news[91]. In the United States for example, the proportion of people claiming to use social media as a source of news weekly has grown from 27% in 2013 to 42% in 2022, whereas for television, this number fell from 72% to 48% in the same period.

---

[87] "Présidentielle 2017 : les comptes de campagne des candidats validés par la CNCCFP," vie-publique.fr, February 13, 2018.
[88] William C. R. Horncastle, "The Scale of US Election Spending Explained in Five Graphs," *The Conversation*, October 15, 2020.
[89] Lata Nott, "Political Advertising on Social Media Platforms," *American Bar Association*, Human Rights Magazine, 45, no. 3 (June 25, 2020).
[90] Andrew Chadwick, *The Hybrid Media System: Politics and Power*, Oxford University Press, Oxford Studies in Digital Politics (Oxford ; New York, 2013).
[91] Nic Newman et al., "Digital News Report 2022" (Reuters Institute for the Study of Journalism, June 2022).

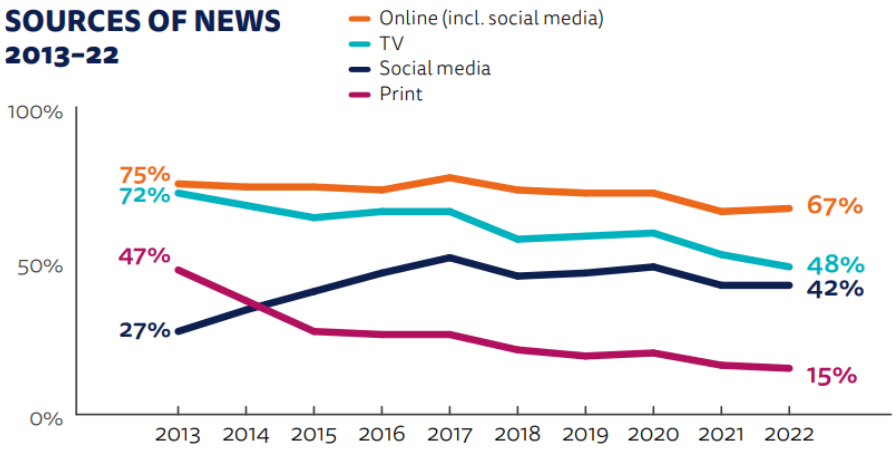

Figure 6: "Sources of news in the United-States (2013-2022)". Digital News Report 2022. *Reuters Institute for the Study of Journalism*. June 2022.

The tendency in France is similar, the number of French claiming to use social media each week as a source of news has more than doubled in less than a decade, from only 18% in 2013 to 40% in 2022, while the use of print news and television has decreased, similarly to the United States.

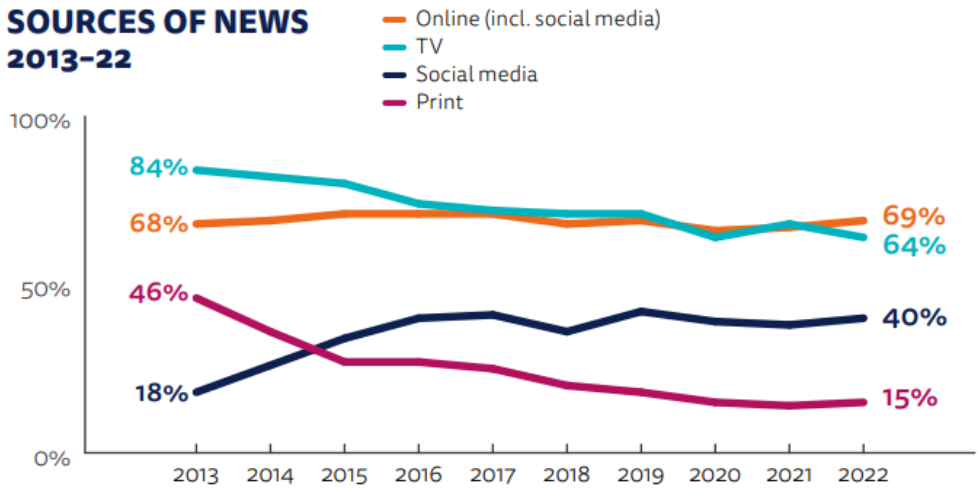

Figure 7: "Sources of news in France (2013-2022)". Digital News Report 2022. *Reuters Institute for the Study of Journalism*. June 2022

Today, the percentage of the population using social media as a source of news is more or less similar in France and the U.S. with 42% and 40% respectively. But the gap was much wider in 2013 with 27% of Americans using social media as a source of news compared to 18% in France. And if the study goes back to 2013, we can easily imagine that the gap was even larger in the years before, for historical reasons.

Social media were born in the U.S. and were used earlier and at a larger scale in the country for political objectives. Barack Obama is considered a pioneer in political campaigns on social media,

when running for President in 2008[92]. If in the same year, Facebook had only recently set up a French interface, and the platform was just emerging in France, while Twitter was not well known, the U.S. had known Facebook since 2004 and its opening to the wider public in 2006, and Twitter in 2006 as well. As soon as 2007, Barack Obama employed Chris Hughes, one of Facebook co-founders, to lead his online communication campaign. The presence of Barack Obama on social media was overwhelming since with two million followers on Facebook, he counted four times more support than his opponent John McCain, and twenty times more on Twitter. French politicians started using social media for their campaign during the 2012 presidential elections, the same year Barack Obama was reelected, with an even more developed digital strategy.

Today, online campaigns on social media are an integral part of the political campaigns and politicians count on social media to interact directly with the population. According to Dan Schill and John Allen Hendricks: "*It is not an exaggeration to say that political campaigns today are social media campaigns*"[93]. Campaigning on social media is a way for political elites to talk directly to the population, without intermediaries, which can create a link that seems stronger[94]. In a 2017 Fox News interview[95], Donald Trump claimed "*I think that maybe I wouldn't be here if it wasn't for Twitter*", and that his audience on all social media reached nearly 100 million people. Questioning the legitimacy of traditional media, Donald Trump actively reinforced the role of social media in political campaigns. The American election being closely followed in France, the role played by social media has been seriously considered and politicians gave more attention to these emerging media. Between Jean-Luc Mélenchon's Youtube channel and Emmanuel Macron's famous interviews on Snapchat with the dog filter, the 2017 election really established social media as a platform for political campaigns. And when politicians are on social media, political debate is on social media. As opposed to the traditional media environment, the social media environment being open and in free access for everyone in the world, it paved the way for foreign interference in political debate and the electoral process on social media.

[92] Andrew Chadwick, James Dennis, and Amy Smith, "Politics in the Age of Hybrid Media," in *The Routledge Companion to Social Media and Politics*, 2015, 7–22.
[93] Dan Schill and John Allen Hendricks, eds., *The Presidency and Social Media: Discourse, Disruption, and Digital Democracy in the 2016 Presidential Election*, 1st edition (New York, NY: Routledge, 2017).
[94] Kreps, *Social Media and International Relations*..
[95] *Trump: Twitter Allows Me to Get My Message Out*, 2017, https://www.youtube.com/watch?v=hKnv7krVni0.

CHAPTER 2: UNDERSTANDING FOREIGN INTERFERENCE ON SOCIAL MEDIA - PROCESSES AND MOTIVES OF INFORMATION MANIPULATION DURING AMERICAN AND FRENCH PRESIDENTIAL ELECTIONS

After having replaced the topic in its context and showed that social media could represent a threat in terms of electoral interference, we will try to understand how and why these interferences occur and in what ways we can say that they are facilitated by the functioning of social media in democracies.

Section 1 : Social media: an unregulated environment particularly vulnerable to information manipulation

First, social media being born relatively recently, there is no clear legal framework regulating it, and their functioning today, when associated with human brain characteristics, is an element that facilitates foreign interference, especially when the targeted regime is democratic.

1. The 'democratic disadvantage' on social media

The 'democratic disadvantage' on social media leaves democracies more vulnerable to foreign interference in their elections, while authoritarian regimes are somewhat protected by their closed media environment.

a. Using the democratic openness of the media…

A democratic regime, by definition, needs to guarantee pluralism and freedom of speech. As Ronald Deibert pointed out, it is crucial to take in consideration the political regime of a state when analyzing cyber issues[96]. With an independent and free press in democracies, the state has no direct control on what is published. On social media, it is particularly striking since every individual can express their opinion, and social media companies are the regulators of what can or cannot be said on their platforms. In this sense, democratic states cannot directly compel a social media company to suppress some content that would be against the state's interests. Moreover, since there are no geographical limits on social media, people from everywhere in the world can easily reach French or American citizens and communities, without having to leave their country. The open media environment is an open gate for false information to spread, since no censorship is organized to remove this type of

[96] Deibert, "Trajectories for Future Cybersecurity Research.". Op.cit.

content[97]. The U.S. National Security Agency in publishing the 2010 National Security Strategy has underlined the duality of cyberspace and its differentiated, potentially dangerous use by the following statement: "*The very technologies that empower us to lead and create also empower those who would disrupt and destroy*"[98]. Democracies indeed face a dilemma in countering foreign interference in elections on social media. This is what Sarah Kreps calls the "*double edged sword of democratic free press*"[99], according to her, "*the openness of the media environment presents vulnerabilities that can be mitigated only by reducing the transparency or access that is part of what makes a democracy a democracy*". A solution would be to operate a stricter control on online content, but this would appear as a slide towards authoritarianism. Many democracies have taken this slippery slope, controlling information on social media internally, and are now considered as hybrid regimes. It is the case of Turkey, that can hardly be qualified a democracy today, mainly due to the lack of pluralism and free speech, and whose leader Recep Tayyip Erdogan accused social media of being "*the worst menace to society*", banning Facebook, YouTube and Twitter of the country[100]. All in all, the easiest way to control national political debate is to control channels of information, including social media.

b. While being protected as an authoritarian regime by a closed media environment

Therefore, it is relatively easy to penetrate political debates of a democratic regime, while authoritarian regimes are protected in that they can filter what content appears in their state. The easiest way for authoritarian regimes to avoid electoral interference through social media is obviously to ban social media. That is why traditional social media that we know today that are born in the U.S. such as Facebook, Instagram, WhatsApp or Twitter, are not available in China. In response, China has built its own social media. WeChat (Weixin) is the platform that largely dominates the Chinese Internet with more than one billion users monthly[101]. Providing a wide range of services, WeChat is called a "Super App", with features ranging from a messaging service, to a transaction operator, or games. Other famous applications are Weibo which is similar to Twitter, and Douyin (Tik-Tok). If China closed its online environment to American platforms, Chinese social media are not limited to the country, and they are beginning to be exported abroad, as is the case of Tik-Tok, which is experiencing a tremendous success in Europe, and in the United States, after having been banned for some time by Donald Trump, for its close ties with the Chinese Communist Party regime. Russia is also filtering content on its online environment. Recently, the Kremlin has restricted access to Facebook, Instagram and Twitter, mainly in order to control the narratives around the war in

[97] Kreps, *Social Media and International Relations*.
[98] U.S. Department of Justice, National Security Strategy.
[99] Kreps, *Social Media and International Relations*.
[100] Constanze Letsch, "Social Media and Opposition to Blame for Protests, Says Turkish PM," *The Guardian*, June 3, 2013.
[101] Christina Lu, "China's Social Media Explosion," *Foreign Policy*, November 11, 2021.

Ukraine[102]. Russians are now compelled to use domestic social media platforms, such as Vkontakte or Odnoklassniki, that are deeply scrutinized by the government. As a matter of fact, former Vkontakte's CEO has been evinced, and replaced by Vladimir Sergeevich Kiriyenko, whose father is one of the closest allies of Vladimir Putin, and whose name appears on the European list of Russian figures to sanction. Thus, Vkontakte follows the Kremlin guidelines closely, and bans all discourse that is considered by Russia as false information. Consequently, we can easily understand the divide between democracies and authoritarian regimes on social media, and the offensive advantage[103] that authoritarian regimes have, being able to interfere in other countries' political debate on social media, while strictly restricting access and content in their country. If authoritarian regimes can strictly control social media in their country or ban them when they cannot control them, at the international level, rules that apply to social media are less evident. Moreover, authoritarian regimes benefit from the offense-defense advantage, in the sense that defending from information manipulation operations is much more difficult and costly than leading these operations[104].

2. Social media companies as decision-makers in a poorly regulated space

At the international level, no legal framework has been set up to regulate social media companies' behavior which means that they are often responsible for establishing the rules that will regulate their own content. Cyberspace, more broadly, has been the object of extensive debate in the field of law, in order to know what laws would be applicable to cyberspace. Cyberspace was once qualified by Barack Obama and many after him, as the new "Wild West"[105], referring to a no-law zone. Indeed, as Ronald Deibert claimed, social media and private companies on cyberspace operate in legal gray areas with "relative impunity"[106].

Today, the main point of agreement refers to the fact that international law indeed applies to cyberspace. Before recognizing cyberspace as a military domain in 2016, NATO allies had affirmed that international law applied to cyberspace[107]. Other international organizations took the same path in applying international law to cyberspace, such as the United Nations (UN) that also took further steps in building working groups with independent experts (such as the UN Group of Governmental Experts on Cyber-Security), or the G20 and the European Union. However, the debate does not stop here, and how it applies along with how it is enforced remain open questions. Important work has been done by scholars, along with international organizations, as it is the case of the UN working groups, or the group of independent experts mandated by NATO, that published two well-known reports (a third one

[102] Dan Milmo, "Russia Blocks Access to Facebook and Twitter," *The Guardian*, March 4, 2022.
[103] Kreps, *Social Media and International Relations*.
[104] Deibert, "Trajectories for Future Cybersecurity Research."
[105] Bill Chappell, "Obama: Cyberspace Is The New 'Wild West,'" *NPR*, February 13, 2015.
[106] Deibert, "Trajectories for Future Cybersecurity Research."
[107] NATO, "NATO Cyber Defence - NATO Factsheets.". Op.Cit.

is in construction): the Tallinn manuals[108], that are regularly referred to as basis for common understanding of the application of international law to cyberspace.

Applying international laws to cyberspace and defining how it can be enforced is not an easy task, for many reasons. First, international law usually applies to states, while individuals and private companies' behavior is generally regulated by domestic law. Thus, an international legal framework regarding cyberspace would necessitate a multi-stakeholder governance.

Moreover, key challenges remain, that are grouped into five main categories by Duncan B. Hollis[109]: silence, existential disagreements, interpretative challenges, attribution, and accountability. Silence refers to the fact that states have remained silent for a long time before explaining how they considered international law applied to cyberspace. Even if diverse governments have started explaining their vision in statements and speeches (starting with the U.S. in 2012), the majority of states still remain silent, either to not enter some disputes or because of a lack of resources to address the problem. Then, existential disagreements remain among states and scholars who have addressed the issue, such as if international humanitarian law also applies in cyberspace, or the possibility to invoke self-defense and retaliation, which have a huge impact on what can be done in cyberspace. These issues also depend on different interpretations of related concepts such as sovereignty or non-intervention, that can take other forms in cyberspace. Finally, the attribution of malicious actions on cyberspace and the accountability of the actors linked to those actions represent difficult legal challenges in that they resort to complex technical characteristics and uncertainty. These two final aspects will be the object of deeper analysis further in the Chapter. Therefore, due to all these issues, activities on cyberspace remain largely unregulated and are extremely difficult to frame. The basis of international law relies in great part on secondary sources or customary law, but less on actual binding legislation. In this context, social media companies have no international legal framework to rely on and are the ones responsible for establishing their rules at the international level. If, at the domestic level, states have more power to compel social media companies to respect some rules, international or regional steps that have been taken are more recommendations than binding laws. However, even at the domestic level, obtaining social media's compliance to certain laws is not easy, due to the incredible power social media companies gained, at the international level.

With billions of subscribers and huge profit margins, social media companies are becoming extremely powerful, challenging states' regulation. Mark Zuckerberg repeatedly underlined the importance of Facebook and stated that "*in a lot of ways Facebook is more like a government than a traditional*

[108] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Reprint édition (Cambridge; New York: Cambridge University Press, 2013); Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edition (Cambridge; New York: Cambridge University Press, 2017).

[109] Duncan Hollis, "A Brief Primer on International Law and Cyberspace," *Carnegie Endowment for International Peace*, June 2021.

company"[110]. With 2,7 billion active users in the world, Facebook is more populated than China, and its revenue is comparable to Argentina's GDP ($560.622 billion for Facebook and $518.092 billion for Argentina in 2019)[111]. The GAFA companies (Google, Amazon, Facebook, and Apple) have amassed such economic influence that they can also choose to exercise their own control rather than acquiescing to a legal framework that requires the removal of user content or information[112]. Thus, it is sometimes more profitable or convenient for social media companies to pay a fine than to abide with some rules that they find undesirable. Partly due to the lacking legal framework encompassing social media's functioning, and partly due to its business model, social media have vulnerabilities that facilitate the spread of dis/mis/mal-information.

3. A system vulnerable to dis/mis/mal-information, spreading faster and further

Disinformation, the deliberate spread of false, distorted or misleading messages to cause harm, is to distinguish from misinformation that refers to sharing false, distorted or misleading information unconsciously and with no intent to hurt, and malinformation that characterizes the spread of true information but in a distorted manner to cause harm[113]. Information manipulation operations therefore relies mainly on disinformation, although they can be associated to malinformation, or misinformation by foreign or domestic actors re-sharing some news. The social media environment is particularly prone to the spread of false or distorted information for several reasons. First, content filtering as operated on traditional media by editors, does not exist on social media, and every individual can publish a message without having to respond to intermediaries. This means that the flow of information on social media is much greater, and if most information is verified on traditional media – that generally do not intentionally spread false or distorted news – this is not the case on social media, on which information is not verified. With one million tweets every two minutes[114], we can easily understand that no human organization could verify each message. Second, studies have shown that false news spreads faster and at a larger extent on social media. One particularly prominent study by MIT researchers published in 2018[115] showed that "*false news spread farther, faster, deeper and more broadly than the truth in every category of information*", especially regarding political information. Working on a dataset of verified true and false news from 2006 to 2017 on Twitter, the researchers analyzed more than 126,000 stories that were (re)tweeted about 4,5 million times by 3 million people.

[110] Cited in: Franklin Foer, "Facebook's War on Free Will," *The Guardian*, September 19, 2017.
[111] Raul Amoros, "Who Is More Powerful – Countries or Companies?," HowMuch, July 11, 2019.
[112] Douzet, "Understanding Cyberspace with Geopolitics.". Op.Cit.
[113] Wardle and Derakhshan, "Information disorder."
[114] "Data Never Sleeps 9.0."
[115] Sinan Aral, Soroush Vosoughi, and Deb Roy, "The Spread of True and False News Online," *Science, with Massachusetts Institute of Technology,* March 9, 2018.

With this data, they found that false stories spread six times faster than true stories. The main reason provided is that false news tends to be more novel and surprising. Previous studies have shown that novelty is a characteristic that adds value to the news, in the sense that it gives people more social status when they share it. Therefore, people are more prone to share false news unconsciously, as it is more novel. Moreover, the main recurring emotions when reading false information are surprise, fear and disgust, whereas for true information, they are sadness, joy, anticipation and trust. The first emotions are more likely to bring strong reactions and will thus be shared more easily. One hypothesis they made for why false news spread faster than true news, and that is regularly made in the media or in research, is the fact that the presence of political bots participates in the spread of disinformation. However, they found that bots actually spread true and false information at approximately the same rate, while human beings were responsible for most of the spread of false information, mainly due to psychological reasons as mentioned above.

Bots can be defined as "*automated software operating online*"[116]. This very broad definition encompasses several types of bots, including social bots that operate on social media. Political bots are, according to Samuel C. Woolley and Philip N. Howard: "*algorithms that operate over social media, written to learn from and mimic real people so as to manipulate public opinion across a diverse range of social media and device networks*". In their book, Woolley and Howard stated that political bots are meant to amplify messages both in terms of volume and speed, and are used to manipulate information. They refer to this phenomenon as "computational propaganda", which can be defined as the "*use of algorithms, automation, and human curation to purposefully manage and distribute misleading information over social media networks*". A combination of robots and humans is therefore essential for computational propaganda and participates in the spread of misleading or false information. For them, the possibility of using bots on social media is an element that clearly disturbs political debate and can be used in malicious ways. If bots in general might not spread more false than true news as stated before, they can therefore still represent a threat if used at a large-scale for a specific campaign. Astroturfing – that stems from AstroTurf, a brand of artificial turf – for example, is one of the key techniques in information manipulation campaigns. It refers to the simulation of a large spontaneous popular movement on social media, and in politics generally the image of a large consensus over a political topic or candidate[117]. Malicious actors can therefore use bots to amplify a movement and make it appear as wide and consensual when it is actually not representative of reality. Finally, bots considerably increase the flow of messages on social media, which can participate in confusions due to information overload. In a study by Onur Varol et al., over Twitter data[118], authors estimated the percentage of bots in all Twitter accounts to 9% to 15%, while

[116] Samuel C. Woolley and Philip N. Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford Studies in Digital Politics (New York: Oxford University Press, 2018).
[117] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies.". Op.Cit.
[118] Onur Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization," March 8, 2017.

Woolley and Howard estimate it to about a third of all Twitter users[119]. If numbers vary, depending on definitions and available data, the percentage remains very high and automated accounts can be hard to detect. The possibility of generating content through bots is a characteristic of social media that makes them more vulnerable to information manipulation, along with many other techniques that will be developed further in this Chapter.

4. Exploiting vulnerabilities on social media

Malicious actors can easily take advantage of social media to manipulate information, due to the vulnerabilities of the human brain, associated with the algorithms designed by these platforms.

a. Cognitive vulnerabilities: how our brain gets tricked

"It's easier to manipulate people rather than technology."
– famous hacker Kevin Mitnick[120]

In order to understand cognitive biases, it is helpful to provide insights on the brain's functioning. Two main systems are at play in the human brain when processing information: the first is fast and instinctive while the second is slower and reflexive. The first is used to make rapid decisions and is mostly controlled by emotions, while the second takes more time since it analyzes the first evaluation and adds other factors to form a reasoning.

On social media, the balance between the two systems is altered and the first system that engages emotions takes precedence over the more reflexive system[121], due to the short messages, images and videos online. This superficial processing of information is adequate for everyday tasks, but should be substituted by reasoning for online content that requires a deeper analysis[122]. Moreover, the first system, based on rapidity and emotions, tend to be more sensible to cognitive bias detailed just after. This means that people are more easily misled and less able to detect misinformation. Several studies[123] have indeed shown that people that tend to use their reflexive system more, can more easily detect false information and are less susceptible to believe it. The fact that our brain relies more on emotions for content that we see on social media leads to cognitive biases that are unconscious and therefore not easy to counter.

---

[119] Woolley and Howard, *Computational Propaganda*.Op.Cit.
[120] In: Timothy Summers, "How the Russian Government Used Disinformation and Cyber Warfare in 2016 Election – an Ethical Hacker Explains," *The Conversation*, July 27, 2018.
[121] Chavalarias, *Toxic Data*.
[122] Herbert Lin, "Conclusion: An Outsider Looks In," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Jens David Ohlin and Duncan B. Hollis, Ethics National Security Rule Law Series (New York: Oxford University Press, 2021).
[123] Robert M. Ross, David Rand, and Gordon Pennycook, "Beyond 'Fake News': Analytic Thinking and the Detection of False and Hyperpartisan News Headlines," *Judgment and Decision Making* 16, no. 2 (March 2021); Didem Pehlivanoglu et al., "The Role of Analytical Reasoning and Source Credibility on the Evaluation of Real and Fake Full-Length News Articles," *Cognitive Research: Principles and Implications* 6, no. 1 (March 31, 2021): 24.

Our brain reacts in different ways to different messages, in the sense that they can trigger emotions that will lead to various reactions. As a matter of facts, we saw earlier that psychological factors could explain the spread of false information. The fact that false information provokes a strong emotional response is one of the characteristics that make this message more attractive, and therefore, more easily spread. Other factors highlighted by Claire Wardle and Hossein Derakhshan[124] that increase a message's attractiveness include the fact that it has a powerful visual component, a strong narrative, and is repeated. The visual component is extensively used to spread disinformation through images, videos, and often memes (that are pieces of image or videos and text generally humorous widely copied and spread on the Internet, often with slight variations). While Facebook algorithms tend to favor videos and images over text only, the human brain is also more reactive to this type of content[125]. Memes are therefore a powerful tool for foreign actors to engage in political debates and banks of memes are established to produce a large number of memes by choosing a picture and replacing the text to make humorous content that will be spread at a wider scale after. A strong narrative is also essential for stories to attract attention. Although it can be totally false, the story's authors will demonstrate why they are right, by using plausible explanations. Finally, the role of bots can be crucial in repeating a message, using what we call the repetition bias. The more one piece of information is repeated, the more the brain will tend to believe that it is true[126]. Moreover, due to the validation bias, we tend to believe this story even more if it was shared by a close relative. Because of how large our social network is, with hundreds of 'friends' on Facebook, we can readily envision that some of one's friends will post a story they just saw without checking the content, giving it more credibility in their friends' eyes. The credulity is also reinforced by the authority argument, which means that a figure of authority sharing an information will considerably reinforce its credibility[127].
Moreover, the confirmation bias, also called congeniality bias leads us to remain consistent with our preconceived ideas[128]. This means that we tend to be less critical regarding information that confirms our viewpoint. Therefore, due to the high availability of all types of content and viewpoints on social media, we can easily find a story that will confirm our analysis and re-share it, without verifying its accuracy. Finally, this confirmation bias is reinforced by algorithms that are designed in a way to suggest content in line with what the user has previously 'liked' or shared.

[124] Wardle and Derakhshan, "Information disorder."
[125] Wardle and Derakhshan.
[126] Gérald Bronner, "Les lumières à l'ère numérique," Rapport officiel de la Commission (Présidence de la République, January 2022).
[127] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[128] Chavalarias, *Toxic Data*; Bronner, "Les lumières à l'ère numérique."

b. Algorithms as generators of 'engagement', at all costs

Algorithms are characterized by technological biases that go hand in hand with cognitive biases, and are even often designed to reinforce the latter. We mentioned that algorithms tend to suggest content that confirms individuals' viewpoints. This leads to the creation of 'filter bubbles', a term that was popularized by Eli Pariser and his 2011 best seller: *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*[129]. Many studies after him confirmed that, since algorithms of social media and the Internet tend to deliver content that is linked to our interests and viewpoints, we become trapped in a social media environment that reflects our worldviews excluding alternative perspectives, leading us to a distorted vision of the society we live in. Interacting in a 'filter bubble', also known as 'echo chamber', is comforting because individuals do not need to be confronted to disagreements, so it represents a safe online place where people will mostly agree with each other. However, this is not representative of the reality and it tends to favor polarization of the society since less and less debate occurs between opposite opinions. A study by Stanford scholars showed that both France and the U.S. were experiencing greater polarization since the 1980s, with the U.S. being the most polarized of the studied countries[130]. It is indeed often stated that American citizens live in different worlds and realities due to the way information is provided in different ways. The political system, including bipartisanship in the U.S. is an aggravating factor in that it does not inspire the population to try to find consensus. For Nirupama Rao, former Indian foreign affairs' secretary, "*This is the age of anger, of political extremity, with audiences or media users who inhabit their own echo chambers and subscribe only to the views of the like-minded*"[131].

Several studies have shown that algorithms also tend to show more extreme or violent content, since they produce more 'engagement'. A study by Norwegian scholars[132] found that some emotions were overrepresented on social media content, such as anger. Not only is anger overrepresented but angry messages seem to break the filter bubble and participate in a phenomenon called "trench warfare dynamics", which is the fact that individuals on two opposite sides tend to be galvanized by the contradiction of the opposite side that leads to virulent and angry debates. This means that, while algorithms tend to suggest content that supports our viewpoints, they will also show us some opposite content, but tinged with anger or violence that might be susceptible to engage us, which will further distort our view of alternative opinions, as only extreme and angry ones are represented. The same study showed that effects of anger leads to a less constructive debate, in the sense that this emotion tends to reduce our capacity to engage with the reflexive part of our brain, to overcome preconceived

[129] Eli Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think* (London: Penguin Books, 2011).
[130] Levi Boxell, Matthew Gentzkow, and Jesse M. Shapiro, "Cross-Country Trends in Affective Polarization" (Stanford University, November 2021).
[131] Nirupama Rao, "Diplomacy in the Age of Social Media," *The Wire*, July 19, 2017.
[132] Dag Wollebæk et al., "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior," *Social Media + Society* 5 (April 1, 2019).

ideas and stereotypes, to refute a false information if it supports our argument, or to moderate our discourse and try to find compromise. All in all, "*the association between anger and engagement in online debates does not bode well for the quality of the public sphere*"[133].

Furthermore, algorithms tend to favor violent content. One study showed that Youtube's algorithms favor more extreme content, and even tend to favor far-right extremist content and conspiracy theories[134]. When looking for specific news coverage, Youtube tends to suggest more of that content, even when the individual does not engage in any way with that content. Once the user has engaged with far-right extremist content related to the news, the algorithm goes further in suggesting almost exclusively this type of content, even though not related to the news that was looked for initially. In the same way, algorithms tend to favor more conservative than liberal parties, as found by a study on 9,3 million Twitter users in seven countries (including the U.S. and France). In all countries, conservative discourse was amplified by algorithms[135]. False information is also favored by social media algorithms, since they favor engagement by arousing strong emotions such as outrage and anger, as we analyzed previously.

Although social media are well aware of these phenomena, their algorithms keep favoring these types of content and create filter bubbles, because of their need to foster 'engagement'. Engagement is what makes users spend more time on social media, and is the basis of social media's business model. Individuals' news feed is therefore completely altered by what social media want users to see to keep them engaged, and as we showed in this section, this is not conducive to a healthy and fair political democratic debate. Technological biases of algorithms, along with cognitive biases therefore form an environment that is particularly vulnerable to information manipulation. Coupled to a particular societal context, malicious foreign actors can use countless techniques to interfere in the political debate during elections, that play on these pitfalls for greater efficiency.

Section 2 : Techniques and processes of information manipulation in the U.S. and France

After having analyzed different possible methods of information manipulation on social media, we will analyze similar methods that were employed in the U.S. and France, underlining the *modus operandi* of one particular actor: Russia. However, we will see that the scale of these operations was different in the U.S. and France, along with the level of available proof of the intervening actors.

[133] Wollebæk et al.

[134] Max Fisher and Katrin Bennhold, "As Germans Seek News, YouTube Delivers Far-Right Tirades," *The New York Times*, September 7, 2018.

[135] Cited in: Chavalarias, *Toxic Data*. Op.Cit.

1. Analyzing methods for information manipulation

Social media offered new opportunities for foreign actors to manipulate information and interfere in national elections. The cases of the U.S. and France in 2016 and 2017 offer valuable insights on the use of these techniques and their efficiency.

a. Mapping of the techniques employed to spread, amplify and target a message

Actors that want to manipulate information have a wide range of opportunities to exploit social media vulnerabilities and achieve their ends. These techniques can be grouped into main interrelated categories: microtargeting, disinformation, amplification of the information, or personal attacks, usually cyberattacks (such as theft of personal information) associated with communication on this attack (disclosure of personal information).

The first type of technique that comes to mind when analyzing foreign interference in elections through social media is the resort to disinformation. Several elements are essential for an efficient disinformation campaign, but the main goal is to try to appear credible enough, through the creation of stories with a powerful narrative, as mentioned above, and a large support to repeat the story. As RAND analysts have highlighted in 2016, the "firehose of falsehoods" propaganda model relies on the massive amplification of false information, blended with true or distorted information, leaving the debate unreadable and confusing the population[136]. In order to do that, actors can rely on several tools, including automated tools that have a crucial impact[137].

Sock puppets are defined as social media accounts created as fake personas to promote ideas or share false information. Trolls are considered as accounts regularly interacting on the Internet with an objective of causing controversies, generally to provoke emotional responses. Bots are automated accounts amplifying activities and messages on social media. While bots are entirely automated, trolls and sock puppets are controlled by humans, although under another identity. The institutionalization of trolls and sock puppets is facilitated through troll farms, which organize and pay people to carry out coordinated actions online[138]. Account hijacking is also used to take the control of an already existing account. Foreign actors, when trying to penetrate a national political debate through social media, must coordinate their actions between automated and human accounts. Jarred Prier has mapped out this process[139], useful for understanding the dynamics and actors involved in introducing a message into an external sphere.

[136] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model - Why It Might Work and Options to Counter It" (RAND Corporation, July 11, 2016).
[137] Woolley and Howard, *Computational Propaganda*.
[138] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[139] Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017).

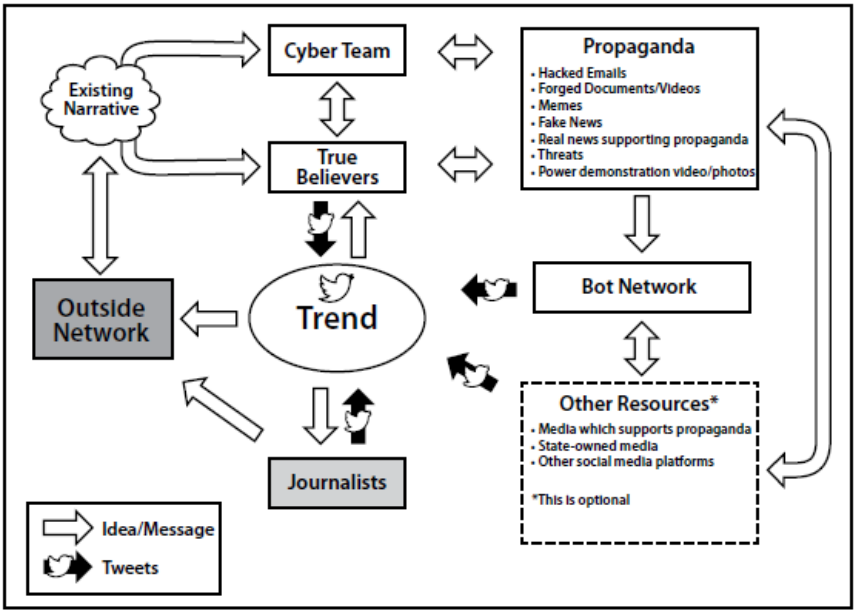

Figure 8: Process map of how propaganda spreads via the trend, Jarred Prier, 2017.

The cyber team (operating in troll farms mostly), is here to share messages that include propaganda in an already existing narrative, that will be linked unconsciously and shared by true believers that are real individuals that genuinely believe the news. The trend is created with the help of bots that share massively the information, and of journalists that relay the information. The reporting of information in the traditional media is crucial in the extent to which it legitimizes the information. All this enables the message to become a trend and be seen by a wider public with no direct link to external actors, and not ideologically in phase with true believers.

Social bots are designed to mimic human behavior as closely as possible, *e.g.*, creating social media accounts on diverse platforms with the same name, acting according to a credible human sleep-wake cycle, etc. However, despite those techniques, and the development of artificial intelligence that can recreate more and more human behavior, bots are usually more easily identifiable than trolls. A mix between humans and robots is therefore essential to reach a large number of people, while still spreading a message that seems authentic, hence the role of accounts controlled by real people coupled to the bots[140]. These tools are used to amplify messages and create a trend, and are therefore used to manipulate information, although not all messages are disinformation. This is why referring to information manipulation is preferable to disinformation, in the sense that it includes other techniques that manipulate information to influence the elections, without resorting to false information.

In general, there are three main ways to command a trend on social media, either by creating the trend from the start – method which necessitates the more resources but efficient; by hijacking a trend – through extensive shares; or by trend distribution – which amounts to spread a message through already existing trends that have no link with the message but are extremely popular. An example of trend distribution would be to post a meme against a candidate with an irrelevant but popular hashtag,

such as #SuperBowl, so that every person that looks for information on the SuperBowl with the hashtag will see the propaganda meme[141].

These amplifiers of messages are also essential in the use of another technique of information manipulation, that is the 'hack-and-leak' operations. These operations link a cyberattack to an information operation. The cyber team of external actors first tries to hack a political party or a candidate, logically rival to the one supported by them. This is usually made through a technique of phishing, i.e., sending a fraudulent link to the target that allows (through the victim's click) the author to obtain access to the desired data. The goal is then to spread the stolen information to the population. This type of operation was used both in the American and the French presidential campaigns of 2016 and 2017, analyzed in the following point.

Another way to manipulate information is through microtargeting. Social medias' financial model is based on advertisement, and the more advertisement is seen, the more money social media win. Therefore, in order to increase users' engagement and visibility of advertisement, the content is targeted to specific individuals, using their personal data. Data used are all the data available on social media such as age, sex, hobbies or interests. By liking a Facebook page on running, an individual is more susceptible to receive ads of running shoes for example. However, this can also be used for political purposes. Political parties can pay to promote content, and use social medias' data to target specific individuals that could be responsive to the political campaign[142].

Legislation has changed rapidly on the topic of political advertising with Twitter forbidding it and France applying strict rules that forbid political advertising on all social media during political campaigns. However, on other social media such as Facebook and YouTube, political advertising is still possible in the U.S., and no specific rule has been established for advertising on social topics, although the line between social and political is sometimes blurry. This means that microtargeting for political purposes is still possible, and political campaigns can differ significantly when addressed to an individual or another.

Once established a mapping of the main techniques and tools used to spread, amplify and target messages in information manipulation campaigns by foreign actors, although the list is not exhaustive, we will now provide more detailed analysis on the specific cases of the 2016 and 2017 American and French presidential elections.

b. A similar pattern in the U.S. and France in election disruption

Both in the U.S. and France, claims were made about a foreign actor interfering in presidential elections (in both cases, Russia was at the center of accusations). This claim was supported by more or

---

[140] Woolley and Howard, *Computational Propaganda*.

[141] Prier, "Commanding the Trend."

[142] Michaël Szadkowski and Damien Leloup, "Tout comprendre aux publicités politiques sur les réseaux sociaux," *Le Monde*, November 6, 2019.

less strong evidence that these operations can be attributed to Russia, which will be the object of deeper analysis later in the Chapter. In this part, we will focus essentially on the techniques used to highlight similarities and differences between the two cases. In the presidential elections in the U.S. and France of 2016 and 2017, the same pattern of information manipulation can be evidenced, despite some discrepancies.

The general pattern that is usually followed is a phase of preparation, with the building of fake accounts and integration in debates or communities, to then reach a phase of large diffusion of propaganda and disinformation messages. At one point in the campaign, a specific operation with high impact is integrated as a phase that takes place at a specific chosen moment[143]. For both campaigns, this high impact operation was characterized by what we call a 'hack-and-leak' operation, *i.e.*, the unauthorized intrusion in private computers of one candidate or political party members, stealing of private data and release of these information, generally followed by a campaign of amplification to give visibility to these documents[144]. The most used technique by hackers for accessing confidential data and documents is through *phishing*: they send an email pretending to be a trustful company, person or institution and include a link on which a click by the target will grant access to personal data. This technique was used both in the U.S. and France.

In the U.S., private files, emails and documents were stolen to the Clinton campaign through the intrusion in the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) computer networks, around April 2016. This cyberattack was possible through a *phishing* operation that successfully tricked an employee, which permitted the planting of a malware in a total of 29 computers, granting access to private documents[145]. The documents were released by purposefully created websites "DCLeaks" and "Guccifer 2.0", along with the organization WikiLeaks later. A second round of email leaks were linked to John Podesta's, after being victim of a phishing operation also.

In February 2017[146], Emmanuel Macron's campaign team in France observed numerous attempts to penetrate their networks, coming from tens of thousands different computers simultaneously, which suggested an organized operation. In May 2017, during the last political debate, Marine Le Pen mentioned potential tax evasions by Emmanuel Macron. At the same time, two documents purporting to be proofs of the tax evasion (later proven to be false), were circulated on "4chan" by William Craddick, founder of Disobedient Media, a pro-Trump American media, famous for having spread the Pizzagate rumor that we will mention later. Two days later, Disobedient Media warned for something big to come. Indeed, a few minutes later, that is to say at 8:35pm, a few hours before the end of the official political campaign[147],

[143] Chavalarias, *Toxic Data*.
[144] Susan Davis, "Russian Meddling in Elections and Referenda in the Alliance," Science and Technology Committee (USA: NATO Parliamentary Assembly, November 18, 2018).
[145] Robert S. Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election" (Washington D.C.: U.S. Department of Justice, March 2019).
[146] Jean-Baptiste Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem," *Atlantic Council*, June 2019, 58.
[147] Cf the next section for more information on the French official campaign.

more than 150,000 documents were published on the website "4chan" and spread on social media with the hashtag #Macronleaks (first used by Jack Posobiec). In France also, WikiLeaks has largely participated in the diffusion of the hashtag and the leaks[148].

Moreover, both campaigns were characterized by a large diffusion of false and distorted information. From precise and elaborate conspiracy theories to simple false facts, disinformation has infiltrated the electoral campaign. In the U.S., uncountable false stories circulated, mainly targeted at Hillary Clinton and the Democratic Party. On the one hand, Clinton was accused to have approved a sale of weapons to ISIS, or to be linked to a pedophile underground network (the famous "pizzagate"). She was also said to be seriously ill, questioning her ability to govern. On the other hand, false stories favorable to Donald Trump also emerged thanks to amplification techniques, such as the fact that the Pope endorsed him, which, despite its inaccuracy, was shared more than a million times[149]. In France, stories of Emmanuel Macron being gay, having hidden bank accounts, being supported by Saudi Arabia or Al-Qaeda, and many others, circulated[150]. All these stories were spread through memes, false articles or cut video extracts, to stain the candidate's image.

Evidence of foreign implication is always difficult to prove (cf. later in the Chapter), however, both in the U.S. and in France, foreign actors were involved in some ways in national elections. In France, we can find evidence of foreign implication in the campaign, especially in the spread of the Macron leaks. As mentioned before, the documents were first published by an American account, and indeed, in the next hours, content about the WikiLeaks was spread almost exclusively by American accounts, which is relatively easy to show since all the posts were written in English, yet French people rarely talk about their national political campaign in English. The same English pattern was found in broader information manipulation campaigns through the dissemination of anti-Macron memes, that were written exclusively in English, and in fact, two messages out of three containing the hashtag "MFGA" (Make France Great Again) can be traced back to the United States[151]. However, if American alt-right communities participated in information manipulation in the French campaign, it is impossible to refer to it as foreign interference in elections as a state-sponsored operation, in the sense that the state was in no way linked to the alt-right communities. Evidence of Russia's implication is more difficult to prove although very likely, and will be discussed later. Regarding American elections, evidence of Russia's interference in elections has been extensively discussed and the Mueller or the U.S. Senate Select Committee on Intelligence reports that will be detailed further provide significant evidence to prove that Russia interfered in American elections[152].

---

[148] Naz Durakoglu, "Hashtag Campaign: #MacronLeaks," *DFR Lab - Atlantic Council*, May 8, 2017.
[149] Prier, "Commanding the Trend."
[150] Marie de Fournas, "Présidentielle: 14 fake news qui circulent sur Emmanuel Macron," *20minutes*, April 28, 2017.
[151] Chavalarias, *Toxic Data*.
[152] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election"; U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V" (U.S. Senate Select Committee on Intelligence, 2020 2019).

In both countries, documents' leaks and the spread of false information was deeply amplified by bots. As an example, leaks were spread in a short lapse of time, which can make us think that they benefited from amplification tools. In France, a few hours were sufficient for the Macron leaks to reach high visibility. According to the Digital Forensic Research Lab (DFR Lab)[153], renowned for its studies on disinformation, ten main accounts related to the #MacronLeaks hashtag totaled more than 1,300 tweets in only three hours. Some of these accounts averaged 150 to 200 posts per hour, which is uncommon for people to do. In the U.S., a study[154] showed that: "*during waking hours, highly automated accounts were generating between 20 and 25 percent of the traffic about the election during the days leading up to the vote*". They also found that a vast majority of these accounts were deleted as soon as elections' results were released, another sign of automated accounts.

The main difference in analyzing tools and techniques that were employed in election disruption was the use of psychographic targeting, through microtargeting. On the one hand, in France, no evidence of microtargeting was found, although it remains very likely, the scale to which it was used might not be meaningful. On the other hand, the use of microtargeting in the U.S. is extensively documented and has been the object of an infamous scandal regarding Cambridge Analytica. Cambridge Analytica was a company that used personal information on social media users, to set profiles and provide detailed information so as to target specific groups or individuals. It is intended to make individuals' political choice appear spontaneous[155]. If proof of the use of Cambridge Analytica by the Trump campaign has been found, links with Russia are not evident. However, the U.S. Senate Select Committee on Intelligence found that Russia's Internet Research Agency (IRA), a company considered as a 'troll farm', and linked to Russian officials, funded targeted political advertising on social media and had an interest in favoring Donald Trump, as we will see later in the Chapter[156]. In the Intelligence Community Assessment of January 2017, a report by U.S. Intelligence agencies, it is claimed that the IRA purchased a total of 3,519 advertisements on Facebook, which are considered to have reached more than 11.4 million Americans[157]. In the legal case United States of America V. Internet Research Agency LLC, they found that more than one million dollars were spent by the Russian government each month towards the end of the campaign for online propaganda[158]. Microtargeting is generally used to convince some individuals and groups to vote for a candidate. As an example, it can be used to target pro-conservative individuals in exposing them to content representing candidate Trump as an advocate for the right to bear arms when the data shows that the individual has liked the National Rifle

[153] Naz Durakoglu, "Hashtag Campaign: #MacronLeaks," *DFR Lab - Atlantic Council*, May 8, 2017.
[154] Bence Kollanyi, Philip N. Howard, and Samuel C. Woolley, "Bots and Automation over Twitter during the U.S. Election" (Oxford, UK: Project on Computational Propaganda, November 17, 2016).
[155] François-Bernard Huyghe, "Que changent les fake news ?," *Revue internationale et strategique* 110, no. 2 (June 29, 2018): 79–87.
[156] U.S. Senate Select Committee on Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections" (Office of the Director of National Intelligence, January 6, 2017).
[157] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," U.S. House of Representatives Permanent Select Committee on Intelligence, May 2018.
[158] United States of America V. Internet Research Agency LLC, No. Case 1:18-cr-00032-DLF (February 16, 2018).

Association (NRA) page. The main goal here is to link people's interests to a candidate, but also to make them go to the polls or not. In the case of the 2016 U.S. elections, the use of microtargeting, since it mostly favored Donald Trump, was done in order to convince conservatives to go vote, whereas for individuals considered as more liberals, the goal was to convince them not to vote. For example, campaigns targeted mainly at African-American communities, or LGBTQ and Latino communities, historically and demographically generally more favorable to Democrat candidates, were designed to discourage them to vote for Hillary Clinton, through the spread of false or distorted information on her[159]. Interestingly, the vast majority (65%) of Russian advertising was indeed targeted to populations considered as more progressive[160]. According to a report by New Knowledge researchers, requested by the U.S. Senate, IRA content consistently targeted Black-communities in the last days before the election to incite them to not vote[161].

Figure 9: IRA-related content on Twitter. Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency", *U.S. Senate Documents*, 2019.

c. … At a different scale and more or less successful

The main differences in the two elections depend on the scale to which information manipulation was undertaken, and their success.

France is often considered as a 'success story' in terms of mitigating negative effects of information manipulation operations. In France in 2017, Emmanuel Macron eventually won the presidential elections by far (66,10% for Emmanuel Macron *versus* 33,90% for Marine Le Pen), which can make us think that the overall impact of this anti-Macron information manipulation campaign was low. For Jean-Baptiste Jeangène Vilmer, they "*neither succeeded in interfering with the election nor in antagonizing French society*"[162]. Whether the MacronLeaks or the broader information manipulation

[159] Pamment et al., "Countering Information Influence Activities."
[160] Pamment et al.
[161] Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency", *U.S. Senate Documents*, October 1, 2019.
[162] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."

campaign, relayed by the American alt-right, were not successful and largely remained within American circles.

Cyberattacks targeted at Macron's campaign team were considered as destabilizing, but not so as to hinder their activity, in a report by the French CNCCEP[163], supposed to monitor the proper conduct of the elections. However, the Commission was not asked to produce a report on election interference in order to assess the impact of information manipulation operations in the final election.

Conversely, in the U.S., several official reports showed the scale of election interference through information manipulation *via* social media, and how they favored candidate Donald Trump. Several studies even showed that these operations of information manipulation might have cost the election to Hillary Clinton. Although the success is disputed, the overall negative effects of these operations over the election are largely accepted. Few are the people that refute the idea that information manipulation operations had an impact on 2016 American elections, if not in deciding the outcome, then in disrupting the electoral campaign in a broader sense. Studies have shown that disinformation posts linked to Russia on Facebook were seen by roughly 126 million Americans over the period of the electoral campaign, 20 million on Instagram and 1.5 million on Twitter[164].

Taking into account the fact that this election was extremely close in the sense that Hillary Clinton won the popular vote, it is generally agreed that thousands of vote in some key states could have changed the outcome of the election. For Jens David Ohlin[165], approximately 80,000 votes in southern key states for Democrats could have made Clinton President. When you take into account that 126 million Americans were impacted by Russian disinformation, it only takes a small percentage of those people to have been misled about Clinton and voted for Trump, or more likely, ended up not voting when they would have voted for Clinton otherwise, to change the outcome of the election. A study from Ohio State University researchers[166] showed that roughly 4% of people who voted for Barack Obama in 2012, did not vote for Hillary Clinton in 2016 because they believed false information about her. Through a multiple regression analysis, authors were able to isolate some independent variables and found that without any false information in the key states of Michigan, Pennsylvania and Wisconsin (in which she lost by less than 1%), Hillary Clinton would have won those states, and therefore the election. These two operations have, hence, been more or less successful depending on the country, which can be explained by different factors.

[163] "Rapport Établi Par La Commission Nationale de Contrôle de La Campagne Électorale En Vue de l'élection Présidentielle (Scrutins Des 23 Avril et 7 Mai 2017)" (Commission Nationale de Contrôle de la Campagne Electorale en vue de l'Election Présidentielle (CNCCEP), n.d.).

[164] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements."

[165] Jens David Ohlin, "A Roadmap for Fighting Election Interference," *American Journal of International Law* 115 (ed 2021): 69–73.

[166] Alexandre Bovet and Hernán A. Makse, "Influence of Fake News in Twitter during the 2016 US Presidential Election," *Nature Communications* 10, no. 1 (January 2, 2019): 7.

2. Explaining differences in the information manipulation operations' success

Main differences in political and electoral systems, foreign actors' campaign sophistication or anticipation of the threat, can help explain why the information manipulation campaign was more successful in the U.S. than in France.

a. Key differences in political and electoral systems and the importance of bipartisanship

Majoritarian systems with one round are more susceptible to produce bipartisan political environments. The American political system is extremely polarized around two main parties, the Republican and the Democrat parties, and presidential elections take place in one round. This makes it easier for foreign actors to understand the political landscape and place a wager on a particular candidate. On the other hand, in France, the two rounds lead to a political system favorable to multiple parties, which means that it is impossible to know which candidate will reach the second round. This means that it is riskier to launch a campaign favoring one candidate, if there is a possibility that this candidate does not make it to the second round[167]. Polls can help in this sense to have a better idea of candidates that are most likely to win the first rounds, however, they are not totally reliable and can evolve rapidly. While in the U.S., the information manipulation campaign was clearly favorable to Donald Trump (cf. same Chapter later), this was not as clear in France. If Emmanuel Macron was clearly the target of an anti-Macron campaign due to his liberal, centrist and pro-European positions, support was initially provided to François Fillon, right-conservative candidate, whose probability to reach the second round was considered high, and had good relations with Russians. However, after the "Pénélopegate" scandal on fictitious jobs, the campaign shifted towards support for Marine Le Pen[168]. In the end, the most active part of the foreign information manipulation operations started late, once the two opposing candidates for the second round were known, leaving less than two weeks to have a meaningful impact. As a result, the two-rounds and multiparty electoral system in France might have participated in the relative failure of the operations. On the contrary, campaigning for or against a candidate when only two parties are opposed to each other, and are historically well anchored in the society and people's minds, is consequently more straightforward.

b. Levels of campaigns' sophistication and potential errors from foreign actors

The significance of the election for foreign actors should logically explain the means and implication granted to the information manipulation operation. The outcome of the U.S. presidential elections undoubtedly has higher repercussions on foreign actors, especially for Russia in this case, than French presidential elections. The sophistication of the attack can therefore be proportionate to the

[167] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[168] Emmanuel Grynszpan, "Les médias pro-Russes s'engouffrent dans le tout sauf Macron," *Euractiv*, February 14, 2017.

importance of the country and interests at stake. We can imagine that fewer resources were employed for interfering in French elections than for the U.S. elections, which can explain part of why it was less efficient.

Mistakes were made by foreign actors, which had a detrimental effect on the operation's effectiveness. First, leaks were released a few hours before the end of the official campaign. Yet, in France, electoral campaigns are regulated by several laws, including Article L48-2 of the electoral code, that prohibits media from covering the campaign starting the day before the vote at 0.00. Candidates and political parties are not able to communicate. Given the time of the publication of the MacronLeaks, a few hours before the closing of the official campaign, the news did not have time to spread at a large scale and was relayed mainly by U.S. alt-right, i.e. in English, which had logically less impact on French people. The choice of the timing was a gamble in the sense that, since political parties could not communicate, Emmanuel Macron was unable to defend himself and respond to the attack. However, it was a double-edged sword, as the leaks did not have time to spread massively and the impact was therefore minimal. Moreover, the main goal of the operation was to overwhelm French people with a massive flow of information and to send a message to the population: the fact that there is a leak is a sign that the candidate or party has something to hide[169]. Nevertheless, the release of such a huge number of documents discouraged many from looking at them and no suspicious activity from Macron's team was found. In 2016, the release of the DNC leaks emphasized specific emails and shocking revelations on how the DNC favored Hillary Clinton over Bernie Sanders for the Democratic primaries, and was released just before the Democratic National Convention, causing Debbie Wasserman Schultz to resign as the DNC Chairman[170]. Similarly, emails' leaks from John Podesta, chairman in the Clinton's presidential campaign revealed questionable practices, although not illegal, from the Clinton's campaign team[171]. Thus, leaks in the U.S. were published purposefully for specific controversial documents, whereas the MacronLeaks revealed nothing controversial, perhaps meaning that the actors did not have time to sort through the information.

c. Anticipation of the threat: 2016 U.S. elections as a warning for France

One major factor that was favorable to France in countering the information manipulation campaign, was the preparedness of the campaign teams and the country to this threat. France had time to hear about the 2016 scandal regarding Russian interference in U.S. elections, that blew the whistle and raised awareness in other countries regarding potential similar threats. Therefore, François Hollande, incumbent President at the time, along with his administration, have shown a strong commitment to

[169] Martin Untersinger, "Les preuves de l'ingérence russe dans la campagne de Macron en 2017," *Le Monde.fr*, December 6, 2019.

[170] James Lamond and Jeremy Venook, "Blunting Foreign Interference Efforts by Learning the Lessons of the Past" (Center for American Progress, September 2, 2020).

fighting disinformation, and put pressure on social media companies[172]. Facebook ended up suspending 70,000 fake accounts, ten days before the election[173]. Other steps were taken by the French administration in order to deter foreign actors, especially Russia after been warned of Russian attacks, from interfering in the elections. Messages were sent by François Hollande to Vladimir Putin, and by French Defense minister Jean-Yves Le Drian to his Russian counterpart, as well as a public announcement that "*France reserves the right to retaliate by any means it deems appropriate*", through cyber or conventional military means[174].

Furthermore, U.S. intelligence services that were monitoring Russian activities, in particular those of the IRA, warned 21 countries that Russian tried to enter the national electoral database[175]. NSA Director Michael Rogers claimed that he specifically informed French officials that Russians were trying to penetrate French digital infrastructure[176].

French agencies monitoring the elections, such as the ANSSI (that aims to secure information), and CNCCEP, responded well and "*alerted the media, political parties and the public to the risk of cyberattacks and disinformation during the presidential campaign*"[177]. Emmanuel Macron's campaign team, that was informed, and also faced hacking attempts of their networks, therefore had the occasion to prepare and respond to the attack. They deliberately integrated false documents and false emails in their database, which means that when the leaks were published, since no tri was made, the false documents were also published, despite their rough nature, which delegitimized the whole leak. For example, the false document of the soi-disant bank account of Emmanuel Macron in the Bahamas was integrated purposefully by Macron's team and signaled to the ANSSI agency prior to the leaks[178].

Macron's campaign team also responded efficiently by publicizing the fact that hacking attempts were operated by foreign actors, which informed the public about potential information manipulation, and raised awareness on the topic. Benjamin Griveaux claimed that, after the U.S. and the U.K., Russia was "*interfering in the French presidential campaign, and that [was] not normal*"[179]. However, finding the responsible actor is not that easy, and if many indications point to Russia, official proof is not always evident.

---

[171] Sam Frizell, "What Leaked Emails Reveal About Clinton's Campaign," *Time*, October 7, 2016.
[172] Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."
[173] Margaret L. Taylor, "Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe," *Brookings*, TechTank, July 31, 2019.
[174] In: Jean-Baptiste Jeangène Vilmer, "Information Defense: Policy Measures Taken against Foreign Information Manipulation" (Atlantic Council, July 22, 2021).
[175] Davis, "Russian Meddling in Elections and Referenda in the Alliance."
[176] Andy Greenberg, "NSA Director Confirms That Russia Really Did Hack the French Election," *Wired*, May 9, 2017.
[177] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[178] Benjamin Terrasson, "Présidentielle 2022 : comment s'organise sa cybersécurité ?," *Siècle Digital*, October 14, 2021.
[179] J. CI, "L'équipe de Macron persuadée d'une ingérence russe dans sa campagne," *Le Parisien*, February 13, 2017.

3. Who got in the way? The challenging task of identifying the culprits

If we can highlight similar Russian techniques and tools employed for interfering in elections, the attribution of cyberattacks in general, and information manipulation operations on social media, is often delicate, and if the U.S. officially attributed it to Russia, the French government never explicitly accused the Russian government of such information manipulation operation.

a. Same actors: Evidence of Russia's *modus operandi*

Russia's interference in the U.S. presidential election of 2016, has been proven by several official reports, such as the U.S. Senate Select Committee on Intelligence reports in five volumes[180] for a total of 1,313 pages with more than 200 witnesses and a million documents reviewed[181] published between 2019 and 2020. Another important report is the so-called 'Mueller report'[182]. Robert S. Mueller, former FBI Director, was commissioned by the U.S. executive to investigate Russian interference in the 2016 presidential elections, and the potential links with the Trump administration. Through testimonies (including the famous one of James Comey, FBI director at the time of the election), interviews, data analysis, and diverse intelligence techniques, Robert S. Mueller and his team collected a considerable amount of valuable information. This huge work resulted in two volumes of more than 400 pages on the topic. Main findings were that Russia indeed interfered in elections, favoring candidate Donald Trump. Nevertheless, no strong evidence has proven the links between Donald Trump and Russian officials, although some details highlighted show that it is very likely. The second report moves away from Russian interference, to focus on Donald Trump's obstructions of justice[183].

Attorney General Rod Rodenstein affirmed that DcLeaks and Gucifer 2.0, that published the DNC and Podesta Leaks, were created and administered by Russian GRU, the Main Intelligence Directorate of the General Staff of the Russian Army[184]. The Mueller report also found that the IRA, controlled and financed by Russian officials with close ties to Vladimir Putin (including the famous Yevgeniy Viktorovich Prigozhin), moved from a general social media campaign designed to "*provoke and amplify political and social discord in the United States*" already in 2014, to a "*targeted operation that by early 2016 favored candidate Trump and disparaged candidate Clinton*"[185]. The large-scale operations and established links between activities, agencies, and the government, evidenced a state-sponsored campaign, controlled by Russian authorities.

---

[180] U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V."

[181] "Press Release of Intelligence Committee: Senate Intel Releases Volume 5 of Bipartisan Russia Report," U.S. Senate Select Committee on Intelligence, August 18, 2020, https://www.intelligence.senate.gov/press/senate-intel-releases-volume-5-bipartisan-russia-report.

[182] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

[183] This part will deliberately be left behind, as not directly linked to our topic.

[184] Davis, "Russian Meddling in Elections and Referenda in the Alliance."

[185] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

As we saw earlier, similar techniques were used in France, which remind Russian *modus operandi*. Since no official report was established in France, main proof come from private cyber companies (Trend Micro, FireEye) or investigative journalism. An interesting article was published by LeMonde[186], thanks to interviews with two Google experts, and with specialists from the FireEye company, that tracked Russian hackers for private reports, and opened one of their reports to the public. It was found that first hacking attempts against Emmanuel Macron and his relatives or collaborators were operated by APT-28 (also referred to as FancyBear, or Pawn Storm), a Russian hacker group linked to the GRU. The link used for Macron's phishing operation was also found in GRU communications[187]. APT-28 is also considered to have conducted the phishing operation against Clinton's team in the DNC Leaks[188].

A report by Trend Micro, a Japanese cybersecurity company detailed the activity of APT-28, that they call Pawn Storm, underlining the numerous operations in which the group was involved, including the U.S. and France[189].

Date	Organization	Phishing Domain
04/01/16	Democratic Party US	myaccount.google.com-changepasswordmyaccount-idx8jxcn4ufdmncudd.gq
04/22/16	CDU	webmail-cdu.de
05/06/16	CDU	support-cdu.de
06/06/16	Democratic Party US	actblues.com
10/20/16	Parliament Montenegro	mail-skupstina.me
03/15/17	Emmanuel Macron campaign	onedrive-en-marche.fr
04/05/17	Konrad Adenauer Stiftung	kasapp.de

Figure 10: Extract from Feike Hacquebord, "Two Years Of Pawn Storm: Examining An Increasingly Relevant Threat", *Trend Micro*, 2018.

Moreover, in examining documents of the Macron Leaks published first on 4Chan, it was found metadata in Cyrillic, which indicates Russian origins[190]. According to investigations, around April just before the election, APT-28 was replaced by another well-known hacker group: Sandworm, which is known to operate in risky and rushing situations[191]. FireEye is the company that first discovered Sandworm, a unit that is directly linked to the GRU and that operated in other famous information

[186] Untersinger, "Les preuves de l'ingérence russe dans la campagne de Macron en 2017."
[187] Andy Greenberg, "Hackers Hit Macron With Huge Email Leak Ahead of French Election," *Wired*, May 5, 2017.
[188] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."
[189] Feike Hacquebord, "Two Years Of Pawn Storm: Examining An Increasingly Relevant Threat" (Trend Micro, October 17, 2018).
[190] Greenberg, "NSA Director Confirms That Russia Really Did Hack the French Election."
[191] Untersinger, "Les preuves de l'ingérence russe dans la campagne de Macron en 2017."

manipulation operations, as illustrated thereafter by the company, that gave access to this content of an unreleased report to Andy Greenberg[192].

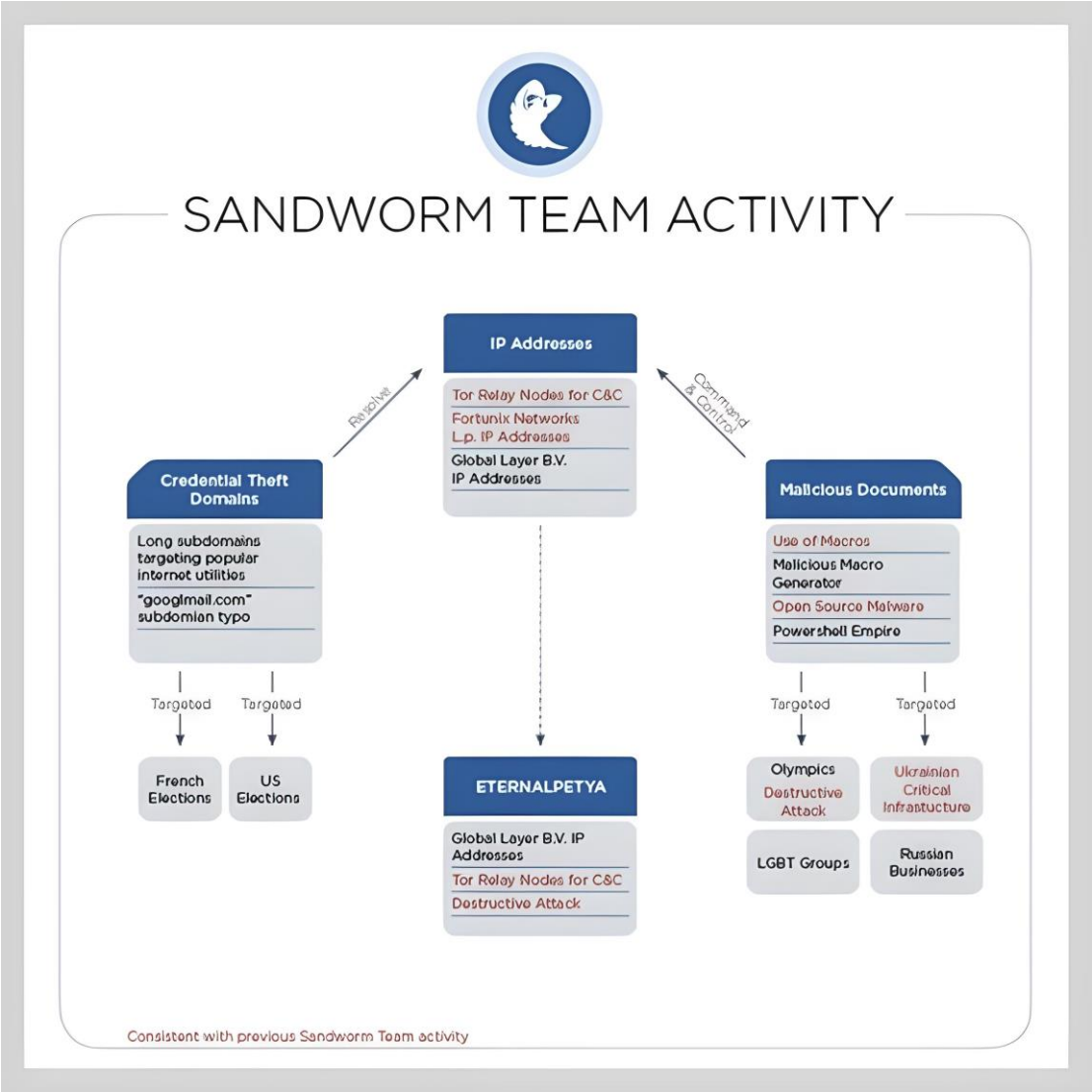

Figure 11: Andy Greenberg, "Here's The Evidence That Links Russia's Most Brazen Hacking Efforts," *Wired*, November 15, 2019.

In addition to the hack and leak operations in the U.S. and France, a similar pattern of information manipulation on social media through disinformation and the use of amplification techniques tend to point at Russia, as instigator of this campaign, through the IRA. From $1,046 a month for a low-ranked employee, to $2,100 for managers, the IRA employed not less than 80 to 90 employees in 2016 to create trolls, spread disinformation, and amplify the societal divide among the American population[193]. However, IRA's efforts to manipulate information to influence other populations' opinions did not stop after the U.S. elections, and by 2018, it had doubled its budget, spending in one

[192] In: Andy Greenberg, "Here's The Evidence That Links Russia's Most Brazen Hacking Efforts," *Wired*, November 15, 2019.
[193] "Kremlin Troll Factory's Methods and Figures Revealed," *The Moscow Times*, October 17, 2017.

semester (January to June 2018) what they spent in the whole 2016 year[194]. Not all the budget is allocated to the U.S. and the European Union or Ukraine are also targets of the IRA, which suggests that resources allocated to a wide disinformation campaign on social media against candidate Emmanuel Macron in France is likely.

Therefore, all the indications tend to point at Russia, as responsible for interfering in elections both in the U.S. and in France, especially when we know that Russia's officials recognized information warfare and influence operations as crucial aspects of their official military strategy, even involving destabilization and intimidation techniques[195] (although Russia always denied any allegations of interfering in French or American elections). However, uneven evidence in both countries resulted in divergent interpretations and official attribution.

b. How the U.S. and France differ in attributing the operations

In the U.S., at the political level, official attribution of election interference to Russia remained delicate, since the President elected Donald Trump, along with Republicans, had no interest in recognizing that Russia interfered in the elections in his favor. Likewise, Democrats' position was tricky in the sense that accusing Russia of interfering in U.S. elections by favoring Republican Donald Trump could have been seen as inappropriate and a way to delegitimize the election. Democrats were for this reason constrained to not speak out publicly about the issue after their proposal to sign a bipartisan statement denouncing the Russian government's role in election interference was rejected by Senate Majority Leader Mitch McConnell[196]. Many Democrats still individually recognized Russian election interference, such as Joe Biden that claimed he *knew* Russia interfered in the elections[197].

However, many official reports were published in the U.S. recognizing through official institutions such as the Senate or Intelligence services, the role of Russia in interfering in the 2016 elections (cf Chapter 3). Intelligence officials' testimonies to the Senate had a great impact in recognizing the role of Russia in election interference. Of all the six Intelligence leaders interrogated, none refuted the Kremlin's role in interfering in U.S. elections (including some of Donald Trump's close allies, Mike Pompeo and Dan Coats).

Conversely, France was reluctant in attributing the information manipulation campaign during the 2017 presidential elections to Russia, and although some comments were made implying Russian interference in elections[198], no official statement was made accusing the Russian government of these

[194] United States of America V. Elena Alekseevna Khusyaynova, No. Case No. 1:18-mj-464 (September 28, 2018).
[195] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[196] Scott Neuman, "Biden: McConnell Refused To Sign Bipartisan Statement On Russian Interference," *NPR*, January 24, 2018, sec. National Security.
[197] Neuman.
[198] A tense first meeting between Emmanuel Macron and Vladimir Putin took place at Versailles on May 29th 2017, in which the French President told his Russian counterpart that he knew what Russia did and could do in terms of election interference. Meeting Macron-Putin, France 24. https://www.youtube.com/watch?v=QV_mwKoAHtU

operations. Guillaume Poupard, director of the ANSSI, responsible for information systems' cybersecurity, claimed that there was no sufficient evidence to prove Russian interference in French elections, in line with most French cybersecurity experts' opinion. According to Kévin Limonier, specialist of Russian's cyberspace, it is almost impossible to know precisely the level of involvement of the Kremlin, and which operations have been planned, controlled or approved. French officials have nevertheless underlined the fact that not attributing the attack to Russia directly was not synonymous with passiveness, and that France was using other levers such as through diplomatic means to face the threat[199]. France has a long-term tradition of non-attribution, but only at the public level and action might therefore be taken, although not publicly[200]. Extreme caution is used when attributing such attacks as false evidence can also be used to divert attention towards a particular actor. Therefore, without directly accusing Russia, French's position can be synthetized by this excerpt from the report by Jean-Baptiste Jeangène-Vilmer et al.: "*whoever the perpetrator was, they were at least linked to Russian interests and received help from the American alt-right and French farright, two communities that share a very close vision to that which is articulated by the Kremlin*"[201].

Moreover, historical positions represent an explicative factor of the diverging positions of the U.S. and France. On the one hand, the longstanding rivalry between the U.S. and Russia have anchored a conflictual relationship based on suspicion which heightens the likelihood of open conflict between the two countries. On the other hand, although clearly a U.S. ally, France has often tried to keep a more neutral and nuanced position towards Russia, which could partly explain its reluctance in officially attributing information manipulation operations to Russia. Geographically, and historically, France is closer to Russia and attributing this operation to Russia would have had a significant impact on their relations.

However, differences in attribution are essentially linked to the fact that, although the U.S. succeeded in finding clear evidence of Russian interference in elections, attribution of foreign interference in elections and cyberattacks in general are extremely rare and remain a sensitive issue.

c. Attribution of foreign interference in general: a sensitive issue

Attribution of election interference through cyberspace (in this case, cyberattacks and social media), is extremely difficult. First, the main difficulty of attributing actions in cyberspace resides in the multiplicity and diversification of actors. Unlike weapons of the past, today everyone has access to social media and information, cyber-warfare necessitates few resources and is not restricted to states[202]. The ability to remain anonymous online is a factor that makes it more difficult to pinpoint

[199] Terrasson, "Présidentielle 2022."
[200] Jeangène Vilmer, "Information Defense."
[201] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[202] Kremer and Müller, *Cyberspace and International Relations*.

the origin of attacks. Third parties therefore enter into consideration and proving their association to the state is troublesome[203]. As an example, Russian patriots might interfere in American or French elections on behalf of Russian interests, nevertheless acting independently without the Kremlin's consent. Moreover, finding the original source of the attack is tedious work in the sense that the perpetrator is generally able to find ways to impede tracing, and the data is rarely available[204]. Social media keep most of their data unavailable to the public, even to governments, which makes investigation more difficult, and governments might prefer to investigate and operate secretly rather than attributing an attack publicly, also because of the potential embarrassment faced by a state in admitting to be a victim of such attack[205]. On the legal level, attribution might be tricky in the sense that individuals are not subject to international law, and if the state employs third parties when interfering in elections on social media, the 'control' of the state over these proxies has to be proven, which represents a delicate mission. The international law framework is not well-adapted, and states rarely refer to it when accusing another state of election interference through social media. Most of the time, 'naming and shaming' remain the way to hold another state accountable, without resorting to sanctions[206]. Finally, attribution might be a sensitive issue in the sense that it can generate risks of escalation of a conflict. These types of attacks or threats occur in a "gray zone-scenario"[207], between war and peace, where the conflict can escalate rapidly and might even break out in war if attributions of attacks are considered as provocations. Due to the potential doubts resulting from the difficulty to prove a state's implication in such information manipulation operation, and the consequences linked to attribution, states rarely resolve to international law and even when attribution to another state is made, it is rarely followed by concrete sanctions, other than naming and shaming. This is also due to the fact that information manipulation operations on social media go beyond one particular cyberattack, their goal is much broader and ranges from favoring one candidate, to sow discord and disrupt democracies in general, with a wide spectrum of available tools.

Section 3 : Drivers of information manipulation through social media: a foreign policy tool with more than one political objective

After analyzing the means employed to interfere in elections through social media and which actors were at the origins of such attacks, especially in the cases of the U.S. and France, it is necessary to understand the motives of such interference.

[203] Gheciu and Wohlforth, *The Oxford Handbook of International Security*.
[204] Barela and Duberry, "Understanding Disinformation Operations in the Twenty-First Century."
[205] Davis, "Russian Meddling in Elections and Referenda in the Alliance."
[206] Hollis, "A Brief Primer on International Law and Cyberspace."
[207] Pamment et al., "Countering Information Influence Activities."

1. Manipulating opinions: an alternative foreign policy tool at low costs

The first explicative factor for initiating information manipulation operations in order to interfere in elections is simply that it does not require much resources. As we saw earlier, social media represents a fairly open environment, accessible to everyone. Therefore, manipulating information on social media does not necessarily require advanced digital skills and the barriers to entry are low. If some technical issues necessitate precise computer knowledge, many activities are done by individuals with no computer science background, especially in troll farms, where individuals create memes and messages that have to appear as credible as possible. Managers generally select some topics to insist on and employees have to put messages on these topics. In this case, knowledge about the other country and culture is thus more necessary than digital skills, and little research is sufficient to create multiple messages[208]. The accessibility of information manipulation can also be underlined by the fact that no specific expensive infrastructure is needed[209]. Every individual can manipulate information on social media from home through their computer. Coordination can either be done online, or through troll factories, that are merely ordinary businesses buildings with computers. When working on a report on the online black market, researchers from NATO Strategic Communications Centre of Excellence and Singularex (Ukrainian Social Media analytics company), were surprised by the accessibility of online black markets and information manipulation tools[210]. They found that it was actually extremely easy to access online bots, and buy tools and services for information manipulation on social media. This is in part due to the surprising scale of the online black market, which researchers described as 'impressive' in their report, with services available 24/7 for everyone through any search engine. Besides, they discovered that resorting to these tools was substantially easy to hide, as well as noticeably cheap. An interesting finding of this report is that the market is dominated by Russian providers, and that researching this type of services in Russian languages tend to offer results of cheaper tools. According to Samuel C. Woolley and Philip N. Howard, political bots are developing and becoming even cheaper, with "*armies of bots built to like particular content or send message "bombs" costing less than 100 US dollars*"[211]. In addition to bots and black market tools, social media advertising is also a cheap way to spread information. Facebook's hearings before the U.S. Senate Intelligence Committee revealed that the cost of Russian advertising on their platform, that reached approximately 126 million people, did not exceed $46,000, an amount considered as extremely low for a state[212]. A former employee in a Russian troll farm revealed to work full time there and receive a monthly income of $700. Russia is not the only actor to use information manipulation, although it is the actor most highlighted in this research due to its specific role in American and French elections.

[208] Dan Harris, "Former Employees Expose Inner Workings of Russian Troll Farm," *ABC News*, November 2, 2017.
[209] Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*.
[210] NATO StratCom COE and Singularex, "The Black Market for Social Media Manipulation" (NATO Strategic Communications Centre of Excellence & Singularex, November 2018).
[211] Woolley and Howard, *Computational Propaganda*.

China, Iran, Turkey or Israel are also countries considered to use information manipulation techniques through social media. Israel, for example, is investing in information warfare through its "online army". The country offers the possibility for students to join the Israeli Defense Forces online army for their mandatory military service, providing the country with ways to manipulate information and promote Israeli interests at low costs[213]. Regarding China, the regime does rely on individuals to post messages on social media that amount to 448 million per year, which represents nearly 1,2 million posts per day[214]. These individuals are 'Internet commentators' (not the '50c army', for their earning of 50 cents by post, as was falsely claimed) that are hired by government-linked agencies. These 2 million commentators are helped in their work by "*20 million part-time trolls, most of them students and CYL [Communist Youth League] members",* according to a report on Chinese influence operations by Paul Charon and Jean-Baptiste Jeangène Vilmer[215]. A report by researchers of the RAND Corporation also studied the role of China in foreign disinformation. They show that the whole budget allocated by China to its propaganda was estimated to around 10 billion dollars[216]. Yet, if we take into account the fact that the central part of this propaganda is targeted at Chinese citizens nationally, and that the overall Chinese Defense budget reached roughly 177,5 billion dollars in 2019, we can assume that the resources allocated to online propaganda by the Chinese regime is quite low, although not neglected considering the number of messages posted each day[217]. As underlined by this RAND report, China does not use foreign information manipulation as much as Russia, partly because it could be considered as a "*weapon of the weak*". For them, "*it might be mostly employed rogue states, not peer competitors, that can reasonably aspire to build a lasting order*". In this respect, Russia has a particular interest in launching information manipulation operations, "*as a way to offset conventional disadvantages*"[218]. Russia is generally considered as a weak power which cannot seriously compete economically with the United States or regional organizations such as NATO or the EU[219].

[212] "Open Hearings of the Intelligence Committee" (U.S. Senate - Hart 216, November 1, 2017).
[213] Singer and Brooking, *LikeWar: The Weaponization of Social Media*.
[214] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review* 111, no. 3 (August 2017).
[215] Paul Charon and Jean-Baptiste Jeangène Vilmer, "Chinese Influence Operations: A Machiavellian Moment" (IRSEM - Institute for Strategic Research of the French Ministry for the Armed Forces, October 2021).
[216] Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*.
[217] Cohen et al.; Charon and Jeangène Vilmer, "Chinese Influence Operations: A Machiavellian Moment."
[218] Kremer and Müller, *Cyberspace and International Relations*.
[219] Davis, "Russian Meddling in Elections and Referenda in the Alliance."

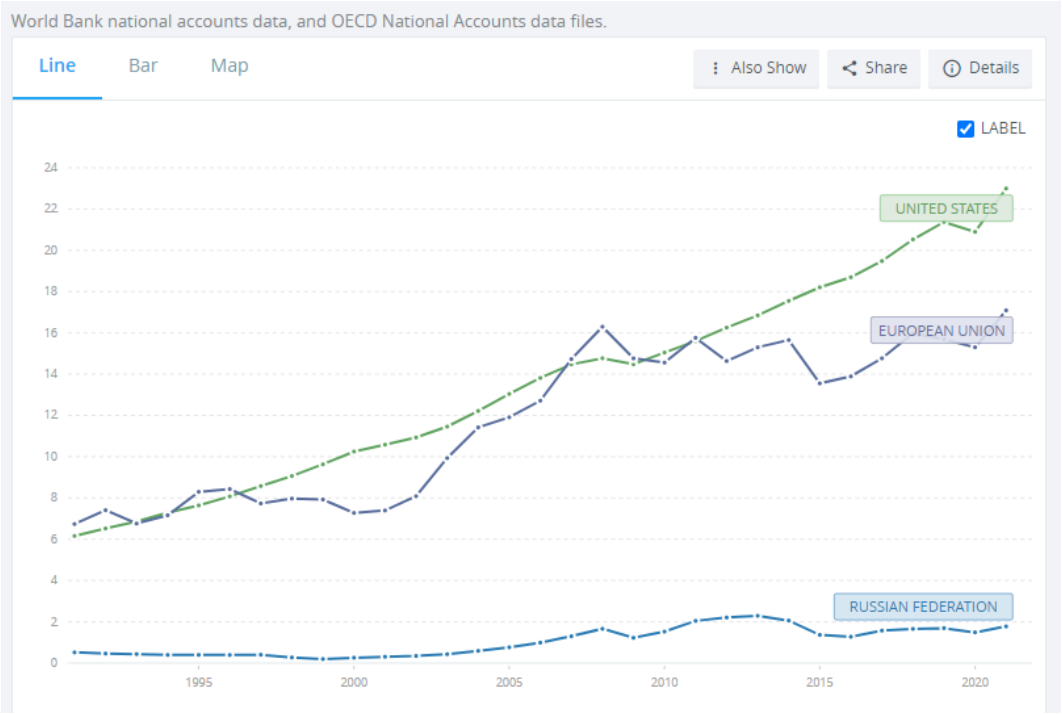

Figure 12: "GDP (current US$) - Russian Federation, United States, European Union" (1991-2021), World Bank, 2021.

According to these World Bank data, in 2021, Russian GDP amounted to $1,78 trillion, while the European Union reached $17,09 trillion and the U.S. $23 trillion[220]. To compete with big powers, Russia cannot rely exclusively on economic or conventional military means, and information manipulation operations appear as an efficient and accessible way to promote its interests[221]. Investing in information manipulation operations is also more convenient when on the offensive side, as for Russia, because of the "*perceived 'advantage' offense has over defense in cyberspace*"[222]. It is indeed much costlier and difficult to protect all systems and counter attacks on cyberspace rather than attack. The same goes for social media, where it is much easier to spread information than to detect and counter information manipulation. Therefore, states use information manipulation in great part because it represents a convenient and relatively cheap way of achieving certain goals. Usually, when states engage in election interference, it is in order to favor one candidate that would be more favorable to the state's interests.

2. Favoring one candidate or undermining another for particular interests

Both in the U.S. and France, identifying one candidate that was favored, or conversely, reviled, is relatively straightforward.

[220] "GDP (Current US$) - Russian Federation, United States, European Union," The World Bank, 2021, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2021&locations=RU-US-EU&start=1991.
[221] Davis, "Russian Meddling in Elections and Referenda in the Alliance"; Kreps, *Social Media and International Relations*.
[222] Deibert, "Trajectories for Future Cybersecurity Research."

a. Donald Trump clearly favored in the U.S.

Favoring one candidate can, if this candidate wins the election and become head of state, guarantee the promotion of significant interests for the original country. Russia, for example, considered more favorable – and did not hide it – to see Donald Trump become President instead of Hillary Clinton. In a press conference in Helsinki together with Donald Trump, Vladimir Putin responded as follows to the question whether he wanted Trump to win the election and if he directed some of his officials to achieve this goal: "*Yes, I did. Yes, I did. Because he talked about bringing the U.S.-Russia relationship back to normal*", ignoring the second part of the question[223]. Evidence mentioned earlier shows that the Kremlin did favor Donald Trump in information manipulation operations. In all the reports on the topic, the fact that Donald Trump was favored over Hillary Clinton is put forward. The U.S. Intelligence Community Assessment (ICA), emanating from CIA, FBI and NSA, stated that the Russian government "*aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him*"[224]. The same goes for the Mueller report, the case of United States v. IRA and other official sources. This claim is evidenced in many ways in the different reports and we will try to provide some of them in this paragraph. First, bots traced to Russia were generally favorable to Donald Trump. Although Hillary Clinton received some retweets and likes from Russian bots, it is at a much lesser extent than Trump: 4.25% of total Trump retweets were actually Russian bots, while the latter represented only 0.55% of Hillary Clinton's retweets[225].

Russian bots targeted against Hillary Clinton were evidenced by Ben Nimmo[226], well-known for his research at the DFR Lab on trolls and bots. Analyzing Twitter posts and accounts during the 2016 elections, he found several signs of bots participating in an automated campaign against Hillary Clinton coming from Russia, although claiming to represent the African-American community. First, he found many accounts with a random name tweeting only once with a meme and the hashtag #BlacksAgainstHillary.

[223] Stephanie Murray, "Putin: I Wanted Trump to Win the Election," *Politico*, July 16, 2018.
[224] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements."
[225] "Twitter reconnaît mais nuance les tentatives russes d'influencer l'élection de 2016," *Le Monde*, January 29, 2018.
[226] Ben Nimmo, "#TrollTracker: Russia's Other Troll Team," *Digital Forensic Rresearch Lab - Medium,* August 2, 2018,.

Figure 13: Left to right: Profiles of @euyy450, @meqypiwute, and @vriwyt, all archived on July 19, 2018. (Source: Twitter)

Then, he found that some accounts, created at the beginning of the campaign, tweeted extensively and regularly until the end of the campaign, marking the last post, often including a link with "fb.me", which are all signs, if not proofs, of automated accounts.

Figure 14: Tweets by @DaWash3241 in August 2016, archived on July 19, 2018. (Source: Twitter / @DaWash3241).

Moreover, Hunt Allcott and Matthew Gentzkow showed in a study that fake news favorable to Donald Trump were distributed more broadly than those favorable to Hillary Clinton. While favorable fake news to Trump were shared 30.3 million times on Facebook, those in favor of Clinton received only

7.6 million shares[227]. "*Overall, Trump received 15 percent more coverage than she [Clinton] did*", according to a paper on news coverage in 2016 elections by Thomas E. Patterson[228], which is the result of many factors, including the information manipulation campaign operated by Russia that amplified Trump's support on social media. More broadly, according to the Mueller report, "*IRA-purchased advertisements featuring Clinton were, with very few exceptions, negative*", while those regarding Trump "*largely supported his campaign*"[229]. Former workers at Russian troll farms also testified that going after Clinton, even in violent ways, was a general instruction: "*Everything about Hillary Clinton had to be negative and you really had to tear into her*"[230]. As mentioned before, the hack and leak operations were also targeted at Clinton and the Democrat party. The timing of the leak of the Podesta emails is also significant: their publication by WikiLeaks took place a few minutes after the release of an extremely disturbing recording for Trump, by The Washington Post, in which he brags about his sexual assaults on women in 2005. The media agenda of the end of the campaign was consequently marked by the Podesta and DNC leaks, overshadowing revelations against Trump[231].

b. A visible campaign against Emmanuel Macron

In a similar way in France, Emmanuel Macron was the target of information manipulation and hack and leak operations. The candidate, known for his positions not favorable to Russia, such as the continuation and reinforcing of the sanctions against Moscow, or his strong liberal and European perspectives, was considered to represent a danger for Russian interests. Conversely, Marine Le Pen is considered to share more interests with Russia, as she supported lifting the economic sanctions against the country. David Chavalarias analyzed Twitter conversations during the 2017 French presidential campaign[232]. If the rhythm of Twitter political posts was considered regular during the first part of the campaign and after, the period between the two rounds, opposing Emmanuel Macron to Marine Le Pen was characterized by irregular activity during time frames that did not correspond to day and night French routines. This showed activity from foreign actors that he found later coming mainly from the American far right. This community launched a "StopMacron" operation through 4chan as the main channel of coordination with the discussion thread /Le Pen General/. This included hashtag hijacking in amplifying anti-Macron or pro-Le Pen hashtags, such as #dangermacron or #jamaismacron[233]. Knowing that convincing people to vote for Marine Le Pen in a short period of time was a tricky

[227] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives* 31, no. 2 (May 2017): 211–36.
[228] Thomas E. Patterson, "News Coverage of the 2016 General Election: How the Press Failed the Voters," *Harvard Kennedy School*, Faculty Research Working Paper Series, December 2016.
[229] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."
[230] Summers, "How the Russian Government Used Disinformation and Cyber Warfare in 2016 Election – an Ethical Hacker Explains."
[231] Lamond and Venook, "Blunting Foreign Interference Efforts by Learning the Lessons of the Past."
[232] Chavalarias, *Toxic Data*.
[233][233] Translation: #macrondanger #nevermacron

challenge, they generally focused on advocating against Emmanuel Macron, and dissuading people not convinced about Macron from voting (through a hashtag #SansMoiLe7mai[234] for example).

Memes and comments shared by the American far right and Russia against Emmanuel Macron included political attacks such as calling him "a*n aristocrat who despises the common man, a rich banker, a globalist puppet, a supporter of Islamic extremism and uncontrolled immigration*", as well as personal attacks such as "*salacious remarks about the age difference between him and his wife, rumors that he was having an affair with his stepdaughter, and speculation over his sexuality*"[235]. Although other candidates faced similar violent campaigns of denigration, they were not found to be supported by foreign actors.

Here is an example of a meme that was spread on social media by American alt-right, against Emmanuel Macron, referring to their previous campaign against Hillary Clinton, showing a clear anti-Macron positioning[236].

Figure 15: "We beat'em before... We'll beat'em again !", David Chavalarias, Toxic Data: Comment les réseaux manipulent nos opinions, 2022.

[234] Translation: #WithoutMeOnMay7th, which was Election Day
[235] Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."
[236] Chavalarias, *Toxic Data*.

3. A wider objective: undermining trust in liberal democracies

If supporting one candidate is often an objective of interfering in elections, the main driver behind election interference through social media is generally to disrupt the democratic process and affect the society as a whole.

a. Playing on pre-existing tensions to polarize the society

The primary way to manipulate information on social media is by exploiting pre-existing tensions so as to fuel the conflict and polarize society. The goal is to foster extreme positions in order to shape the public debate. In doing so, extreme positions become normalized and polarization deepens, resulting in a lack of cohesion and common points of reference[237]. A short evaluation of the divisive conflicts and tensions in a society is sufficient to stress the major points of friction and polarize the debate, which does not necessarily require deeper knowledge of the targeted society. Exploiting another country's divisions is not a new technique, but social media offer new possibilities in opening the national public debate to everyone on the planet. They represent a particularly efficient tool in the sense that their functioning and algorithms already tend to polarize the public debate (cf. Chapter 2), which facilitates the operation. Russia went in this direction during the 2016 American presidential elections by identifying "*who dislikes whom within the United States and then flood[s] the information space with content to amplify these cleavages*"[238]. As an example, the IRA is known for having organized political events that were particularly polarizing. One striking example stressed in David Chavalarias' book is an event that took place on May 21st 2016. This event featured two protests, one organized by a Facebook group called "Heart of Texas" shouting "Stop Texas' Islamization", and the other counter protest organized by another Facebook group called "United Muslims of America". In the end, the protests mobilized only a dozen people and some were surprised that the organizers were not even on site. Something that David Chavalarias found not so surprising in the sense that the administrators of both of these groups were actually from Russia's IRA.

Russia is not the only actor to play on societal tensions to manipulate information, and other countries are also engaged in this type of operation. If China is not known to have interfered in American or French elections in favoring one candidate, it does not preclude the regime from manipulating information during elections through social media, by sowing discord and play on pre-existing tensions and emotional topics. For example, during the 2020 American presidential elections, China was found to have participated in the dissemination of messages on all sides of the spectrum. Chinese operators spread messages both in support for the Black Lives Matter movement, as well as for the opposite movement Blue Lives Matter, playing on the particularly divisive topic of police violence

[237] Kreps, *Social Media and International Relations*; Davis, "Russian Meddling in Elections and Referenda in the Alliance."

and racial discriminations. On the international stage, Chinese trolls are considered as particularly aggressive and violent, resorting to harassment, in order to divert attention from controversial issues about China.

b. Sowing discord and undermining trust in democratic institutions

The underlying objective of these operations is to sow discord in societies and undermine trust in democratic institutions. Disturbing the electoral process amounts to questioning the legitimacy of leaders and institutions themselves. How can we be sure that our elected leaders are representative of the population's will if we know that foreign actors manipulated information and interfered in the electoral process? As highlighted in the last report of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation: "*foreign interference aims to introduce doubt, uncertainty and mistrust, and not just to alter the result of elections but to delegitimise the entire electoral process*"[239]. Xymena Kurowska and Anatoly Reshetnikov talk about Russia's strategy as 'trickster diplomacy', insofar as "*it fully embedded within dominant institutions but subverts them by adopting a cynical and derisive attitude towards them*", with the goal of corrupting the system from within[240].

With the diffusion of false information, individuals are prompted to be cautious and suspicious with information relayed by the media or governments, and take into consideration rumors or conspiracy theories[241]. This phenomenon takes place and is facilitated by a general tendency towards erosion of trust in democratic institutions, experts or traditional media, as underlined in various studies[242]. According to the Reuters Institute, less than one third of Americans and French claim to trust most news most of the time (in 2022, 26% for American and 29% for France)[243]. Similarly, more than half of Americans and French people say they are not satisfied with the way their democracy works, according to the Pew Research Center, levels that are fairly low compared to other well-established liberal democracies[244].

---

[238] Marek N. Posard, Hilary Reininger, and Todd C. Helmus, "Countering Foreign Interference in U.S. Elections" (RAND Corporation, March 29, 2021).

[239] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation."

[240] Xymena Kurowska and Anatoly Reshetnikov, "Russia's Trolling Complex at Home and Abroad," in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, ed. N. Popescu and S. Secrieru, Chaillot Papers (EU Institute for Security Studies, 2018).

[241] Davis, "Russian Meddling in Elections and Referenda in the Alliance."

[242] Wardle and Derakhshan, "Information disorder."

[243] Newman et al., "Digital News Report 2022."

[244] Richard Wike et al., "Citizens in Advanced Economies Want Significant Changes to Their Political Systems," Pew Research Center's Global Attitudes Project (Pew Research Center, October 21, 2021).

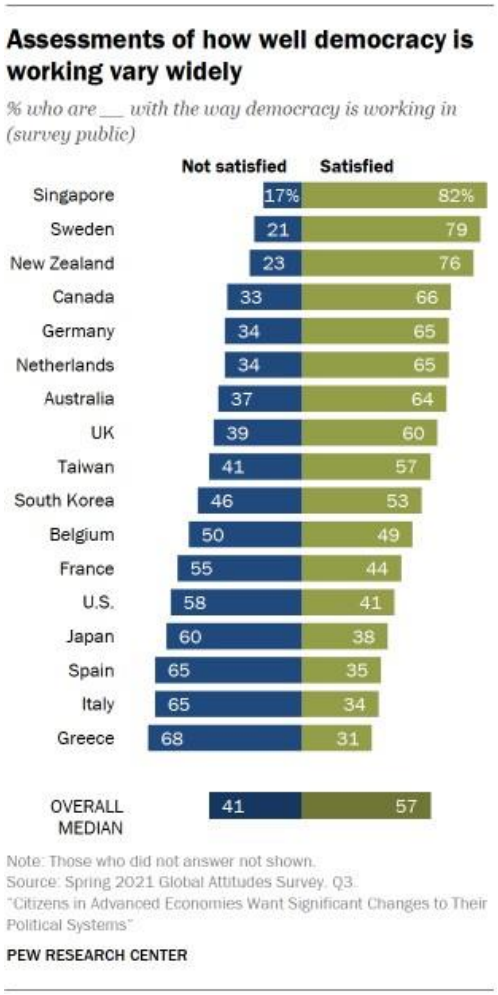

Figure 16: "Assessments of how well democracy is working vary widely". *Pew Research Center*. 2021

"*For complex demographic, economic and social reasons, levels of social trust in many societies have ebbed*"[245]. If foreign interference in elections is not the only cause of this phenomenon, it has surely participated in its acceleration, according to Herbert Lin[246]. And this might be the major impact of election interference through information manipulation on social media, more than the victory of one candidate over the other[247]. According to W. Lance Bennett and Steven Livingston, "*a crisis of legitimacy of authoritative institutions lies at the heart of our current disinformation disorder*"[248], and while social media are responsible for a part of that disorder, the erosion of trust in elected leaders and institutions as providers of authoritative information are also key in addressing the problem. Yet, foreign interference in elections further erodes this confidence.

Foreign regimes might use information manipulation to spread the idea that Western lifestyle is not ideal, and promote their regimes. Devaluing one model results in the appreciation of another model, consequently, countries like Russia or China use information manipulation operations in order to emphasize liberal democracies' flaws, and make their political system appear to be the most adequate.

[245] Pamment et al., "Countering Information Influence Activities."
[246] Lin, "Conclusion: An Outsider Looks In."
[247] Jens David Ohlin and Duncan B. Hollis, eds., *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, Ethics National Security Rule Law Series (New York: Oxford University Press, 2021).
[248] Bennett and Livingston, *The Disinformation Age*.

This allows Russia to promote another mode of governance, known as 'sovereign democracy'[249]. A 2018 U.S. Senate Committee on Foreign Relations report started as followed: "*For years, Vladimir Putin's government has engaged in a relentless assault to undermine democracy and the rule of law in Europe and the United States*."[250], including disinformation and cyberattacks as main methods to achieve that goal. All the reports from U.S. intelligence and institutions highlighted that beyond favoring one candidate the main goal of Russian interference was indeed to sow discord and undermine trust in democratic institutions.

[249] Davis, "Russian Meddling in Elections and Referenda in the Alliance."
[250] U.S. Senate Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," Government (Washington D.C.: Congress, January 10, 2018).

CHAPTER 3: RESPONDING TO ELECTION INTERFERENCE THROUGH SOCIAL MEDIA: VARYING APPROACHES AND POTENTIAL IMPROVEMENTS

Claims and evidence of foreign interference in elections through social media raised awareness and generated various responses by the United States and France, as well as other non-state actors, to counter those threats. However, these responses triggered reactions and debates and their efficiency is often disputed, which brings us to discuss potential solutions and improvements for countering foreign interference in elections through social media.

Section 1 : How the U.S. and France responded to information manipulation

The U.S. and France both took the threat seriously and implemented various measures in order to try to fight it, in generally similar ways, although some different steps ought to be highlighted. One major difference between the U.S. and France in fighting foreign information manipulation operations lies in France's membership to the European Union, whose role in this respect is worth mentioning. Other similarities and differences in responses by non-state actors will also be highlighted.

1. Similarities and differences in state responses

If similar responses regarding administrative agencies were implemented, approaches regarding regulation and official positions through works of investigation and official statements, differed in some ways.

a. Similar measures and structures at the administrative level

If general structures to tackle cyber and information threats in the U.S. and France are not new, specific structures regarding the fight against information manipulation through social media are fairly recent. In Chapter 1 we discussed states' will to expand their capabilities in terms of cyber. USCYBERCOM and French COMCYBER can consequently represent useful tools in detecting attempts of cyberattacks, although their goal is primarily military. The NDDP (at the time of the 2016 election), and the ANSSI, mentioned in Chapter 1 were also important actors for securing information and trying to prevent cyberattacks. However, they were not originally built to identify and counter foreign interference and information manipulation on social media, and before the 2016 and 2017 elections in the U.S. and France, no specific agency existed with this aim. In the U.S. these missions were rapidly added to the prerogatives of the newborn Global Engagement Center (GEC) related to the

State Department, through the Countering Foreign Propaganda and Disinformation Act that was signed into law by Barack Obama just before the end of his term on 23 December 2016[251]. The original mission of the GEC was to fight terrorism propaganda, but Russia's interference in the U.S. elections led to the extension of its missions, which core objective is defined as followed on the website: "*direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government* to *recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations*". The GEC gained importance and consideration in the following years, with additional resources granted. As an example, following the first results of inquiries on Russia's interference in presidential elections, in 2018, $40 million were allocated to the GEC through a transfer by the Department of Defense[252], and its budget for the year 2021 amounted to $138 million. However, the GEC is not the only actor working on the matter, with support (or competition) from other Federal administrations such as the State Department, the Department of Defense or Homeland Security. The Intelligence community also plays a prominent role in addressing this threat, especially with the Federal Bureau of Investigation (FBI) and its Foreign Influence Task Force (FITF) created in 2017[253]. The fact that election interference through information manipulation is addressed by several agencies is important in the sense that this is a multifaceted threat that necessitates a cross-cutting approach. The coordination role of the GEC is therefore essential in this respect, although sometimes tricky.

France can also count on the Intelligence community to detect potential foreign interference in elections through information manipulation operations thanks to the role of the Directorate-General for External Security (direction générale de la sécurité extérieure, DGSE) and of the Directorate-General for Internal Security (direction générale de la sécurité intérieure, DGSI), the latter being the main responsible for attributing an interference to a foreign actor[254]. However, no specific agency existed until very recently, with the creation of Viginum, the "vigilance and protection service against foreign digital interference" by the law-decree n° 2021-922 of 13 July 2021[255]. After establishing a specific Task Force on disinformation called "Honfleur Task Force", the government stepped up and replaced it by an agency under the authority of the SGDSN (that controls different services such as the

[251] Issie Lapowsky, "The State Department's Fumbled Fight Against Russian Propaganda," *Wired*, November 22, 2017, sec. tags.

[252] Oren Dorell, "State Department's Answer to Russian Meddling Is about to Be Funded," *USA Today*, February 13, 2018.

[253] "Counterintelligence - Combating Foreign Influence," FBI, Federal Bureau of Investigation, accessed September 6, 2022, https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

[254] "Commission de la défense nationale et des forces armées. Audition, à huis clos, de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme.," fevrier 2021.

[255] "Décret N° 2021-922 Du 13 Juillet 2021 Portant Création, Auprès Du Secrétaire Général de La Défense et de La Sécurité Nationale, d'un Service à Compétence Nationale Dénommé « service de Vigilance et de Protection Contre Les Ingérences Numériques Étrangères »," Légifrance.

ANSSI), entirely dedicated to foreign digital interference: Viginum. Operational since October 2021, Viginum should count 65 employees by the end of 2022[256].

However, if similar structures were established in the U.S. and in France, France's action is more covert, while the U.S.' is more frontal, and includes important works of investigation.

b. A more frontal approach in the U.S. *versus* Russia and important works of investigation

On the one hand, as mentioned previously, France never attributed the information manipulation operation to Russia, and more generally, never attributed a cyberattack to any country. The government tends to act more under covert ways that are not easily identifiable in open-source. There is no doubt that reports are being produced and circulated within the French administration and the executive branch about foreign interference and information manipulation on social media. However, these reports are generally not public. For example, reports from Viginum are not expected to be available to the wider public, and finding governmental reports on the topic is hardly achievable. Although some government-linked agencies produced in-depth works on the topic – such as the report by CAPS and IRSEM, already cited in this research – main reports come from independent research centers and think tanks, or newspapers through investigative journalism.

On the other hand, the U.S. governmental and federal institutions, such as Committees in the U.S. Senate or in the House of Representatives, produced important works of investigation on foreign interference in elections and information manipulation. Some reports such as the one by Special Counsel Robert S. Mueller or the five volumes from the U.S. Senate Select Committee on Intelligence are remarkable in the level of investigation and details regarding Russian interference in the U.S. elections, and are crucial to understand the tools used by foreign actors for manipulating information[257]. These reports allow for the general public to be better informed, while acting as a deterrent, insofar as they show the high level of detection of intelligence services[258].

Other than official reports, resources on the topic are available through legal affairs such as the United States V. IRA. Appealing to the courts and the justice system is also a tool used by the American government, and less by France. By resorting to law, and officially attributing the information manipulation operations to Russia, the U.S. government is taking a more frontal stance than France, which tends to be more prudent. In response to Russian interference in elections, the U.S. also expulsed 35 Russian diplomats from the U.S.[259] on December 29th 2016. The same day, Barack Obama also amended an executive order (EO 13964) so as to allow sanctions on individuals or organizations that "*tamper with, alter, or cause a misappropriation of information with the purpose or effect of*

[256] "Viginum, Vigilance et Protection Contre Les Ingérences Numériques Étrangères."

[257] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election"; U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V."

[258] Jeangène Vilmer, "Information Defense."

interfering with or undermining election processes or institutions.". According to the U.S. Senate Select Committee on Intelligence, this enabled the sanctioning of *"nine Russian entities and individuals, including the GRU, the FSB, three companies that supported the GRU, Chief and Deputy Chief of the GRU, and two additional GRU officers*"[260]. The U.S. thus has a strict policy against foreign interference in elections, and attributes attacks to other countries more easily even when not directly targeted at them. American authorities even sanctioned a GRU employee: Anatoliy Sergeyevich Kovalev, member of the Unit 74445 (the Sandworm group mentioned in Chapter 2) for "*interference in the 2017 French elections*", due to France being considered as a U.S. ally[261].

c. Different perceptions of the role of the state and regulation

One main difference between the American and French response is their vision of the state's role in regulation. This is partly due to differences in their political systems with federal *versus* centralized political systems. In France, the centralized system implies that legislation is taken at the national level through the Congress, and laws are applied all over France, while regions and departments have very little power in designing their own legislation. In the U.S., although the Federal state has a relatively strong legislative power, states can also build their own legislative framework while respecting the U.S. Constitution. The U.S. and its citizens in general are strongly attached to their Constitution, and especially to the First Amendment which ensures, among other things, freedom of speech and press. Implementing legislation that restricts freedom of speech is thus often frowned upon. Yet, in order to prevent information manipulation, it might be worth conceiving certain laws that would regulate the content of social media. For example, France adopted in July 2018 a law on information manipulation, following the example of Germany and its law about false information[262]. This law was promulgated in December, after the decision of the Constitutional Council, that provided some clarifications on content restrictions. Particularly focused on the electoral period (the three months preceding the election), the law states that the judge can compel online platforms to delete content that is considered to be manifestly false or misleading, if the risk of altering the fairness of the vote was evident. The law also requires transparency on advertised content on social media platforms, and empowers the Arcom (previously CSA), to monitor and make sure social media platforms are doing the necessary to fight information manipulation (although no sanctioning power is provided for in the law). More broadly, France has shown the will to regulate social media platforms whereas the U.S. tends to keep a more liberal stance, with the state interfering as little as possible in social media companies' rules and content. The Digital News Report of 2018, after French and American elections,

[259] U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V."
[260] U.S. Senate Select Committee on Intelligence.
[261] Jeangène Vilmer, "Information Defense."
[262] "Loi Organique N° 2018-1201 Du 22 Décembre 2018 Relative à La Lutte Contre La Manipulation de l'information," Pub. L. No. n° 2018-1201 (2018).

seems to corroborate the fact that French (or Europeans) are more prone to governmental action than Americans. In their survey, they found that while 60% of Europeans would like to see more governmental action to stop 'fake news', they were only 41% of Americans to state that the government should do more[263]. Along with Americans' reluctance towards more regulation by the state, the fact that the U.S. system is federal compared to the French centralized system might explain differences in states' response. In France, regions have little power and decisions on this type of issue are generally taken at the national level. Presidential elections in France are indeed controlled by the national state, while in the U.S. states have more power and liberty to apply specific rules regarding electoral procedures for the presidential elections, since American citizens vote for an Electoral College, at the state level. Measures that have been introduced since the disclosures of Russian interference in the election are more focused on voting infrastructure, such as the recognition in January 2017 of electoral systems as critical infrastructure by the Department of Homeland Security[264], and less on social media manipulation operations. Many American scholars do not see the regulation of social media by the state as desirable. According to Herbert Lin, it is highly unlikely that the U.S. government will take action to counter the spread of false information on social media, nor it is desirable: "*imagine a Ministry or Department of Internet Information subject to the direction of the present administration*" (referring to Trump's administration)[265]. All in all, regulation regarding social media companies remains quite low in the U.S. compared to France, especially if we take into account other rules that apply to France, as part of the European Union (EU).

2. Action at the regional level: the gap between the U.S.A. and France through the role of the European Union

The main difference at the regulatory level lies in France's membership to the EU, which provides a major regulatory framework and other measures for European countries.

The EU started acknowledging the need to counter threats of manipulation of opinions through social media after Russia was accused of manipulating information about the annexation of Crimea in 2014, and established as a response, the EU Strategic Communication Task Force composed of the East StratCom Task Force set up in 2015, as well as the Balkans Task Force and Task Force South, that were added later, which aim at increasing prevention, awareness, knowledge and resilience against hybrid threats including campaigns of information manipulation on social media[266].

A significant step on the issue is with the publication in 2016 of the Joint Framework on countering hybrid threats, that provides main common guidelines to EU institutions. The same year, the EU

[263] Nic Newman et al., "Digital News Report 2018" (Reuters Institute for the Study of Journalism, 2018).

[264] "Election Infrastructure Security," Cybersecurity and Infrastructure Security Agency, accessed September 7, 2022, https://www.cisa.gov/election-security.

[265] Lin, "Conclusion: An Outsider Looks In."

[266] They produce weekly reports that can be found on the website: euvsdisinfo.eu

adopted the famous General Data Protection Regulation (GDPR) and although it mainly tackles the protection of users' data, its implementation since 2018, proves that the EU has the power to constrain social media companies to abide by European rules in order to access the European market. A particular focus on information manipulation in the context of elections was made later, the 2019 European elections approaching. In 2018, the EU published a Communication on securing free and fair European elections, and recommendations regarding elections' protection, including against foreign interference through social media. The EU has also signed a Code of practice with social media companies in September 2018 to enjoin them to respect certain rules that would allow the debate on their platforms to run smoothly and protect citizens, to fight disinformation, that was updated recently through the 2022 Strengthened Code of Practice, with 34 signatory companies (including big social media companies) following the EU Commission's guidelines[267].

Regarding social media, the EU Commission presented a regulation proposal on transparency and targeting of political advertising with rules that would provide a better framework for political advertising practices on social media[268]. The regulation is currently under discussion in the Parliament, but would have a direct impact on the EU member states, considering that only three of them currently have a specific legal framework for online political advertising media. This regulation would represent a real progress in two main aspects: first it would establish strict rules regarding political advertising and transparency mainly through labels, but also ban targeted political advertising based on personal data regarding characteristics such as ethnic origins, race and religion. This would help protect individuals' privacy, guarantee their freedom of choice, and prevent the use of these techniques to spread false or distorted information to some individuals. The Action Plan Against Disinformation also provided specific responses to information manipulation with the establishment of Rapid Alert System (operational since March 2019), an online platform that allows European countries to share information about disinformation campaigns, raise awareness and coordinate their response in cooperation with EU institutions[269].

Finally, the EU Parliament has set up a Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE)[270] that was followed by its successor INGE II at the end of the first term on 23 March 2022. The main goals of these committees are to carry out in-depth studies on the topic and work on recommendations. Other noticeable initiatives are the European Centre of Excellence for Countering Hybrid Threats based in Helsinki,

[267] European Commission, "2022 Strengthened Code of Practice on Disinformation," June 16, 2022.
[268] "Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising" (2021).
[269] "Action Plan Against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions" (Brussels: European Commission, December 5, 2018).
[270] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation."

that acts more as a research center, and the Hybrid Fusion Cell that aims at coordinating and protecting EU member states against hybrid threats.

All in all, since the adoption of the Joint Framework in 2016, more than 200 measures have been taken by the EU in order to increase its resilience against hybrid threats[271]. If not all directly relate to information manipulation on social media during the electoral process, many of them have at least an indirect impact on this phenomenon. France is considered as a major actor in the European Union advocating for stronger EU cooperation and action against information manipulation. As an example, France included in its priorities in the context of the French Presidency of the European Union this year, the deepening of the regulation and accountability of online platforms[272]. The EU thus represents a significant lever of action for France that is worth highlighting.

3. Beyond states: the role of other actors such as private companies and civil society

States are not the only actors that responded to election interference and information manipulation in the U.S. and France. Private companies and civil society also played a role in the post-election interference.

The main targets of information manipulation operations are citizens, and learning that they might have been victims of disinformation led many of them to try to take action. One major aspect that was widely discussed when addressing information manipulation on social media was the spread of false information, most commonly referred to as 'fake news'. In combating fake news, democratic states have little room for maneuver if they do not want to appear as authoritarian states that censor what they consider as untrue. In this sense, it is generally agreed that states should be involved as little as possible in debunking fake news. Civil society therefore filled that void in taking initiatives to debunk fake news on social media and try to counter these disinformation campaigns. Many initiatives predate the 2016 and 2017 elections or the emergence of social media, but their number dramatically increased in the following years of election interference scandals. Today (2022), the Duke University Reporters' Lab[273] identified 379 active fact-checking websites around the world, while they were only 64 in 2015. These include 17 websites in France – largely above other European countries – and 73 in the U.S., which can make us believe that information manipulation operations in these two countries had an impact on the national civil society that took steps in launching these initiatives. In France, one famous fact-checking source is the "Décodeurs", launched by the newspaper *Le Monde* in 2014, but

[271] High Representative of the Union for Foreign Affairs and Security Policy, "Mapping of Measures Related to Enhancing Resilience and Countering Hybrid Threats - Joint Staff Working Document" (Brussels: European Commission, July 24, 2020).

[272] "Priorities - French Presidency of the Council of the European Union 2022," French Presidency of the Council of the European Union, accessed September 7, 2022.

[273] "Reporters Lab Fact-Checking Category," Duke Reporters' Lab, accessed September 8, 2022, https://reporterslab.org/category/fact-checking/.

considerably developed and improved in the following years, with the inauguration in 2017 of an extension for search engines called "Decodex" that provides insights on the information's reliability. From non-governmental organizations, individual initiatives or media projects, fact-checking systems employ diverse techniques, and they have room for improvement in the sense that their efficiency is not consensual[274]. Individual actions against disinformation campaigns took many other different forms such as hashtags against a rumor or research and the development of education tools. For example, Rose-Marie Farinella, a teacher in a French school of Grenoble, wrote a book and built a program, destined to children from ten years old on, to provide them tools to recognize false information and accounts, giving them a diploma of 'hoaxbusters' at the end of the lessons[275]. This initiative was granted several prices at the national and international level, such as a price from the European Commission in 2018.

Civil society also played a major role in pressuring governments and social media to take action in order to protect the safety of elections through a fair and healthy information environment. Pressure from civil society and governments led social media companies to also act in order to fight information manipulation in their platforms. This led to a hearing of Mark Zuckerberg, director of Facebook, before the U.S. Senate Committee on the Judiciary and the U.S. Senate Committee on Commerce, Science and Transportation, on April 10th 2018, in which he stated: "*One of my greatest regrets in running the company is that we were slow in identifying the Russian information operations in 2016*"[276]. He also admitted that Facebook was not prepared in 2016 for information manipulation operations on their platform, but that they "*have learned a lot since then and have developed sophisticated systems that combine technology and people to prevent election interference on our services*"[277]. In order to combat disinformation, Facebook adopted several initiatives and invested more resources. As an example, they announced that media literacy campaigns would represent one of the main objectives of the company with the Facebook Journalism Project, and invested $14 million in the News Integrity Initiative built by the CUNY Journalism School in New York for improving media literacy[278]. In April 2017, Facebook took two important steps: first in writing a report on information operations, recognizing that "*social media platforms can serve as a new tool of collection and dissemination for these activities*" and the necessity to address it[279], and then by deleting 70,000 accounts a few days prior to French presidential elections as mentioned earlier. Still in 2017, Facebook asserted that it was closing one million accounts per day worldwide, showing the efforts put

[274] Tanja Pavleska et al., "Performance Analysis of Fact-Checking Organizations and Initiatives in Europe: A Critical Overview of Online Platforms Fighting Fake News," in *Disinformation and Digital Media as a Challenge for Democracy*, ed. Georgios Terzis et al., Intersentia, 2018.

[275] Rose-Marie Farinella and Estelle Warin, *Stop à La Manipulation : Comprendre l'info, Décrypter Les Fake-News* (Bayard Jeunesse, 2021).

[276] "S.Hrg. 115-683 — Facebook, Social Media Privacy, and the Use and Abuse of Data" (Washington D.C., April 10, 2018), http://www.congress.gov/.

[277] In: Nye, "Protecting Democracy in an Era of Cyber Information War."

[278] Wardle and Derakhshan, "Information disorder."

[279] Weedon, Nuland, and Stamos, "Information Operations and Facebook."

in place notably to counteract inauthentic coordinated behavior[280]. Twitter also reacted to information manipulation on the platform. After the U.S. elections, the company informed up to 1.4 million Americans by e-mail that they had interacted or followed an account linked to the IRA during the 2016 presidential elections. In order to fight dis/mis/malinformation, Twitter also implemented a prompt that pops up before retweeting an article that asks the user if they did read the article before sharing it. The company later revealed on their Twitter feed that this initiative was efficient insofar as people opening the article after reading this message increased by 40%[281]. Twitter's terms of use have also been changed to include foreign interference, which now read: "*You may not use Twitter's services for the purpose of manipulating or interfering in elections. This includes posting or sharing content that may suppress voter turnout or mislead people about when, where, or how to vote*"[282]. Twitter has been recognized as particularly efficient in countering inauthentic coordinated behavior, and according to a NATO report evaluating social media's efficiency in countering information manipulation: "*Twitter is three times faster than Facebook at removing accounts engaged in inauthentic activity*"[283]. However, according to the same report, social media companies' efforts are not sufficient in fighting information manipulation on their platforms. Furthermore, initiatives remain uneven and disjointed among different platforms, and even within different platforms of the same group[284], with less significant efforts on Instagram than Facebook for the group Meta (previously Facebook) for example[285]. Last but not least, we mentioned examples of action being taken in most famous social media platforms, however, by lack of resources or will, less famous or emerging social media companies have not established specific measures to counter information manipulation campaigns. The fast-emerging social media Tik-Tok for example, is considered as "*the defenceless newcomer with much to learn*"[286].

All in all, if states and non-state actors such as civil society and social media companies made efforts in combating information manipulation campaigns, these efforts are still insufficient in preventing election interference, and could benefit from several improvements.

[280] John Shinal, "Facebook Shuts down 1 Million Accounts per Day but Can't Stop All 'threat Actors,' Security Chief Says," *CNBC*, August 24, 2017.
[281] Twitter Comms [@TwitterComms], "More Reading – People Open Articles 40% More Often after Seeing the Prompt. More Informed Tweeting – People Opening Articles before RTing Increased by 33%. Some People Didn't End up RTing after Opening the Article – Which Is Fine! Some Tweets Are Best Left in Drafts.," Tweet, *Twitter*, September 24, 2020.
[282] "Twitter's Civic Integrity Policy," Twitter Help Center, October 2021, https://help.twitter.com/en/rules-and-policies/election-integrity-policy.
[283] Rolf Fredheim et al., "Social Media Manipulation Report 2020" (NATO Strategic Communications Centre of Excellence, December 21, 2020).
[284] Bronner, "Les lumières à l'ère numérique."
[285] Fredheim et al., "Social Media Manipulation Report 2020."
[286] Fredheim et al.

Section 2 : Going beyond: a multidimensional response encompassing various actors

As stated by Myriam Dunn Cavelty and Florian J. Egloff: "*a satisfactory level of cybersecurity can only be achieved by government, business, and society together*". This applies to the specific threat of election interference through social media. These actors must work together and bring changes in education, coordination, and regulation, which could significantly improve the prevention and response to the threat.

1. From pupils to researchers: the crucial role of education in raising awareness and learning

Education is essential in order to respond through a whole-of-society approach. First, education is needed to raise awareness among the general public and help identify information manipulation operations from the younger age. Then, education through research is also essential and helps deepen the topic through all its aspects, useful for citizens, private companies and last but not least, governments to design their policies.

a. Identifying the risks from the younger age: the impact of media-literacy campaigns and schools' programs.

Education is essential from the younger age to learn how to identify reliable and non-reliable sources, automated behaviors and different techniques of information manipulation. This is becoming increasingly meaningful as social media users are getting younger and younger. A survey by Common Sense Media showed that almost one out of five (18%) children from eight to twelve years old say that they use social media every day, which represents an increase from 5 percentage points since 2019[287]. This is even more accurate for teens (from 13 to 18 years old), that are 79% to say that they use social media regularly in 2021. Given the wide use of social media by young people, it is essential that they learn how to use them and how to get reliable information, to try to be as less manipulated as possible. In this respect, Claire Wardle and Hossein Derakhshan suggest some elements that would be interesting to add to any academic program[288]: "(*i) traditional news literacy skills; (ii) forensic social media verification skills; (iii) information about the power of algorithms to shape what is presented to us; (iv) the possibilities but also the ethical implications offered by artificial intelligence; (v) techniques for developing emotional scepticism to override our brain's tendency to be less critical of content that provokes an emotional response; and (vi) statistical numeracy*", obviously at a different level of complexity for different ages.

[287] Victoria Rideout et al., "The Common Sense Census: Media Use by Tweens and Teens, 2021" (Common Sense Media, March 9, 2022).
[288] Wardle and Derakhshan, "Information disorder."

Several research works show signs that can often be associated to inauthentic behavior or foreign interference, that would be useful to teach to people, and not only children. For example, bots accounts, compared to human accounts, are more likely to be less customized, created recently, without geographical metadata but a consistent activity, etc., and oddities about language, time or topic can be a sign of foreign bot[289]. Studies have also shown that helping people identify information manipulation in labeling content or making public announcements can be efficient. As an example, Twitter introduced labels regarding certain messages, after a wave of disinformation around the COVID-19 pandemics started on social media. Many Twitter users have thus been confronted with one of these messages: "*some or all of the content shared in this Tweet conflicts with guidance from public health experts regarding COVID-19*". In the context of the following U.S. election, these labels were used under many tweets of Facebook posts about the elections and mail-in ballots, as "*misleading information*" or "*disputed claim*"[290].

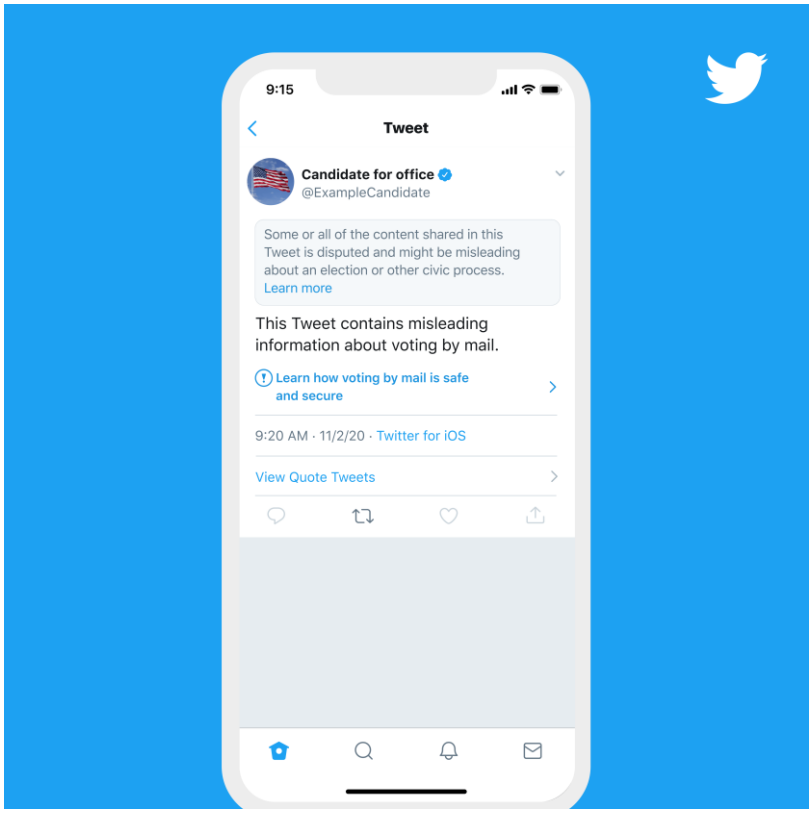

Figure 17: Twitter label. Kayvon Beykpour and Vijaya Gadde, "Additional Steps We're Taking Ahead of the 2020 US Election," Twitter Blog, October 9, 2020.

Official government agencies can also flag content as misleading through Public Service Announcements (PSA) and reveal foreign sources, along with media-literacy campaigns. Several studies found that if the message comes from an official, non-partisan source, the impact can be

[289] Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion," *First Monday*, November 7, 2016; Chavalarias, *Toxic Data*; Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."
[290] Kayvon Beykpour and Vijaya Gadde, "Additional Steps We're Taking Ahead of the 2020 US Election," *Twitter Blog* (blog), October 9, 2020.

significant. People are less likely to engage with a message after learning the source is Russian for example[291].

Finally, the French government has underlined the importance of raising awareness on that topic. A report commissioned by Emmanuel Macron gave several recommendations to the government to increase media literacy, including the need to create an inter-ministerial cell responsible for developing critical mind and education to media and information, as well as coordinating actions[292].

b. Using already existing expertise: the crucial role of research

Today, research on the topic is flourishing, and this research by academics is an excellent source of information that should be extensively considered by the European Union, and national officials so as to take enlightened decisions relying on experts' knowledge. Different laboratories specialized on the topic are emerging, providing excellent insights on specific aspects, such as the Atlantic Council's Digital Forensic Lab that developed a tool to evaluate claims of foreign interference in the 2020 U.S. elections: the Foreign Interference Attribution Tracker, or the Observatory on Social Media built by Indiana University, that created the tool Hoaxy to visualize the spread of claims and fact checking and Botometer to check if an account on Twitter is likely to be a bot or human[293]. These are only a few examples of the tools developed at the international level, and that could be taken into consideration by governments so as to improve their response or share this knowledge to populations.

Computer science research should also be emphasized and developed in order to find technological means to apprehend this threat. Analyzing the millions of posts that come out on a regular basis is hardly feasible by humans only, and technological intelligence appears as an indispensable accelerating tool. In a report by the World Economic Forum, it is underlined that "*It's simply not possible to read the 1 billion tweets produced every two-and-a-half days*"[294]. Nonetheless, bots are becoming increasingly sophisticated, thus, difficult to detect. Computer science is essential in this respect to try to counter information manipulation on social media, and develop artificial intelligence (AI) that is capable of detecting other AIs. As Sarah Kreps put it: "*answer to technology may actually be more technology*", mentioning several studies that show that AIs are roughly 92% accurate when detecting human or machine written posts[295].

However, one key obstacle regarding research on social media remains, and has to be addressed, that is the fact that most social media data are not accessible and kept secret by the companies. These data are considered as essential in order to produce evidence-based policies, as underlined by the Council

[291] Posard, Reininger, and Helmus, "Countering Foreign Interference in U.S. Elections"; Todd C. Helmus et al., "Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions" (RAND Corporation, October 15, 2020), https://www.rand.org/pubs/research_reports/RRA704-3.html.

[292] Bronner, "Les lumières à l'ère numérique."

[293] See https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/ and https://osome.iu.edu/ to use the tools

[294] "Top 10 Trends of 2014: 10. The Rapid Spread of Misinformation Online" (World Economic Forum, 2014).

[295] Sarah Kreps, "The Role of Technology in Online Misinformation," *Foreign Policy - Brookings*, June 2020.

of the EU in a 2019 report[296], and further regulation must therefore be established to compel social media companies to publicize these data or facilitate their accessibility for researchers. Today, the only social media providing minimal information allowing for in-depth research on the topic is Twitter, through their accessible Application Programming Interface (API)[297]. Twitter's open APIs lead to an academic research on disinformation and foreign interference largely focused on Twitter, excluding other platforms such as Facebook or Instagram, that represent yet crucial tools for information manipulation with potentially diverse mechanisms and data. As a consequence, Twitter takes a disproportionate importance in debates related to this issue, while it actually has less users. As an example, the last data of the Digital News Report 2022 revealed that while 41% of Europeans and 35% of North Americans claimed to have gotten their news from Facebook in the last week, only 9% of Europeans and 12% of Americans got them on Twitter. The gap is even higher when looking at the proportion of Europeans and Americans that simply have a Facebook or Twitter account, although they vary largely according to the study. Therefore, Twitter remains used by a small portion of the population, which can also question the importance of information manipulation campaigns (cf Chapter 3 section 3).

Overall, scholars agree upon the fact that research works necessitate the possibility to look at the full picture, which includes data and algorithmic techniques, in order to produce highlighted and adapted recommendations that will have a real impact[298]. Therefore, with adapted resources and a better access to social media data, researchers could deepen their analyses and bring valuable insights for policy-makers so as to design appropriate measures. The role of research is thus crucial, insofar as negative effects of "*regulation uninformed by systematic research, may be as damaging to democratic systems as the threats themselves*"[299]. However, isolated research is useful but not sufficient and information-sharing among different institutions and actors is crucial to produce enlightened analyses.

2. Cooperation and coordination: essential efficiency drivers

From information-sharing to enhanced governance, cooperation and coordination is essential among allies in order to improve countermeasures' efficiency.

[296] "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions" (Brussels: Council of the European Union, December 10, 2019).
[297] Wardle and Derakhshan, "Information disorder."
[298] Barela and Duberry, "Understanding Disinformation Operations in the Twenty-First Century"; Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling," *The Finnish Institute of International Affairs*, FIIA Briefing Papers, November 2017; Bronner, "Les lumières à l'ère numérique."
[299] Woolley and Howard, *Computational Propaganda*.

a. Information-sharing and examples of best practices as sources of inspiration

Knowledge should be shared as much as possible among different institutions, agencies, and people, at the national, as well as international level.

The comparative method in this respect is an excellent tool to gather knowledge from different countries and identify examples of best practices. Here we extend the Franco-American comparison to other countries that are often highlighted in the literature as examples of best practices. While France and the U.S. can take example on one another for several policies, we will present two Northern countries, on which France and the U.S. could draw inspiration for some policies. Finland and Sweden are often considered as inspiring countries in terms of raising awareness on information manipulation.

Sweden represents a model in terms of raising awareness on information manipulation and coordination between civil society and different institutional agencies. Digital literacy campaigns are launched by the government and civil society organizations in public spaces going from schools to the metro, along with social media. Sweden also built several independent agencies, including one responsible for psychological defense against manipulation. Horizontal efforts and cooperation among the Swedish government and national agencies, civil society organizations and the population built a multi-level organization, efficient for raising awareness and fighting information manipulation.

The historical and geographical context in Finland is such that the country is generally relatively well prepared against Russian disinformation campaigns. Children are taught from an early age to think critically and to control their sources. Finnish students seem therefore well-prepared to face information manipulation, and a comparison study indeed showed that Finnish students were better at detecting fake news than American students[300]. Sweden and Finland therefore represent two countries in which efficient policies and measures against information manipulation were implemented, that could be further analyzed along with other countries' policies in order to design more efficient approaches against information manipulation in the U.S. and France.

Additionally, the "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation" built by the EU INGE Special Committee[301] recommends taking into account best practices in diverse countries to build specific policies. Examples included are: "*Australia's National Counter Foreign Interference Coordinator, Finland's Security Committee assisting the government and ministries, Sweden's Civil Contingencies Agency, new agency for psychological defence and National China Centre, France's new national agency Viginum, Lithuania's National Cyber Security Centre, and Taiwan's interagency disinformation coordination taskforce*". Here, the French agency Viginum is mentioned as an example of best practice, although fairly recent.

[300] Annabelle Timsit, "A Study Compared Finnish and American Students' Ability to Detect Fake News," *Quartz*, May 3, 2019.

[301] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation."

Regarding information-sharing, one recommendation would be to reinforce the information-sharing activity of certain centers and agencies among allies. As an example, the European Center of Excellence for countering hybrid threats (Hybrid CoE), that cooperates with NATO and the EU, tries to coordinate member states' activities to share knowledge. The Center recently set up an extremely interesting exercise of cooperation and coordination to improve the response against information manipulation campaigns[302]. Gathering four countries including a wide range of participants (more than 80), from disinformation experts, to EU and NATO employees, along with journalists and national representatives responsible for strategic communication, the exercise was designed to reproduce a situation of false information manipulation campaign to which the various country groups had to respond. This type of exercise is a great way to share knowledge among allies and be better prepared for a future real attack of this kind. The U.S. and the EU should cooperate, according to Daniel Fried and Alina Polyakova[303], by creating a "Counter-Disinformation Coalitiation" that would gather like-minded states and non-states actors in order to share information regularly and establish common principles.

If cooperation is essential to share knowledge and improve the threat's understanding, it must be further developed to achieve a satisfying coordinated governance, at all levels.

b. Coordinating governance, from local to international level

As previously mentioned, election interference through the use of social media in manipulating information is a multifaceted issue to which no clear answer can be given and that requires the involvement of various actors at different levels[304]. At the national level, the government must first build the adapted agencies, but also find a way to coordinate their work. For example, the U.S. built the GEC, as we saw earlier, in order to coordinate the multiple American agencies working on the matter. But if we mainly analyzed national initiatives, it is important to underline that decision-making should not be vertical, and that local projects matter. According to James Lamond and Jeremy Venook: "*information sharing between federal, state, and local officials could prove critical*"[305], each bringing its own expertise to build a multidimensional approach.

The multiplication of projects emerging at different levels to counter the threat brought positive developments, however, building a strong cooperation between actors and structures is essential in order to avoid a counterproductive effect, as highlighted by the last INGE report[306]. Coordination must also be operated at the regional level between institutions of a regional organization such as the EU, or

[302] Anne-Françoise Hivert, "En Finlande, la riposte des démocraties s'organise face aux menaces hybrides," *Le Monde*, June 4, 2022.
[303] Daniel Fried and Alina Polyakova, "Democratic Defense against Disinformation" (Atlantic Council, March 5, 2018).
[304] Petros Iosifidis and Nicholas Nicoli, *Digital Democracy, Social Media and Disinformation* (London: Routledge, 2020).
[305] Lamond and Venook, "Blunting Foreign Interference Efforts by Learning the Lessons of the Past."
[306] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation."

between regional organizations. As an example, EU-NATO cooperation is crucial in that field, and has already been initiated after the Joint Declarations of Warsaw and Brussels in 2016 and 2018. Information-sharing is elaborated through exchanges of staff and knowledge with different structures such as the NATO Centres of Excellence or NATO Hybrid Analysis Branch, along with the Hybrid Fusion Cell, or the EU Strategic Communication Task Force, and could be further developed[307].

Cooperation is also crucial between public and private actors. As Maud Quessard pointed out in her book, officials often regret the lack of cooperation with private actors and the scattering of activities without synchronization, leading to counterproductive effects[308]. Many companies or organizations that are not social media companies but more often operate in the cybersecurity field, can represent a valuable help for governments that might lack cybersecurity expertise. While governments sometimes lack time and resources, "*the private sector is quicker to embrace the latest technologies and should be able to offer solutions to monitor, detect and counteract election meddling*", according to Mika Aaltola[309]. For example, the U.S. FBI and Justice Department worked with Internet Systems Consortium, that is a non-profit corporation in order to detect and take down the Coreflood botnet that was using users' data for a total worth 100 million dollars. France also worked with diverse cybersecurity companies to benefit from their expert's knowledge and tools. The French government indeed asked two cybersecurity companies to equip Viginum and DGSI's computer systems and programs in order to detect information manipulation operations that are Sahar and Storyzy[310].

3. The role of law in guaranteeing the rule of law: a necessary regulation

One crucial element in countering information manipulation operations is in providing the necessary legal framework to address the issue. From national to regional and international regulation, along with working with actors concerned by the regulation, designing an adapted legal framework is not an easy task and there is still room for improvement.

a. Private-public partnerships on regulation: working hand in hand with platforms

After having analyzed the legal loophole encompassing social media in the second chapter, we can measure the importance of regulating these companies. If changes have been brought by governments or social media around regulation since the 2016 and 2017 elections, it is still difficult to identify clear rules applicable to all social media that really contain information manipulation on their networks.

[307] "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions."

[308] Maud Quessard, *Stratégies d'influence et guerres de l'information : Propagande et diplomatie publique des États-Unis depuis la guerre froide*, *Stratégies d'influence et guerres de l'information : Propagande et diplomatie publique des États-Unis depuis la guerre froide*, Des Amériques (Rennes: Presses universitaires de Rennes, 2020).

[309] Mika Aaltola, "Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling," *The Finnish Institute of International Affairs*, FIIA Briefing Papers, November 2017.

Social media companies did make consistent efforts in trying to fight information manipulation on their platforms, after realizing the importance of the threat as we saw earlier. Mark Zuckerberg in 2019, even claimed publicly that he was favorable to more regulation, in the sense that Facebook had too much control[311]. However, as many scholars argue, these efforts are not coordinated between platforms, are often only *ad-hoc* measures, and overall not sufficient. The title of the 2020 NATO report that analyzes five social media platforms (Facebook, Twitter, Instagram, YouTube and Tiktok) says it all: "How social media companies are failing to combat inauthentic behaviour online". They conclude the report by stating that "*despite significant improvements by some, none of the five platforms is doing enough to prevent the manipulation of their services*", and social media should make it more difficult – if not impossible – for manipulation service providers to sell, promote their services and access the platforms[312]. They should also increase their transparency, which could be the object of a new independent oversight that would be able to access social media information and build transparent reports, without intervening in their functioning, in order to evaluate their progress in countering information manipulation[313]. If some important steps have been taken by some social media companies (mainly Twitter and Facebook as previously mentioned), other platforms could benefit from their experience and expertise, and debate and information-sharing among social media companies could be a way to provide new insights to each platform. In this respect, an idea that is often shared is to pursue their work in the Global Internet Forum to Counter Terrorism (GIFCT), in sharing tools to counter terrorism on their platforms, in the domain of information manipulation and election interference with another forum[314].

However, social media should not be left alone in designing their regulation and functioning. First, they must take advantage of experts' knowledge to design more adapted algorithms, in compliance with democratic values. Second, governments and social media platforms should work together at the international level to establish common basic rules, applicable to all globally[315]. In this respect, Emmanuel Macron in his speech at the Internet Governance Forum, a UN event taking place in Paris in 2018, presented three different approaches in regulating social media platforms, underlining the third as the best way to improve the situation[316]. The first method to regulate social media is to let them auto-regulate, as it was the case since these platforms emerged, highlighting that we already saw the deficiencies of this method. The second method would be to impose several obligations on social media, designed by states, that would also be able to control social media's content. If this method is used on a limited scale in some democracies today, its deepening would not be desirable, as it would

---

[310] "France: Viginum and DGSI Consider Partnering with Defence-Backed Startups to Fight Fake News," *Intelligence Online*, December 13, 2021.
[311] In: Ben Epstein, "Why It Is So Difficult to Regulate Disinformation Online," in *The Disinformation Age*, ed. W. Lance Bennett and Steven Livingston, Cambridge University Press (Cambridge University Press, 2020).
[312] Fredheim et al., "Social Media Manipulation Report 2020."
[313] Fredheim et al.
[314] Lamond and Venook, "Blunting Foreign Interference Efforts by Learning the Lessons of the Past."
[315] Bronner, "Les lumières à l'ère numérique."
[316] Emmanuel Macron, "Speech by M. Emmanuel Macron, President of the Republic at the Internet Governance Forum" (Internet Governance Forum, November 12, 2018).

lead to authoritarian methods. The third and best way to regulate social media platforms is therefore a multi-actor regulation, in which states, social media companies, but also civil society and experts could work together in building the appropriate legal framework. In a report on how to combat foreign disinformation, RAND researchers underline the importance of not forgetting smaller social media platforms in the regulating process, as "*smaller, locally popular social media platforms could be at higher risk of disinformation than larger, mainstream ones*"[317], and it is therefore essential to not underestimate the power of these platforms.

b. The role of international law and sanctions

The role of international law and sanctions is a very specific and technical question, that is essential to address, although it will not be developed thoroughly here, insofar as it would require a full legal analysis[318]. However, several aspects are often addressed by scholars and provide indications for countering these hybrid threats. First, as Jacqueline Van de Velde put it: "*Cyber election interference fits awkwardly within this international legal framework*"[319]. The legal framework depends from one country to another, and as time and space are hardly delimited in cyberspace, it makes it a contested and thus inherently political space[320]. However, as Joseph Nye argued[321], if we built treaties to regulate contested domains such as slavery or chemical weapons, they would be equally relevant for cyberspace, and writing treaties could represent a way to clarify basic common principles that should be respected in cyberspace, and on social media platforms in particular[322]. As we saw in Chapter 2, it is now widely accepted that international law applies to cyberspace, although several challenges hinder its practical application. Yet, international law is not sufficient and the scattering of rules at the international level impedes a clear understanding and application of laws, and social media companies therefore often operate in an unregulated environment. As a consequence, harmonization of laws at the international level is necessary. This could be possible through the development of working groups in international relations. The United Nations (UN) already launched similar working groups with the UN Group of Governmental Experts on Cyber-Security (GGE), and after a period of vacancy after a failure in 2017, consultations were launched again and produced a new report in 2021. However, if the major consensual decision that international law applies to cyberspace was approved, how it applies and how it can be implemented remain widely debated issues. Another working group, the UN Open-Ended Working Group (OEWG), included a larger panel with any interested stakeholder, which is a significant step forward. However, it is still not clear how the stakeholders can participate in the decision-making, and their work is mainly targeted at malicious ICT activities on critical

[317] Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*.
[318] Ohlin and Hollis, *Defending Democracies*.
[319] Jacqueline Van De Velde, "The Law of Cyber Interference in Elections," *Social Science Research Network*, SSRN Scholarly Paper, May 15, 2017.
[320] Deibert, "Trajectories for Future Cybersecurity Research."
[321] Joseph S. Nye, "The End of Cyber-Anarchy?," *Foreign Affairs*, February 15, 2022.

infrastructure and information manipulation, disinformation or social media are not mentioned. We argue that a specific working group on foreign interference on social media through information manipulation should be created to discuss what rules could be realistically applicable at the international level. France and the US could take the lead in this cause at the international level, given their key position in international organizations. Although at a lesser extent for France, its role could be crucial in the EU to try to build a common European approach.

The main issue in combating foreign election interference through social media is that sanctions and retaliation are not developed enough and therefore do not prevent malicious actors from using these techniques. According to the 2020 NATO report on social media manipulation: "*Violators can be deterred by economic, diplomatic, and criminal penalties. The ongoing practice of widespread and relatively risk-free social media manipulation needs to stop.*"[323]. One response that could have a deterrent effect that is the main tool today is the naming and shaming strategy. By attributing attacks to Russia, the US government hopes that it would have a deterrent effect in the future. At the national level, although France's Arcom is not granted a sanctioning power, the agency mainly uses the naming and shaming strategy when assessing social media's action in fighting information manipulation, which gives them an incentive to improve their measures to avoid appearing as the black sheep[324].

Some deterrence practices can also be more covert, as the U.S. did in the past through cyber operations, including one in which IRA's internet access was blocked by the US Cyber Command in 2018, along with messages to the individuals directing the operation in order to show Russia that the US was not only aware of Russian activities but also ready and able to respond[325]. Many argue that sanctions are crucial to deter malicious actors from launching information manipulation operations. The European Commission, in a communication to other EU institutions on elections' safety claimed that "*deliberate attempts to manipulate elections should be actively combatted, including through sanctions*", although not specifying what type of sanctions should be applied[326]. Some emphasize on social media platforms' accountability, such as U.S. Senator Mark Warner that supported social media's accountability in removing inauthentic and automated accounts in 2019[327]. However, the implementation of these sanctions can be extremely difficult in practice, and when applied incautiously, they might prove to be not efficient or even counterproductive[328]. An important factor to take into account when deciding on sanctions is the proportionality. Sanctions must be proportional to

---

[322] Van De Velde, "The Law of Cyber Interference in Elections."
[323] Fredheim et al., "Social Media Manipulation Report 2020."
[324] "Lutte contre la manipulation de l'information : déclarations des opérateurs de plateformes en ligne et questionnaires de l'Arcom," Arcom, accessed September 12, 2022, https://www.arcom.fr/vos-services-par-media/internet-et-reseaux-sociaux/lutte-contre-la-manipulation-de-linformation-declarations-des-operateurs-de-plateformes-en-ligne-et-questionnaires-de-larcom.
[325] Jeangène Vilmer, "Information Defense."
[326] European Commission, "Securing Free and Fair European Elections A Contribution from the European Commission to the Leaders' Meeting in Salzburg on 19-20 September 2018" (2018).
[327] In: Max Boot, Jeane J. Kirkpatrick, and Max Bergmann, "Defending America From Foreign Election Interference" (Council on Foreign Relations, March 6, 2019).
[328] Van De Velde, "The Law of Cyber Interference in Elections."

the harm done, and important enough to encourage the actor to change its behavior. For example, when dealing with states and the "*most profitable and influential companies on earth*", economic sanctions might prove inefficient when they appear as a "*drop in the bucket*"[329]. Above all, implementing laws and sanctions raises critical questions on the necessary balance between regulation and liberty that will be addressed in the next part.

Section 3 : Questioning and justifying the necessity to take action

After having presented possibilities of improvement in fighting information manipulation through social media, this last part aims at responding to legitimate questions on the necessity and utility to act, when looking at some particularly controversial aspects of the issue.

1. Is it really worth it?

Controversial issues ranging from countermeasures' drawbacks to the functioning of social media and their role in a broader context makes us wonder if action is really needed and desirable.

a. Ongoing debates: finding balance between regulation and freedom

The previous part aimed at opening doors to better regulation at the international level so as to better frame the threat. However, freedom of speech is at the basis of social media, and states must be extremely careful in finding a balance between regulating while protecting basic liberties.

The main fear that is underlined in various research works, is for the state to react in an authoritarian way by creating what George Orwell called a "Ministry of Truth". Several basic liberties are at stake here: freedom of speech, opinion and information could be infringed by excessive regulation. Most of the reports on information manipulation recommend little intervention from the state in order to ensure that it does not trespass citizens' liberties, as authoritarian regimes do on social media[330]. We saw in the second chapter how democracies were disadvantaged in this regard and how filtering content as a way to respond to foreign interference was a risky step towards authoritarian control of the information. According to Daniel Fried and Alina Polyakova, if responding to these attacks with the same means as authoritarian regimes can be tempting, our liberal democratic regimes will actually be more efficient in countering information manipulation, and "*social resilience is going to be a better defense against influence operations in the long term*"[331].

[329] Epstein, "Why It Is So Difficult to Regulate Disinformation Online."

[330] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies"; Woolley and Howard, *Computational Propaganda*; Deibert, "Trajectories for Future Cybersecurity Research"; Petros Iosifidis and Nicholas Nicoli, *Digital Democracy, Social Media and Disinformation* (London: Routledge, 2020).

[331] Daniel Fried and Alina Polyakova, "Democratic Defense against Disinformation" (Atlantic Council, March 5, 2018).

With the balkanization of the Internet[332], Ronald Deibert noted that there is a tendency of states towards more control of social media content, and many authoritarian regimes now use the filtering and blocking of content as a way to prevent dissident opinions, a trend that will be hardly reversible[333]. Applying a strict regulation and control over social media platforms can appear as an excuse for improving surveillance methods by states and thus represent a privacy violation. In two different chapters of the book *Defending democracies,* Evelyn Douek and Duncan MacIntosh discuss the need to regulate content when coming from foreign actors[334]. They both question the commonly accepted position that foreign speech is not desirable and not protected by freedom of speech, in the sense that foreign speech might be part of the political discourse and should not necessarily be combatted. To this, we would respond that foreign speech is acceptable unless it manipulates opinions, interfering in the electoral process.

The issue of regulation has already triggered huge reactions and debates both in the U.S. and France. Scandals of Cambridge Analytica and the Snowden disclosures that revealed big data surveillance and gathering by private companies and the state, represented issues that were taken very seriously by the American population[335]. As the "land of the free", American citizens are deeply attached to their private liberties, and these scandals showed them how their data could be used without their consent. Although not directly targeting foreign disinformation on social media, the protests and pressure of Americans on the government and companies, in response to these cases show how much citizens value their personal data and privacy, and care about controlling their online environment.

In France, heated debates emerged over regulation and liberties after some of the government's decisions, including the creation of Viginum and the law on information manipulation. While the creation of Viginum did not make a lot of noise and its implications were more extensively discussed by scholars or politicians, the law on information manipulation was subject to protests among the French population. During the discussions in Parliament and after the implementation of the law in 2018, heated debates broke out in response to controversial elements of the law[336]. French citizens feared that the law would deny freedom of speech and that the judge's decision in 48h regarding the accuracy of the information would either be very difficult or against free speech if premature. However, the decision of the Constitutional Council strictly restricted what could be considered as false information, and this part of the law was eventually rarely used, questioning more its utility than its hostility to freedom of speech. According to Couzigou, the French law is for the moment satisfying

[332] The fact that states retake control of their Internet system at the national level.

[333] Ronald J. Deibert, "Cyber-Security," in *Routledge Handbook of Security Studies, Thierry Balzacq &*, by Myriam Dunn Cavelty and Thierry Balzacq, 2nd ed. (Routledge, 2016).

[334] Evelyn Douek, "The Free Speech Blind Spot: Foreign Election Interference on Social Media," and Duncan MacIntosh, "Protecting Democracy by Commingling Polities: The Case for Accepting Foreign Influence and Interference in Democratic Processes,", in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Jens David Ohlin and Duncan B. Hollis, Ethics National Security Rule Law Series (New York: Oxford University Press, 2021).

[335] Deibert, "Cyber-Security."

[336] Coline Vazquez, "Pourquoi la loi contre les fake news suscite une levée de boucliers," *Franceinfo*, June 8, 2018.

and should not go further in obliging platforms to remove false content as its German neighbor did, due to the risks of over-censorship by platforms (when fearing to get a fine for non-removal of false content), and therefore detrimental to freedom of expression[337]. The creation of Viginum also raised questions regarding individuals' liberties, especially due to the fear that a government-linked agency could have access to social media data and therefore control citizens' information. However, the government responded by claiming that data was cancelled after a few months, and by creating an ethical committee in charge of guaranteeing freedom of speech and information. More broadly, we can see that French citizens are concerned with the government's overstepping on their liberties, as depicted on this graph by the Pew Research Center according to a 2021 survey study.

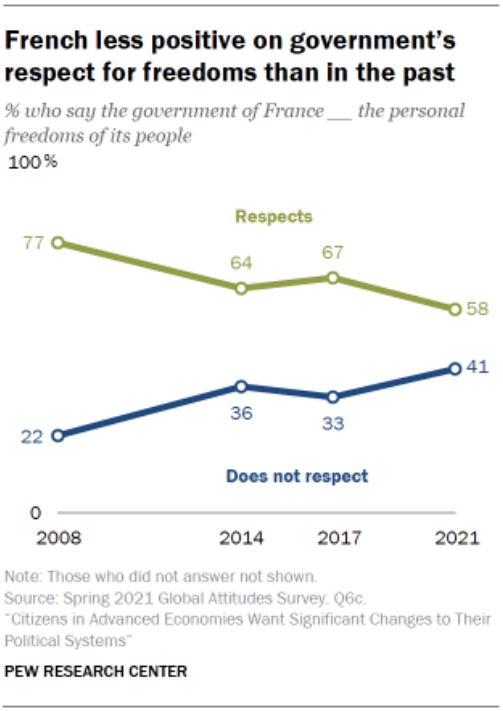

Figure 18: French vision of their government's respect for freedoms (2008-2021). In: Wike et.al., "Citizens in advanced economies want significant changes to their political systems", *Pew Research Center*, 2021.

The proportion of French claiming that their government respects their personal freedoms has decreased from 77% in 2008 to 58% in 2021[338]. A too strong regulation by the state over social media content would only drive that fear.

In order to respond to these interrogations, it is essential to remember that one crucial recommendation is to always bear in mind democratic values, and not use the same techniques as authoritarian regimes. Responding with the same means would play into the hands of authoritarian regimes, and reinforce fears of a state overstepping too much on individual liberties and private companies.

[337] Irène Couzigou, "The French Legislation against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression," *Election Law Journal: Rules, Politics, and Policy* 20, no. 1 (2021).
[338] Wike et al., "Citizens in Advanced Economies Want Significant Changes to Their Political Systems."

b. The social media system *per se:* source of the problem?

Another stance taken in criticizing countermeasures to respond to information manipulation through social media, is to claim that small changes will be inefficient in the sense that the social media system is inherently prone to information manipulation, and is not likely to change. Unless a profound transformation of their financial model is imposed on social media, companies will keep hosting and encouraging all types of content on their platforms.

If some efforts have been made by social media companies to fight information manipulation, we saw that these efforts were not sufficient. Scholars have argued that social media companies will never take the necessary measures if not pressured by an external actor, in the sense that they seek profit, and as long as their algorithms are built in a way that yields more money, social media will have no incentive to change them. According to Joseph Nye: "*The so-called "free" services of social media are based on a profit model in which the user or customer is actually the product, and their information and attention is sold to advertisers*"[339]. In this respect, all the money earned by social media comes from the users, who are constantly encouraged to remain as much as possible on the platforms through hundreds of solicitation techniques. In the second chapter, we analyzed how cognitive biases lead us to engage more with emotional, divisive, novel, or negative content. Yet, if individuals are more responsive to this type of content, algorithms will automatically keep favoring it to keep users engaged[340]. Frances Haugen's disclosures on the topic brought crucial insights on Facebook's algorithms and the vision of the company[341]. After working two years as product manager at Facebook, Frances Haugen left the company with thousands of documents to reveal all the aspects that she thought were dangerous for users. In a testimony before the U.S. Senate in October 2021, she claims that in all the regular conflicts that were arising at Facebook opposing the company's profits to users' safety: "*Facebook consistently resolved those conflicts in favor of its own profits*". Along with issues of health regarding teenagers, Frances Haugen underlined the role of Facebook in favoring disinformation, consciously. In her statement, she reveals that if Facebook created a civic integrity team and changed its algorithms before the 2020 elections to prevent disinformation, the team was dismantled the day after the election, and the company, which saw that the new algorithm was producing less engagement, went back to the previous one. She also claims that if before 2018, algorithms were designed to spend more time on the platform, the change of algorithm to favor engagement was responsible for favoring more divisive, negative and violent content, but that the company knowingly (internal studies reported it to the direction) kept the new algorithm that was yielding more profit. The fact that Facebook and social media are perfectly aware about their algorithms and the potential effects that they generate is largely corroborated by former employees,

[339] Nye, "Protecting Democracy in an Era of Cyber Information War."
[340] Wardle and Derakhshan, "Information disorder"; Lin, "Conclusion: An Outsider Looks In."
[341] "Frances Haugen Testimony before the United States Senate Committee on Commerce, Science and Transportation" (U.S. Senate, October 4, 2021).

who spoke out to show these platforms' flaws[342]. According to David Chavalarias[343] who studied mathematics, the reason is quite simple and can be found in mathematical theorems of information. An increase in the quantity of social influence becomes counterproductive at some point, and is not the reflection of society, in the sense that a minority can have a huge influence through little cooperation and the virtuous circle that the capitalism of influence creates. Hence, for David Chavalarias: the negative effects on the society are not intentional, but "*are consubstantial to any business that seeks to commercialize social influence*"[344]. He even goes further in saying that only totalitarian regimes that can control social media can be stable regimes, and democracies that look for stability within this social media system will only tend towards illiberalism or authoritarianism. However, David Chavalarias concludes in stating that nothing is doomed, and gives many different recommendations that can help in slowing down the process, or best, change in several ways the online environment. Frances Haugen also revealed the Facebook Files for that purpose: because change is possible in diverse manners. If more incentive is given to social media to change their algorithms and to rely on experts' knowledge with an ethical perspective to design them, our online environment could be safer and less prone to information manipulation by foreign actors.

c. Aren't we overestimating the threat?

Beyond those who think that foreign interference in elections through social media manipulation cannot or should not be addressed for several reasons, there are those who believe that this threat might actually not be as important as we think. First, because social media are not used by everybody and might not have a crucial impact on society and then, because it seems unlikely that social media can really change the outcome of the election. These interrogations are legitimate and we wanted to highlight them in order to better frame the issue and respond to it.

First, we can legitimately wonder why this issue seems to matter so much, if traditional media are still more important than social media in the informational landscape, especially if one does not have a social media account. When looking at the data from the Reuters Institute in their Digital News Report 2022[345], 40% of the French population that responded to the survey claim to get their news on social media in 2022, while they were 64% to say their primary source of news is television, and 69% for online news (including social media but also online newspapers, radios, TVs…). The numbers in the U.S. are quite similar with 40% of Americans using primarily social media to get their news in 2022, 67% for online news, and a little lower for television with 48%. Overall, social media only is generally less used to get news than traditional media, either on television or online. A survey data by Michael A. Beam, Paul M. Haridakis, Myiah J. Hutchens, and Jay D. Hmielowski, in the book *The*

[342] *The Social Dilemma*, Documentary (Netflix, 2020).
[343] Chavalarias, *Toxic Data*.
[344] Translated from French. In: Chavalarias.
[345] Newman et al., "Digital News Report 2022."

Presidency and Social Media[346], found that the use of social media during the presidential campaign was actually "*rather anemic*", and that people were informed mostly through local news outlets or day-to-day conversations. When we look at the numbers for each social media, we can see that some social media are actually used at a very little scale.

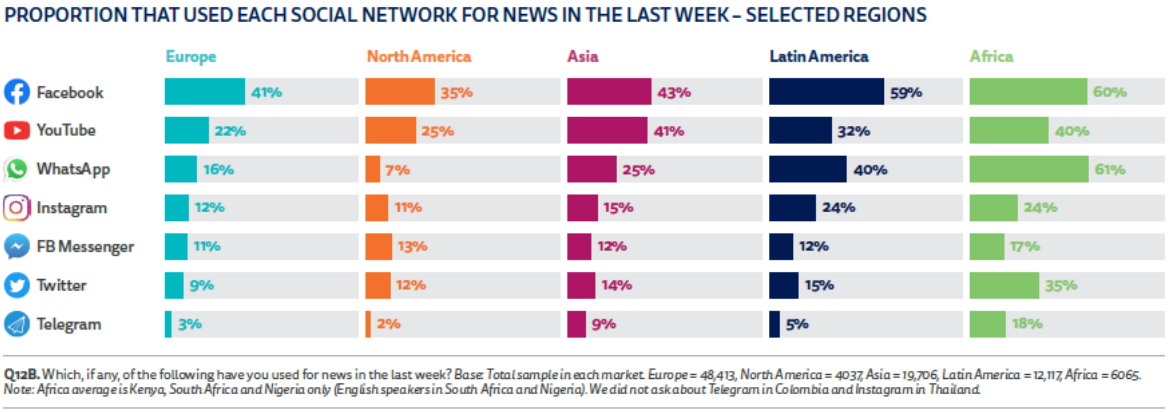

Figure 19: Proportion that used each social network for news in the last week - selected regions. Digital News Report 2022. *Reuters Institute*. June 2022.

On this graph extracted from the Digital News Report 2022, we can see that Facebook is the most used social media for news weekly. One interesting aspect here that was mentioned earlier, is the fact that Twitter takes a disproportionate importance in political debates regarding information manipulation. The fact that research is mainly focused on Twitter due to the lack of other platforms' data brings a bias in the analysis. Moreover, Twitter is known to be a very political social media, and the population that is active on Twitter is not representative of the overall population from a sociological point of view. Educated, white, young males are more likely to have a Twitter account than others for example[347]. The others, and the roughly 90% remaining of Americans and Europeans that do not claim to have used Twitter as a source of news in the last week, could therefore feel that the issue of information manipulation on Twitter is a non-issue since it concerns a small part of the population. We would nevertheless argue that the significance of these operations of information manipulation on Twitter goes beyond social media's users in the sense that many false or distorted information are then reported by traditional news media, that participate in spreading this information to the wider public. Even though individuals might get their information a lot on television, the television channels themselves get their news a lot from social media. Himself journalist and co-founder of *Le Monde* fact-checking channel *Les Décodeurs*, Samuel Laurent wrote a book on how journalists tend to look at Twitter trends and report them as if they were representative of an overall general opinion, which can be a danger for democracy[348]. Traditional media tend to relay information even when they seem

[346] Michael Beam et al., "Social Media, News Platforms, and Partisan Exposure: Discourse, Disruption, and Digital Democracy in the 2016 Presidential Election," in *The Presidency and Social Media*, ed. Dan Schill and John Allen Hendricks (Routledge, 2017).
[347] Mason Walker and Katerina Eva Matsa, "News Consumption Across Social Media in 2021" (Pew Research Center, September 2021).
[348] Samuel Laurent, *J'ai vu naître le monstre. Twitter va-t-il tuer la #démocratie ?*, Les Arènes, 2021.

dubious, as long as they go in line with their partisan affiliation[349]. It is therefore crucial to notice that everyone can be impacted by these campaigns, although not directly using social media.

Another aspect that could trigger some interrogations on the necessity to act and on the fact that this threat might be overvalued, is that it is unlikely that social media information could change the outcome of the election. When studying presidential elections and individuals' vote, we generally see that most of them have their mind set on a candidate long before the vote, and that their preconceived beliefs make that they would not change opinion easily. Many scholars, when studying the impact of fake news and radical content on social media, found that this type of content generally reinforces people's beliefs more than they make them vote for another candidate. Sarah Kreps, for example, finds in her quantitative study that disinformation campaigns had limited impact on political opinions[350], and RAND researchers also show that "*there is limited evidence that they can change strongly held beliefs*"[351]. Nonetheless, these claims generally refer to people that were already convinced, and do not tackle those hesitating, which opinions on candidates might change easily. Another claim underlined by Costica Dumbrava in a report on social media risks to democracy for the European Parliamentary Research Service, is that "*the exposure to and engagement with false content online seem to vary greatly across groups and individuals*"[352], which means that not all individuals are impacted by disinformation, which could diminish the actual impact of these campaigns.

In a hearing before the U.S. Senate in January 2019, Twitter revealed the results of a study of Twitter activity during the electoral period of 2016[353]. They found that "*automated election-related content associated with Russian signals represented a very small fraction of the overall activity on Twitter in the ten-week period preceding the 2016 election*". However, it is important to highlight that, in the methodology detailed in the report, "election-related" content is an ambiguous term. If the number of election-related Tweets linked to Russian activity is only 2.12 million, the overall number of tweets by Russian-related accounts is not mentioned. Yet, if election-related tweets are relatively easy to identify (with hashtags related to the candidates for example), other tweets might be political and influence Americans' opinions on more general political matters that could have a crucial impact on their final decision in the presidential election. Moreover, claiming that disinformation posts represent only a small proportion of all posts is ignoring the fact that not all posts have the same capacity to influence users' votes, as Herbert Lin underlined. Posts falsely claiming that Hillary Clinton is linked to a pedophile network are likely to have more impact on somebody's opinion, than a post from a random individual supporting one policy.

[349] Bronner, "Les lumières à l'ère numérique."
[350] Kreps, *Social Media and International Relations*.
[351] Cohen et al., *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*.
[352] Costica Dumbrava, "Key Social Media Risks to Democracy: Risks from Surveillance, Personalisation, Disinformation, Moderation and Microtargeting" (Brussels: European Parliamentary Research Service, December 2021).
[353] "Update on Results of Retrospective Review of Russian-Related Election Activity," January 19, 2019.

Official reports by the U.S. Senate did not find evidence that could prove that the implication of Russia in the 2016 election had changed the outcome of the election, but still leave the question open, it is a plausible hypothesis. Regarding France, Emmanuel Macron won the presidential election, demonstrating that the information manipulation operation did not have the desired effect. This is especially true given the size of Macron's victory, indicating that even if this operation might have altered some people's opinions, it did not affect the election's outcome. However, when an election is tight as it was the case in the 2016 U.S. presidential election, the victory sometimes relies on small details. A small percentage of the population voting for someone else, or not voting for the candidate they previously supported, after reading content related to disinformation operations, can therefore change the outcome of the election, as we show in Chapter 2. Overall, while some legitimate questions and arguments are made for making the assumption that this threat is overestimated, preliminary responses show that they might not be satisfying, and we argue in this last part that, even if they are right in some aspects, this threat is serious and calls for action.

2. Overcoming doubts: a call for action

Here we show that information manipulation operations on social media in periods of elections especially, can have a negative impact on the society as a whole, beyond elections' results, and that it is not likely to disappear soon. Therefore, we argue that despite all interrogations, potential consequences are too risky not to act.

a. Going beyond the outcome of the election: a risk for democracy

The main idea here is to show that questioning whether information manipulation campaigns changed the outcome of the elections diverts us from the real focus: the disruption of democracy in general. As Jens David Ohlin put it: "*The danger posed by a particular threat is measured not by the actual damage caused but rather by the potential disruption it represents*"[354]. Information manipulation operations might have several negative impacts on the society as a whole.

First of all, information manipulation campaigns on social media, generally succeed in their main objective studied in the previous Chapter, that is to disrupt democratic societies and systems. When individuals know they have been or they are being manipulated by a foreign actor, this leads to an erosion of trust in the institutions, the media or the leaders. One key element of representative democracies is that people accept to be governed by representatives because they have been elected and therefore gained their legitimacy as representatives of the people. Yet, when a foreign power interferes in an election campaign, the winning candidate can accede to power with an "*eroded*

[354] Ohlin, "A Roadmap for Fighting Election Interference."

legitimacy"[355]. In a survey realized by the Pew Research Center after the 2016 elections, it was found that 88% of Americans claimed that false information had left them confused about current basic facts[356].

The Digital News Report of 2018 after the two elections show that France and the U.S. both have low levels of trust in the news overall and in social media among their population.

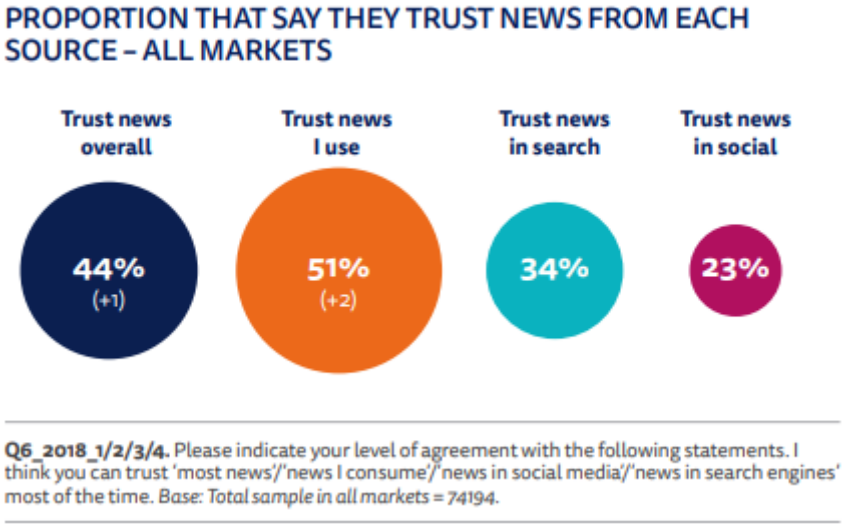

Figure 20: Trust in the news. Newman et.al., "Digital News Report 2018", 2018.

Out of 37 countries, France ranks 29th and the U.S. 31st, with the French and American population trusting news overall at 35% and 34% respectively. Levels of trust in social media news are particularly low with only 19% in France and 13% in the U.S. Campaigns of disinformation on social media are considered as potential explanatory factors in the report[357]. When voting for their representatives, citizens must be able to have access to relatively objective and trustworthy information. A defiant attitude towards the overall news therefore means that the democratic process of the election is somewhat biased. A 2019 survey by the Pew Research Center indeed showed that 68% of Americans claimed that made-up news and information had a big impact on their confidence in government institutions[358].

Another intended result of information manipulation by foreign actors is societies' polarization and division. Divisions among American or French societies largely predate information manipulation operations and can be explained by various different factors, so it would be largely exaggerated to claim that these campaigns are responsible for societal divides. However, we believe that it is no exaggeration to say that these operations reinforced these divisions. If some characteristics of social media's functioning – such as the tendency of algorithms to create filter bubbles or favor extreme content – already tend to reinforce polarization, foreign actors exploit these characteristics, coupled

[355] Barela and Duberry, "Understanding Disinformation Operations in the Twenty-First Century."
[356] Michael Barthel, Amy Mitchell, and Jesse Holcomb, "Many Americans Believe Fake News Is Sowing Confusion" (Pew Research Center, December 15, 2016).
[357] Newman et al., "Digital News Report 2018."

with cognitive biases and pre-existing tensions, to deepen the gap between different groups among the population. These impacts are real, and can also be physical when they lead to real-life confrontations, as we saw in Chapter 2 with the organization of different events by Russian-related accounts. As an illustration of this, from 2015 to 2017, the IRA organized 124 events in the United States, which shows its anchoring in the local reality of Americans[359].

Several studies have shown that citizens are indeed worried about this phenomenon. According to the Eurobarometer survey of 2021, more than half of Europeans are generally concerned by electoral issues that are linked to foreign interference through information manipulation on social media[360].

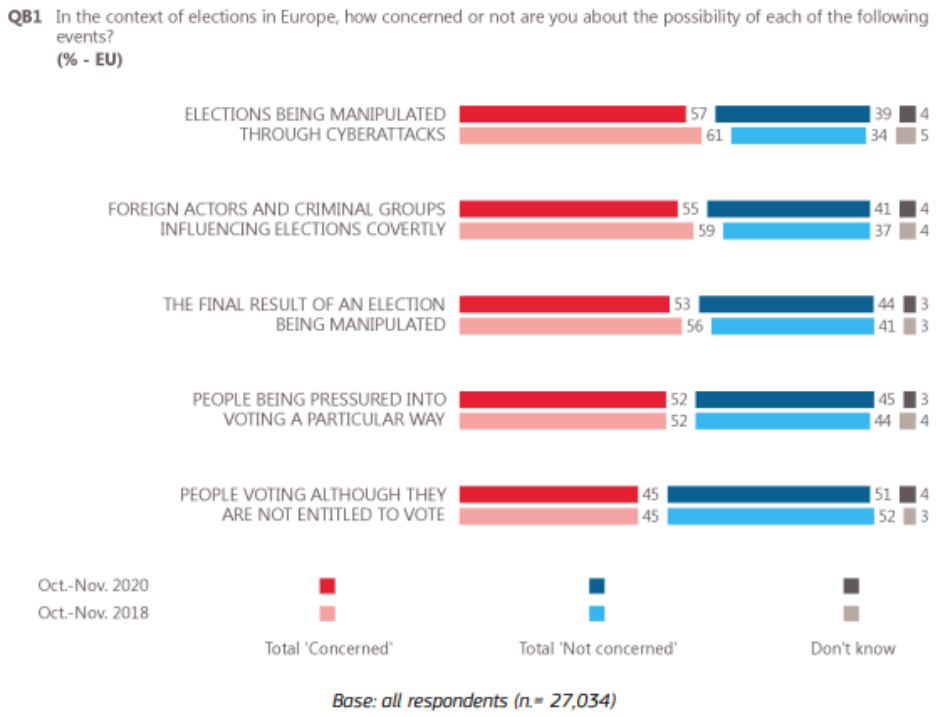

Figure 21: Europeans concerned about particular events in elections. "Democracy in the EU - Eurobarometer Survey 507", *European Commission*, March 2021.

The relative decline between 2018 and 2020 could be an indication that measures applied at the European level are starting to show efficiency, or at least reassuring the population, although some progress is still necessary.

In the U.S., the Pew Research Center found in a study that half of Americans (50%) consider made-up news as a "very big problem in the country today", which is more than those who view violent crime, terrorism, illegal immigration, climate change, racism or sexism that way[361]. If citizens seem to be concerned about the issue of information manipulation on social media and electoral interference, this concern has been shared by international organizations, institutions and states. As soon as 2014, the

[358] Amy Mitchell et al., "Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed" (Pew Research Center, June 5, 2019).
[359] Chavalarias, *Toxic Data*.
[360] European Commission, "Democracy in the EU - Eurobarometer Survey 507" (European Commission, March 2021).
[361] Mitchell et al., "Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed."

World Economic Forum was already warning about the diffusion of false information online as one of the top ten trends to watch as a peril for society[362]. The tone and terms used by Susan Davis, rapporteur of a NATO report on Russian interference in elections, give an idea of the extent of the threat considered by the Alliance: "*threats in the cyber and information space are becoming absolutely critical*", "*it requires responses at every level, in all forums and through every channel*". From NATO to the EU to the U.S. and France individually, the threat of election interference through information manipulation operations on social media is today acknowledged as an important threat. And still, according to Duncan B. Hollis and Jens D. Ohlin, "*election interference has received insufficient scrutiny, despite almost universal recognition of its significance*"[363].

b. A widespread phenomenon that is not fading

The extent of the threat can be understood by its reach today, and its potential developments in the future. The U.S. and France are not isolated cases; the Oxford Internet Institute found that 81 countries were using social media as a way to spread disinformation and so-called "computational propaganda" in 2020, compared to 70 in the previous year[364]. They find that, a large number of countries have at least a low cyber troop capacity (*i.e.* they are active only in periods of elections), but that many countries have a high cyber troop capacity, meaning that they invest significant resources in staff, research, techniques to shape information digital space, at the domestic and international level. These countries are: Australia, China, Egypt, India, Iran, Iraq, Israel, Myanmar, Pakistan, Philippines, Russia, Saudi Arabia, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela, and Vietnam. While the terms of psychological operations and information warfare are large and can encompass other aspects than information manipulation operations on social media, we can still see that these tools are being used by a large number of actors, including democratic states, and remain open to any country that wishes to dedicate the associate means. The numbers of political bots on social media, acting worldwide, as we mentioned previously, is also a sign of the phenomenon's scale and despite all the take-downs by social media companies, automated accounts continue to proliferate, and disrupt the political debate.

Finally, we believe that information manipulation on social media requires specific attention, due to its constantly evolving aspect, and to the potential of social media to take more and more importance in our everyday lives. If we saw that social media is not used by the whole population, it is mainly used by young people. We would argue that social media's use is not a phenomenon of age, but more of generation. We can imagine that today's individuals that are born with social media will be more at

[362] "Top 10 Trends of 2014: 10. The Rapid Spread of Misinformation Online."
[363] Ohlin and Hollis, *Defending Democracies*.
[364] Samantha Bradshaw, Philip N Howard, and Hannah Bailey, "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation," Programme on Democracy & Technology (Oxford Internet Institute - University of Oxford, 2021).

ease with these online platforms and likely to use them later, than people who saw them emerging at an older age, just like it was the case with televisions or cell-phones.

The use of social media among young people is changing particularly quickly, but if they tend to change from one platform to another, their use of social media has not decreased. Today, almost half of the American teens say they are almost constantly using the Internet (46%), and only 3% do not use it daily[365].

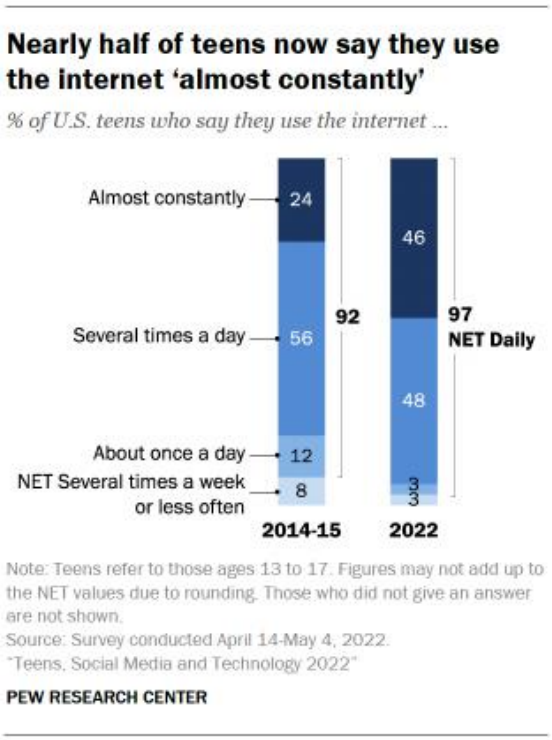

Figure 22: Use of Internet by U.S. teens. "Teens, Social Media and Technology 2022", *Pew Research Center*, 2022.

Another aspect that would corroborate this hypothesis is the fact that few people delete their social media accounts, while more and more accounts are being created. Although social media platforms that are the most "trendy" might evolve (Facebook or Twitter being replaced by other platforms), we believe that the social media environment is not ready to disappear from our daily lives.

[365] Emily a Vogels, Risa Gelles-Watnick, and Navid Massarat, "Teens, Social Media and Technology 2022" (Pew Research Center: Internet, Science & Tech, August 10, 2022).

CONCLUSION

Social media represent a backdoor for foreign interference in elections. Our first hypothesis was that social media's characteristics and vulnerabilities are used by foreign actors as new tools to interfere in elections and favor one candidate. Throughout this research, our hypothesis is partially corroborated, since we indeed found that foreign actors can weigh in the political debate and favor one candidate over another. However, we saw that the main consequence of these operations is not primarily that one candidate might be elected in lieu of another, but rather that they disrupt the democratic electoral process, leading to an erosion of trust in political institutions, elected representatives and the media. If the U.S. and France have faced similar campaigns of interference in their 2016 and 2017 presidential elections, through social media, including hack-and-leak operations and disinformation campaigns, the scale of the operations differed, as well as the states' response. The U.S. faced a more developed and pugnacious campaign, considered as relatively successful, whereas for France, the operation was considered a failure and less elaborated. Mainly due to the scale of the attack, the U.S. and France had different responses, with the U.S. attributing this attack to Russia after thorough investigations while France was said to respond by more covert diplomatic means, only evocating the possibility of a Russian-related campaign. Since 2016, countries and international organizations and institutions have shown the will to take this threat seriously and build more resilient societies to election interference through social media. From regulation, to education and cooperation, various significant measures have been undertaken. However, they should still be constantly reviewed and improved, in light of this rapidly evolving, multifaceted threat. In this respect, our research has permitted a better understanding of two important operations of election interference through social media, underlying similarities and differences both in the tools employed and in the response to these operations. Keeping in mind the necessity to adopt a multidisciplinary approach when tackling this topic has allowed us to present interconnected issues and solutions, sometimes lacking in the present literature. This research has therefore tried to bring insights for an assessment of the threat in two diverse but similar countries, and potential recommendations to tackle the issue at multiple levels. However, for material purposes the research focused on 2016 and 2017 elections, while more recent elections that took place in the U.S. and France might bring further details on the countermeasures' efficiency and the evolution of the threat. Presidential elections in 2020 in the U.S. and 2022 in France, have shown that this threat is still a source of concern in our societies, although occurring under different forms. While for France, it is still too soon to know precisely whether information manipulation operations to interfere in the elections occurred on social media or not, the measures implemented by the governments and social media seem to have helped counter or dissuaded foreign actors from interfering, at least at a large scale. In the U.S. information manipulation regarding the elections have indeed happened, but interestingly, the threat seemed to come first and foremost from within the

country, with alt-right individuals contesting the legitimacy of the election. Therefore, it is crucial to remain persistently vigilant and keep analyzing potential evolutions of this threat, while sharing this knowledge to the population and decision-makers for a whole-of-society response. Going beyond the U.S. and France, we also want to highlight the need for further research on non-Western liberal democracies, where social media companies have not undertaken the same efforts of auto-regulation. Some scholars have carried out valuable works on this issue in Asian or African countries[366], but research remains scarce and more international forums should be held regularly for discussing and developing common solutions.

[366] See the works of Maxime Audinet regarding Russian influence operations in African countries, and Paul Charon regarding Chinese influence operations around the globe and in Asia.

BIBLIOGRAPHY:

Federal Bureau of Investigation. "2016 Election Interference. Most Wanted - Counterintelligence." Accessed September 19, 2022. https://www.fbi.gov/wanted/counterintelligence/2016-election-interference.

Aaltola, Mika. "Democracy's Eleventh Hour: Safeguarding Democratic Elections against Cyber-Enabled Autocratic Meddling." *The Finnish Institute of International Affairs*, FIIA Briefing Papers, November 2017.

"Action Plan Against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions." Brussels: European Commission, December 5, 2018.

Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31, no. 2 (May 2017).

Amoros, Raul. "Who Is More Powerful – Countries or Companies?" HowMuch, July 11, 2019.

Annan, Kofi, Laura Chinchilla, Yves Leterne, Stephen Stedman, Noeleen Heyzer, Toomas Hendrik Ilves, Ory Okolloh, et al. "Protecting Electoral Integrity in the Digital Age." Kofi Annan Commission on Elections and Democracy in the Digital Age, January 2020.

Aral, Sinan, Soroush Vosoughi, and Deb Roy. "The Spread of True and False News Online." *Science, with Massachusetts Institute of Technology*, March 9, 2018.

Arnaudo, Daniel, Samantha Bradshaw, Hui Hui Ooi, Kaleigh Schwalbe, Amy Studdart, Vera Zakem, and Amanda Zink. "Combating Information Manipulation: A Playbook for Elections and Beyond." International Republican Institute, National Democratic Institute, Stanford Internet Observatory, September 28, 2021.

Article L52-1 - Code électoral. Loi en vigueur depuis le 20 avril 2011.

Audinet, Maxime. "RT, pièce maîtresse de la stratégie d'influence russe." *Le Monde diplomatique*, April 1, 2017.

Balzacq, Thierry, and Myriam Dunn Cavelty. *Routledge Handbook of Security Studies*. 2nd ed. Routledge Handbooks. Routledge, 2016.

Barela, Steven, and Jérôme Duberry. "Understanding Disinformation Operations in the Twenty-First Century." In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, 41–72, 2021.

Bargar, A., S. Pitts, J. Butkevics, and I. McCulloh. "Challenges and Opportunities to Counter Information Operations Through Social Network Analysis and Theory," Vol. 2019-May, 2019.

Barthel, Michael, Amy Mitchell, and Jesse Holcomb. "Many Americans Believe Fake News Is Sowing Confusion." Pew Research Center, December 15, 2016.

Beam, Michael, Paul Haridakis, Myiah Hutchens, and Jay Hmielowski. "Social Media, News Platforms, and Partisan Exposure: Discourse, Disruption, and Digital Democracy in the 2016 Presidential Election." In *The Presidency and Social Media*, edited by Dan Schill and John Allen Hendricks, 37–55. Routledge, 2017.

Bennett, W. Lance, and Steven Livingston. *The Disinformation Age*. Cambridge University Press. Cambridge University Press, 2020.

Bentzen, Naja. "Foreign Interference in Democracies. Understanding the Threat, and Evolving Responses." European Parliamentary Research Service, September 2020.

Berzina, Kristine, and Etienne Soula. "Conceptualizing Foreign Interference in Europe." *Alliance for Securing Democracy*, March 18, 2020, 14.

Bessi, Alessandro, and Emilio Ferrara. "Social Bots Distort the 2016 US Presidential Election Online Discussion." *First Monday*, November 7, 2016.

Beykpour, Kayvon, and Vijaya Gadde. "Additional Steps We're Taking Ahead of the 2020 US Election." *Twitter Blog* (blog), October 9, 2020.

Blake, Aaron. “A New Study Suggests Fake News Might Have Won Donald Trump the 2016 Election.” *Washington Post*, April 3, 2018.
Boot, Max, Jeane J. Kirkpatrick, and Max Bergmann. “Defending America From Foreign Election Interference.” Council on Foreign Relations, March 6, 2019.
Borry-Estrade, Elisa. “Elections françaises 2022 : une série d’initiatives dédiées sur Facebook, Instagram et WhatsApp pour aider les citoyens à lire et à décrypter l’information en ligne.” *À propos de Meta* (blog), February 16, 2022.
Boulanger, Philippe. *Géopolitique des médias*. Armand Colin, 2014.
Boulanger, Philippe. *Planète médias. Géopolitique des réseaux et de l’influence*, 2021.
Bovet, Alexandre, and Hernán A. Makse. “Influence of Fake News in Twitter during the 2016 US Presidential Election.” *Nature Communications* 10, no. 1 (January 2, 2019).
Boxell, Levi, Matthew Gentzkow, and Jesse M. Shapiro. “Cross-Country Trends in Affective Polarization.” Stanford University, November 2021.
Bradshaw, S., and P. Howard. “Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation” 2017.12 (2017).
Bradshaw, Samantha, and Philip N. Howard. “The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.” Programme on Democracy & Technology. Oxford Internet Institute - University of Oxford, September 26, 2019.
Bradshaw, Samantha, Philip N Howard, and Hannah Bailey. “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation.” Programme on Democracy & Technology. Oxford Internet Institute - University of Oxford, 2021.
Bronner, Gérald. “Les lumières à l’ère numérique.” Rapport officiel de la Commission. Présidence de la République, January 2022.
Bruns, Axel. “Making Sense of Society Through Social Media.” *Social Media + Society* 1, no. 1 (April 1, 2015).
Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. 1st edition. Cambridge, Massachusetts London, England: Harvard University Press, 2020.
Bulckaert, Ninon. “Comment la France a contré l’ingérence russe dans la campagne présidentielle.” *www.euractiv.fr*, July 16, 2018.
Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2003.
Caulfield, T., J.M. Spring, and M. Angela Sasse. “Why Jenny Can’t Figure out Which of These Messages Is a Covert Information Operation,” 118–28, 2019.
Ceron, Andrea, Luigi Curini, and Stefano Maria Iacus. *Politics and Big Data: Nowcasting and Forecasting Elections with Social Media*. London; New York, NY: Routledge, 2017.
Chadwick, Andrew. *The Hybrid Media System: Politics and Power*. Oxford University Press. Oxford Studies in Digital Politics. Oxford; New York, 2013.
Chadwick, Andrew, James Dennis, and Amy Smith. “Politics in the Age of Hybrid Media.” In *The Routledge Companion to Social Media and Politics*, 7–22, 2015.
Chappell, Bill. “Obama: Cyberspace Is The New ‘Wild West.’” *NPR*, February 13, 2015.
Charillon, Frédéric. *La France dans le monde*. Paris: Cnrs, 2021.
Charon, Paul, and Jean-Baptiste Jeangène Vilmer. “Chinese Influence Operations: A Machiavellian Moment.” IRSEM - Institute for Strategic Research of the French Ministry for the Armed Forces, October 2021.
Chavalarias, David. *Toxic Data: Comment les réseaux manipulent nos opinions*. Illustrated édition. Paris: Flammarion, 2022.
Christensen, Christian, Axel Bruns, Gunn Enli, Eli Skogerbø, and Anders Olof Larsson. *The Routledge Companion to Social Media and Politics*. Routledge Handbooks. London ; New-York: Routledge, 2015.

CI, J. “L’équipe de Macron persuadée d’une ingérence russe dans sa campagne.” *Le Parisien*, February 13, 2017.

Ciampaglia, Giovanni Luca, and Filippo Menczer. “These Are the Three Types of Bias That Explain All the Fake News, Pseudoscience, and Other Junk in Your News Feed.” *Nieman Lab*, June 20, 2018.

Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest. “Combating Foreign Disinformation on Social Media: Study Overview and Conclusions.” RAND Corporation, July 19, 2021.

United States Cyber Command. “Command History.” Accessed August 12, 2022. https://www.cybercom.mil/About/History/.

vie-publique.fr. “Comment est financée la campagne électorale de l’élection présidentielle ? ,” September 13, 2021. https://www.vie-publique.fr/fiches/19431-election-presidentielle-comment-est-financee-la-campagne-electorale.

“Commission de la défense nationale et des forces armées. Audition, à huis clos, de M. Laurent Nuñez, coordonnateur national du renseignement et de la lutte contre le terrorisme.,” fevrier 2021.

“Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions.” Brussels: Council of the European Union, December 10, 2019.

Conley, Heather A., and Jean-Baptiste Jeangène Vilmer. “Successfully Countering Russian Electoral Interference.” CSIS Briefs. Center for Strategic and International Studies, June 21, 2018.

Federal Election Commission. “Contribution Limits.” Accessed August 18, 2022. https://www.fec.gov/help-candidates-and-committees/candidate-taking-receipts/contribution-limits/.

Federal Bureau of Investigation. “Counterintelligence - Combating Foreign Influence.” FBI. Accessed September 6, 2022. https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

Couzigou, Irène. “The French Legislation against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression.” *Election Law Journal: Rules, Politics, and Policy* 20, no. 1 (2021).

Culloty, Eileen, and Jane Suiter. *Disinformation and Manipulation in Digital Media: Information Pathologies*. Routledge Focus. Routledge, 2021.

Courrier international. “Cybersécurité. Un lanceur d’alerte dénonce les failles de sécurité ‘flagrantes’ de Twitter,” August 24, 2022.

“Cyberspace: Definition and Implications - ProQuest.” Accessed April 8, 2022. https://www.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?cbl=396500&pq-origsite=gscholar&parentSessionId=5wgRryh3kwigIOGbn6tFchN0P1746XS8BTNSJ6xkbmc%3D.

Czosseck, Christian. “Conference on Cyber Conflict, Proceedings 2010.” Talinn, Estonia, June 2010.

Domo. “Data Never Sleeps 9.0,” 2021. https://www.domo.com/learn/infographic/data-never-sleeps-9.

Davis, Susan. “Russian Meddling in Elections and Referenda in the Alliance.” Science and Technology Committee. USA: NATO Parliamentary Assembly, November 18, 2018.

Légifrance. “Décret N° 2021-922 Du 13 Juillet 2021 Portant Création, Auprès Du Secrétaire Général de La Défense et de La Sécurité Nationale, d’un Service à Compétence Nationale Dénommé « service de Vigilance et de Protection Contre Les Ingérences Numériques Étrangères ».” Accessed June 9, 2022.

Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d’un traitement automatisé de données à caractère personnel dans le but d’identifier les ingérences numériques étrangères, 2021-1587 § (2021).

Décret n°2001-213 du 8 mars 2001 portant application de la loi n° 62-1292 du 6 novembre 1962 relative à l’élection du Président de la République au suffrage universel, 2001-213 § (2001).

Deibert, Ronald J. “Cyber-Security.” In *Routledge Handbook of Security Studies, Thierry Balzacq &*, by Myriam Dunn Cavelty and Thierry Balzacq, 2nd ed. Routledge, 2016.

Deibert, Ronald J. “The Road to Digital Unfreedom: Three Painful Truths About Social Media.” *Journal of Democracy* 30, no. 1 (January 2019).

Deibert, Ronald J. “Trajectories for Future Cybersecurity Research.” In *The Oxford Handbook of International Security*, edited by Alexandra Gheciu and William C. Wohlforth, 2018.

Dewey, Caitlin. “Facebook Fake-News Writer: ‘I Think Donald Trump Is in the White House Because of Me.’” *Washington Post*, November 17, 2016.
Dews, Fred, and Darrell M. West. “Protecting American Elections from Foreign Interference.” Brookings Cafeteria Podcasts. Accessed August 14, 2022.
Diakopoulos, Nicholas, and Michael Koliska. “Algorithmic Transparency in the News Media.” *Digital Journalism* 5, no. 7 (August 9, 2017).
Diaz Crego, Maria. “Towards New Rules on Transparency and Targeting of Political Advertising.” European Parliamentary ResearchService, July 2022.
Directorate-General for Communications Networks, Content and Technology. “A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation.” European Commission, 2018.
DiResta, Renee, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, and Ben Johnson. “The Tactics & Tropes of the Internet Research Agency.” *U.S. Senate Documents*, October 1, 2019.
Dorell, Oren. “State Department’s Answer to Russian Meddling Is about to Be Funded.” *USA Today*, February 13, 2018.
Douek, Evelyn. “The Free Speech Blind Spot: Foreign Election Interference on Social Media.” In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, edited by Jens David Ohlin and Duncan B. Hollis. Ethics National Security Rule Law Series. New York: Oxford University Press, 2021.
Douzet, Frédérick. “Understanding Cyberspace with Geopolitics.” *Hérodote* 152–153, no. 1–2 (2014).
Dumbrava, Costica. “Key Social Media Risks to Democracy: Risks from Surveillance, Personalisation, Disinformation, Moderation and Microtargeting.” Brussels: European Parliamentary Research Service, December 2021.
Dunn Cavelty, Myriam. “Securing the Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory.” In *International Relations and Security in the Digital Age*, 85–105, 2007.
Dunn Cavelty, Myriam, and Florian J Egloff. “The Politics of Cybersecurity: Balancing Different Roles of the State.” *St Antony’s International Review*, 2019.
Durakoglu, Naz. “Hashtag Campaign: #MacronLeaks.” *DFR Lab - Atlantic Council*, May 8, 2017.
Eichensehr, K.E. “Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election.” *American Journal of International Law* 115, no. 2 (2021).
Cybersecurity and Infrastructure Security Agency. “Election Infrastructure Security.” Accessed September 7, 2022. https://www.cisa.gov/election-security.
Epstein, Ben. “Why It Is So Difficult to Regulate Disinformation Online.” In *The Disinformation Age*, edited by W. Lance Bennett and Steven Livingston, Cambridge University Press, 2020.
Eriksson, Johan, and Giampiero Giacomello. *International Relations and Security in the Digital Age*. Routledge Advances in International Relations and Globl Politics. Routledge, 2007.
“Establishment of the Bureau of Cyberspace and Digital Policy (Press Release).” U.S. Department of State - Office of the Spokesperson, April 4, 2022.
European Commission. “2022 Strengthened Code of Practice on Disinformation,” June 16, 2022.
European Commission. “Democracy in the EU - Eurobarometer Survey 507.” European Commission, March 2021.
European Commission. Securing free and fair European elections: A Contribution from the European Commission to the Leaders’ meeting in Salzburg on 19-20 September 2018 (2018).
“European Parliament Resolution of 9 March 2022 on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation (2020/2268(INI)).” European Parliament, March 9, 2022.

U.S. House of Representatives Permanent Select Committee on Intelligence. “Exposing Russia’s Effort to Sow Discord Online: The Internet Research Agency and Advertisements,” May 2018.
“Facebook: From Election to Insurrection. How Facebook Failed Voters and Nearly Set Democracy Aflame.” Avaaz, March 18, 2021.
Farinella, Rose-Marie, and Estelle Warin. *Stop à La Manipulation : Comprendre l’info, Décrypter Les Fake-News*. Bayard Jeunesse, 2021.
Feingold, Spencer. “Four Key Ways Disinformation Is Spread Online.” World Economic Forum, August 9, 2022.
Ferrand, Richard. “« Ne laissons pas la Russie déstabiliser la présidentielle en France ! ».” *Le Monde.fr*, February 14, 2017.
Fisher, Max, and Katrin Bennhold. “As Germans Seek News, YouTube Delivers Far-Right Tirades.” *The New York Times*, September 7, 2018.
Fletcher, Tom. *The Naked Diplomat: Understanding Power and Politics in the Digital Age*. William Collins, 2016.
Foer, Franklin. “Facebook’s War on Free Will.” *The Guardian*, September 19, 2017.
Fournas, Marie de. “Présidentielle: 14 fake news qui circulent sur Emmanuel Macron.” *20minutes*, April 28, 2017.
Intelligence Online. “France: Viginum and DGSI Consider Partnering with Defence-Backed Startups to Fight Fake News,” December 13, 2021.
“Frances Haugen Testimony before the United States Senate Committee on Commerce, Science and Transportation.” U.S. Senate, October 4, 2021.
Fried, Daniel, and Alina Polyakova. “Democratic Defense against Disinformation.” Atlantic Council, March 5, 2018.
Fried, Daniel, and Alina Polyakova. “Democratic Defense against Disinformation 2.0.” Atlantic Council, June 13, 2019.
Frizell, Sam. “What Leaked Emails Reveal About Clinton’s Campaign.” *Time*, October 7, 2016.
Fuchs, Christian. *Social Media a Critical Introduction*. London: Sage, 2014.
The World Bank. “GDP (Current US$) - Russian Federation, United States, European Union,” 2021. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2021&locations=RU-US-EU&start=1991.
Gibson, William. *Burning Chrome*. Gollancz, 1982.
Giles, Keir. “The Next Phase of Russian Information Warfare.” *NATO Strategic Communications Centre of Excellence*, May 20, 2016.
Greathouse, Craig B. “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” In *Cyberspace and International Relations*, by Alexandra Gheciu and William C. Wohlforth. Oxford University Press, 2018.
Greenberg, Andy. “Hackers Hit Macron With Huge Email Leak Ahead of French Election.” *Wired*, May 5, 2017.
Greenberg, Andy. “Here’s The Evidence That Links Russia’s Most Brazen Hacking Efforts.” *Wired*, November 15, 2019.
Greenberg, Andy. “NSA Director Confirms That Russia Really Did Hack the French Election.” *Wired*, May 9, 2017.
U.S. Bureau of Economic Analysis (BEA). “Gross Domestic Product,” 2022. https://www.bea.gov/data/gdp/gross-domestic-product.
Grynszpan, Emmanuel. “Les médias pro-Russes s’engouffrent dans le tout sauf Macron.” *Euractiv*, February 14, 2017.
Guehenno, Jean-Marie. “Livre Blanc Sur La Défense et La Sécurité Nationale.” Rapport officiel. Présidence de la République - Commission du Livre blanc sur la Défense et la Sécurité nationale, April 29, 2013.

Guess, Andrew M., Michael Lerner, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, Jason Reifler, and Neelanjan Sircar. “A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India.” *Proceedings of the National Academy of Sciences* 117, no. 27 (July 7, 2020).
Hacquebord, Feike. “Two Years Of Pawn Storm: Examining An Increasingly Relevant Threat.” Trend Micro, October 17, 2018.
Haltiwanger, John. “Americans Are Already Exhausted with the 2020 Election, and It’s Just Getting Started. Other Countries Have Laws Limiting the Length of Campaigns.” *Business Insider*, February 10, 2020.
Hamre, John. “The ‘Electronic Pearl Harbor.’” *Politico*, September 12, 2015.
Harris, Dan. “Former Employees Expose Inner Workings of Russian Troll Farm.” *ABC News*, November 2, 2017.
Harvey, Kerric, ed. *Encyclopedia of Social Media and Politics*. 1st edition. Los Angeles: SAGE Publications, Inc, 2014.
Hearn, Kay, Patricia Williams, and Rachel Mahncke. “International Relations and Cyber Attacks: Official and Unofficial Discourse.” *Australian Information Warfare and Security Conference*, March 11, 2012.
Helmus, Todd C., James V. Marrone, Marek N. Posard, and Danielle Schlang. “Russian Propaganda Hits Its Mark: Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions.” RAND Corporation, October 15, 2020.
Hénin, Nicolas. “What Did Disinformation Look like during the 2022 French Presidential Election? An Overview Based on Fact-Checking Articles.” *EU DisinfoLab* (blog), June 28, 2022.
High Representative of the Union for Foreign Affairs and Security Policy. “Mapping of Measures Related to Enhancing Resilience and Countering Hybrid Threats - Joint Staff Working Document.” Brussels: European Commission, July 24, 2020.
Hivert, Anne-Françoise. “En Finlande, la riposte des démocraties s’organise face aux menaces hybrides.” *Le Monde*, June 4, 2022.
Hollis, Duncan. “A Brief Primer on International Law and Cyberspace.” *Carnegie Endowment for International Peace*, June 2021.
Horncastle, William C. R. “The Scale of US Election Spending Explained in Five Graphs.” *The Conversation*, October 15, 2020.
Hughes, Rex. “A Treaty for Cyberspace.” *Oxford University Press on Behalf of the Royal Institute of International Affairs*, International Affairs, 86, no. 2 (March 2010).
Huyghe, François-Bernard. “Cyberespace.” *Inflexions* 43, no. 1 (January 16, 2020).
Huyghe, François-Bernard. *Fake News: La Grande Peur*. VA Editions., 2019.
Huyghe, François-Bernard. “Que changent les fake news ?” *Revue internationale et strategique* 110, no. 2 (June 29, 2018): 79–87.
INGE Special Committee. “Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation.” European Parliament, February 8, 2022.
Iosifidis, Petros, and Nicholas Nicoli. *Digital Democracy, Social Media and Disinformation*. London: Routledge, 2020.
Jeangène Vilmer, Jean-Baptiste. Comment l’UE peut-elle remporter la “bataille des récits”? Institut Open Diplomacy, June 24, 2022.
Jeangène Vilmer, Jean-Baptiste. “Information Defense: Policy Measures Taken against Foreign Information Manipulation.” Atlantic Council, July 22, 2021.
Jeangène Vilmer, Jean-Baptiste. “The ‘Macron Leaks’ Operation: A Post-Mortem.” *Atlantic Council*, June 2019, 58.
Jeangène Vilmer, Jean-Baptiste, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera. “Information Manipulation: A Challenge for Our Democracies.” Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, August 2018.

Joint Framework on countering hybrid threats a European Union response (2016).
Jopling, Lord. “Parades Aux Menaces Hybrides Émanant de La Russie : Une Mise à Jour.” Commission sur la Dimension Civile de la Sécurité (CDS) - Assemblée Parlementaire de l’OTAN, September 28, 2018.
Julienne, Marc, and Sophie Hanck. “Diplomatie chinoise : de l’« esprit combattant » au « loup guerrier »:” *Politique étrangère* Printemps, no. 1 (February 15, 2021).
Keating, William R. (Chairman) “Russian Disinformation Attacks on Elections: Lessons from Europe.” Open hearing of the Committee on Foreign Affairs. Washington D.C., July 16, 2019.
Kemp, Simon. “The Global State of Digital in July 2022.” DataReportal, We are social, Hootsuite, July 21, 2022.
King, Gary, Jennifer Pan, and Margaret E. Roberts. “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument.” *American Political Science Review* 111, no. 3 (August 2017).
Kollanyi, Bence, Philip N. Howard, and Samuel C. Woolley. “Bots and Automation over Twitter during the U.S. Election.” Oxford, UK: Project on Computational Propaganda, November 17, 2016.
Kremer, Jan-Frederik, and Benedikt Müller. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer, 2016.
The Moscow Times. “Kremlin Troll Factory’s Methods and Figures Revealed,” October 17, 2017, sec. news.
Kreps, Sarah. *Social Media and International Relations*. Cambridge Elements in International Relations. Cambridge New York Port Melbourne New Delhi Singapore: Cambridge University Press, 2020.
Kreps, Sarah. “The Role of Technology in Online Misinformation.” *Foreign Policy - Brookings*, June 2020.
Kurowska, Xymena, and Anatoly Reshetnikov. “Russia’s Trolling Complex at Home and Abroad.” In *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, edited by N. Popescu and S. Secrieru. Chaillot Papers. EU Institute for Security Studies, 2018.
Lamond, James, and Jeremy Venook. “Blunting Foreign Interference Efforts by Learning the Lessons of the Past.” Center for American Progress, September 2, 2020.
Lapowsky, Issie. “The State Department’s Fumbled Fight Against Russian Propaganda.” *Wired*, November 22, 2017.
Laurent, Samuel. *J’ai vu naître le monstre. Twitter va-t-il tuer la #démocratie ?* Les Arènes., 2021.
Ministère des Armées. “Le commandement de la cyberdéfense (COMCYBER),” February 14, 2022. https://www.defense.gouv.fr//ema/commandement-cyberdefense-comcyber.
Le Drian, Jean-Yves. Entretien de M. Jean-Yves Le Drian, ministre de l’Europe et des affaires étrangères, avec France 5 le 17 octobre 2021, sur les relations avec la Russie, son ingérence pendant la campagne présidentielle de 2017 et le groupe privé de mercenaires, Wagner. Vie-publique.fr, October 17, 2021.
Lederer, Edith M. “UN Chief Calls for Regulating Social Media Companies.” ABC News. January 29, 2021.
Lequeux, Vincent. “La France dans l’Union européenne.” Touteleurope.eu, March 28, 2022.
Letsch, Constanze. “Social Media and Opposition to Blame for Protests, Says Turkish PM.” *The Guardian*, June 3, 2013.
Levin, Dov H. *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*. New York: Oxford University Press, 2020.
Levin, Dov H. “Should We Worry about Partisan Electoral Interventions? The Nature, History, and Known Effects of Foreign Interference in Elections.” In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, Oxford University Press., 2021.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.
Lilleker, Darren, Karolina Koc-Michalska, Ralph Negrine, Rachel Gibson, Thierry Vedel, and Sylvie Strudel. “Social Media Campaigning in Europe: Mapping the Terrain.” *Journal of Information Technology and Politics* 14, no. 4 (2018).

Limonier, Kévin, and Maxime Audinet. “La stratégie d’influence informationnelle et numérique de la Russie en Europe.” *Herodote* 164, no. 1 (May 10, 2017).
Lin, Herbert. “Conclusion: An Outsider Looks In.” In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, edited by Jens David Ohlin and Duncan B. Hollis. Ethics National Security Rule Law Series. New York: Oxford University Press, 2021.
Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information, Pub. L. No. n° 2018-1201 (2018).
Lu, Christina. “China’s Social Media Explosion.” *Foreign Policy*, November 11, 2021.
Arcom. “Lutte contre la manipulation de l’information : déclarations des opérateurs de plateformes en ligne et questionnaires de l’Arcom.” Accessed September 12, 2022. https://www.arcom.fr/vos-services-par-media/internet-et-reseaux-sociaux/lutte-contre-la-manipulation-de-linformation-declarations-des-operateurs-de-plateformes-en-ligne-et-questionnaires-de-larcom.
Luttrell, Regina, Jon Glass, and Lu Xiao. *Democracy in the Disinformation Age: Influence and Activism in American Politics*. Routledge., 2021.
MacIntosh, Duncan. “Protecting Democracy by Commingling Polities: The Case for Accepting Foreign Influence and Interference in Democratic Processes.” In *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, edited by Jens David Ohlin and Duncan B. Hollis. Ethics National Security Rule Law Series. New York: Oxford University Press, 2021.
Macron, Emmanuel. “Speech by M. Emmanuel Macron, President of the Republic at the Internet Governance Forum.” Internet Governance Forum, November 12, 2018.
“Macronleaks : y a-t-il eu ingérence russe dans l’élection présidentielle française ?” *La question du jour par Guillaume Erner*, December 6, 2019.
Marangé, Céline, and Maud Quessard. *Les guerres de l’information à l’ère numérique*. Paris: PUF, 2021.
McKay, Spencer, and Chris Tenove. “Disinformation as a Threat to Deliberative Democracy.” *Political Research Quarterly* 74, no. 3 (September 1, 2021).
Memoli, Mike, and Kilian Dilanian. “Biden, Citing Briefings, Says Russia Again Working to Interfere with the Election.” *NBC News*, July 18, 2020.
Milmo, Dan. “Russia Blocks Access to Facebook and Twitter.” *The Guardian*, March 4, 2022.
Mitchell, Amy, Jeffrey Gottfried, Galen Stocking, Mason Walker, and Sophia Fedeli. “Many Americans Say Made-Up News Is a Critical Problem That Needs To Be Fixed.” Pew Research Center, June 5, 2019.
Morlino, Leonardo. *Comparison: A Methodological Introduction for the Social Sciences*. Verlag Barbara Budrich, 2018.
Mueller, Robert S. “Report On The Investigation Into Russian Interference In The 2016 Presidential Election.” Washington D.C.: U.S. Department of Justice, March 2019.
Murray, Stephanie. “Putin: I Wanted Trump to Win the Election.” *Politico*, July 16, 2018.
Nast, Condé. “How the Kremlin Infiltrated Russia’s Facebook.” *Wired UK*. Accessed August 19, 2022.
NATO. “NATO Cyber Defence - NATO Factsheets,” August 2020.
NATO StratCom COE, and Singularex. “The Black Market for Social Media Manipulation.” NATO Strategic Communications Centre of Excellence & Singularex, November 2018.
Neuman, Scott. “Biden: McConnell Refused To Sign Bipartisan Statement On Russian Interference.” *NPR*, January 24, 2018, sec. National Security.
Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy, and Rasmus Kleis Nielsen. “Digital News Report 2018.” Reuters Institute for the Study of Journalism, 2018.
Newman, Nic, Richard Fletcher, Craig T. Robertson, Kirsten Eddy, and Rasmus Kleis Nielsen. “Digital News Report 2022.” Reuters Institute for the Study of Journalism, June 2022.
Nikolskaya, Polina, and Christian Lowe. “Putin Hosts French Presidential Contender Le Pen in Kremlin.” *Reuters*, March 24, 2017, sec. Media and Telecoms.
Nimmo, Ben. “#TrollTracker: Russia’s Other Troll Team.” *Digital Forensic Rresearch Lab - Medium*, August 2, 2018.

Nocetti, Julien. “Comment l’information recompose les relations internationales. La faute à Internet ?” In *Ramses 2018. La guerre de l’information aura-t-elle lieu ?*, 138–43. Ramses. Paris: Institut français des relations internationales, 2017.
Nott, Lata. “Political Advertising on Social Media Platforms.” *American Bar Association*, Human Rights Magazine, 45, no. 3 (June 25, 2020).
Nye, Joseph S. “Cyber Power.” *Belfer Center for Science and International Affairs*, May 2010.
Nye, Joseph S. “Protecting Democracy in an Era of Cyber Information War.” *Belfer Center for Science and International Affairs, Harvard Kennedy School*, Paper, February 2019.
Nye, Joseph S. “Soft Power.” *Foreign Policy*, no. 80 (1990).
Nye, Joseph S. “The End of Cyber-Anarchy?” *Foreign Affairs*, February 15, 2022.
Ohlin, Jens David. “A Roadmap for Fighting Election Interference.” *American Journal of International Law* 115 (2021).
Ohlin, Jens David, and Duncan B. Hollis, eds. *Defending Democracies: Combating Foreign Election Interference in a Digital Age*. Ethics National Security Rule Law Series. New York: Oxford University Press, 2021.
“Open Hearings of the Intelligence Committee.” U.S. Senate - Hart 216, November 1, 2017.
Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. “Countering Information Influence Activities: The State of the Art: Research Report.” Lund University, July 1, 2018.
Pariser, Eli. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. London: Penguin Books, 2011.
Parkinson, Hannah Jane. “Click and Elect: How Fake News Helped Donald Trump Win a Real Election.” *The Guardian*, November 14, 2016.
Patterson, Thomas E. “News Coverage of the 2016 General Election: How the Press Failed the Voters.” *Harvard Kennedy School*, Faculty Research Working Paper Series, December 2016.
Paul, Christopher, and Miriam Matthews. “The Russian ‘Firehose of Falsehood’ Propaganda Model.” RAND Corporation, July 11, 2016.
Pavleska, Tanja, Andrej Skolkay, Bissera Zankova, Nelson Ribeiro, and Anja Bechmann. “Performance Analysis of Fact-Checking Organizations and Initiatives in Europe: A Critical Overview of Online Platforms Fighting Fake News.” In *Disinformation and Digital Media as a Challenge for Democracy*, edited by Georgios Terzis, Dariusz Kloza, Elżbieta Kużelewska, and Daniel Trottier, Intersentia., 2018.
Pehlivanoglu, Didem, Tian Lin, Farha Deceus, Amber Heemskerk, Natalie C. Ebner, and Brian S. Cahill. “The Role of Analytical Reasoning and Source Credibility on the Evaluation of Real and Fake Full-Length News Articles.” *Cognitive Research: Principles and Implications* 6, no. 1 (March 31, 2021).
Pétiniaud, Louis, and Kévin Limonier. “Cartographier le cyberespace : le cas des actions informationnelles russes en France.” *Les Champs de Mars* 30, no. 1 (2018).
Pharo, Patrick. *Les data contre la liberté*. Presses Universitaires de France PUF., 2022.
Piore, Adam. “Technologists Are Trying to Fix the ‘Filter Bubble’ Problem That Tech Helped Create.” *MIT Technology Review*, August 22, 2018.
Popescu, N., and S. Secrieru, eds. *Hacks, Leaks and Disruptions: Russian Cyber Strategies*. Chaillot Papers. EU Institute for Security Studies, 2018.
Posard, Marek N., Hilary Reininger, and Todd C. Helmus. “Countering Foreign Interference in U.S. Elections.” RAND Corporation, March 29, 2021.
vie-publique.fr. “Présidentielle 2017 : les comptes de campagne des candidats validés par la CNCCFP,” February 13, 2018. https://www.vie-publique.fr/en-bref/19843-presidentielle-2017-publication-des-comptes-de-campagne.
U.S. Senate Select Committee on Intelligence. “Press Release of Intelligence Committee: Senate Intel Releases Volume 5 of Bipartisan Russia Report,” August 18, 2020.

Prier, Jarred. “Commanding the Trend: Social Media as Information Warfare.” *Strategic Studies Quarterly* 11, no. 4 (2017): 50–85.
French Presidency of the Council of the European Union. “Priorities - French Presidency of the Council of the European Union 2022.” Accessed September 7, 2022.
Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising (2021).
Quénel, Nicolas. “Présidentielle 2022 : comment des Russes veulent pourrir la campagne électorale française.” *Marianne*, March 21, 2022.
Quessard, Maud. *Stratégies d’influence et guerres de l’information : Propagande et diplomatie publique des États-Unis depuis la guerre froide*. Des Amériques. Rennes: Presses universitaires de Rennes, 2020.
Rao, Nirupama. “Diplomacy in the Age of Social Media.” *The Wire*, July 19, 2017.
“Rapport Établi Par La Commission Nationale de Contrôle de La Campagne Électorale En Vue de l’élection Présidentielle (Scrutins Des 23 Avril et 7 Mai 2017).” Commission Nationale de Contrôle de la Campagne Electorale en vue de l’Election Présidentielle (CNCCEP), n.d.
Duke Reporters’ Lab. “Reporters Lab Fact-Checking Category.” Accessed September 8, 2022.
“Rewards for Justice – Reward Offer for Information on Russian Interference in U.S. Elections.” U.S. Department of State - Office of the Spokesperson, July 28, 2022.
Rideout, Victoria, Alanna Peebles, Supreet Mann, and Michael B. Robb. “The Common Sense Census: Media Use by Tweens and Teens, 2021.” Common Sense Media, March 9, 2022.
Ringhand, L.A. “Foreign Election Interference: Comparative Approaches to a Global Challenge.” *Election Law Journal: Rules, Politics, and Policy* 20, no. 1 (2021): 1–9.
Roberts, Rachel. “Russia Targeted Key States with Anti-Clinton Fake News, Trump-Russia Hearings Chairman Reveals.” *The Independent*, March 30, 2017.
Ross, Robert M., David Rand, and Gordon Pennycook. “Beyond ‘Fake News’: Analytic Thinking and the Detection of False and Hyperpartisan News Headlines.” *Judgment and Decision Making* 16, no. 2 (March 2021).
Schafer, Joseph. “The Influence of Information Power Upon the Great Game in Cyberspace: U.S. Wins Over Russian Meddling in the 2018 Elections.” *Military Cyber Affairs* 4, no. 2 (December 2020).
Schill, Dan, and John Allen Hendricks, eds. *The Presidency and Social Media: Discourse, Disruption, and Digital Democracy in the 2016 Presidential Election*. 1st edition. New York, NY: Routledge, 2017.
Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd edition. Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017.
Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Reprint edition. Cambridge; New York: Cambridge University Press, 2013.
Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Reprint edition. New York London: W. W. Norton & Company, 2016.
Shinal, John. “Facebook Shuts down 1 Million Accounts per Day but Can’t Stop All ‘threat Actors,’ Security Chief Says.” *CNBC*, August 24, 2017.
“S.Hrg. 115-683 — Facebook, Social Media Privacy, and the Use and Abuse of Data.” Washington D.C., April 10, 2018.
Singer, Peter W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. Mariner Books., 2018.
Statista. “Number of Social Media Users 2025.” Statista, 2022. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
Summers, Timothy. “How the Russian Government Used Disinformation and Cyber Warfare in 2016 Election – an Ethical Hacker Explains.” *The Conversation*, July 27, 2018.
Svetoka, Sanda. “Social Media as a Tool of Hybrid Warfare.” Riga: NATO Strategic Communications Centre of Excellence, 2016.

Szadkowski, Michaël, and Damien Leloup. “Tout comprendre aux publicités politiques sur les réseaux sociaux.” *Le Monde*, November 6, 2019.
Taylor, Margaret L. “Combating Disinformation and Foreign Interference in Democracies: Lessons from Europe.” *Brookings*, TechTank, July 31, 2019.
Terrasson, Benjamin. “Présidentielle 2022 : comment s’organise sa cybersécurité ?” *Siècle Digital*, October 14, 2021.
“The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections” Senate Select Committee on Intelligence, July 3, 2018. https://www.intelligence.senate.gov/publications/committee-findings-2017-intelligence-community-assessment.
The Social Dilemma. Directed by: Jeff Orlowski, Documentary. Netflix, 2020.
Theviot, Anaïs. “Réseaux sociaux, la force du nombre.” *Les Grands Dossiers*, Sciences Humaines, no. 62 (May 2021).
Timsit, Annabelle. “A Study Compared Finnish and American Students’ Ability to Detect Fake News.” *Quartz*, May 3, 2019.
“Top 10 Trends of 2014: 10. The Rapid Spread of Misinformation Online.” World Economic Forum, 2014.
Trump, Donald J. Executive Order 13848 - Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, Pub. L. No. Executive Order 13848 (2018).
Trump: Twitter Allows Me to Get My Message Out, 2017. https://www.youtube.com/watch?v=hKnv7krVni0.
Tufekci, Zeynep. “Opinion | Facebook’s Surveillance Machine.” *The New York Times*, March 19, 2018.
Twitter Comms [@TwitterComms]. “More Reading – People Open Articles 40% More Often after Seeing the Prompt. More Informed Tweeting – People Opening Articles before RTing Increased by 33%. Some People Didn’t End up RTing after Opening the Article – Which Is Fine! Some Tweets Are Best Left in Drafts.” Tweet. *Twitter*, September 24, 2020. https://twitter.com/TwitterComms/status/1309178716988354561.
Twitter Public Policy. “Update on Twitter’s Review of the 2016 US Election.” *Twitter Blog* (blog), January 31, 2018.
Le Monde. “Twitter reconnaît mais nuance les tentatives russes d’influencer l’élection de 2016,” January 29, 2018.
Twitter Help Center. “Twitter’s Civic Integrity Policy,” October 2021. https://help.twitter.com/en/rules-and-policies/election-integrity-policy.
Tzu, Sun. *The Art Of War*. CreateSpace Independent Publishing Platform, 2014.
UN Open-ended working group on developments. “Final Open-Ended Working Group Report.” United Nations General Assembly, March 10, 2021.
France 24. “Un rapport pointe du doigt l’ingérence russe dans la présidentielle américaine 2020,” March 17, 2021.
United States of America V. Elena Alekseevna Khusyaynova, No. Case No. 1:18-mj-464 (September 28, 2018).
United States of America V. Internet Research Agency LLC, No. Case 1:18-cr-00032-DLF (February 16, 2018).
Untersinger, Martin. “Cyberattaques : la France menace de « mesures de rétorsion » tout Etat qui interférerait dans l’élection.” *Le Monde.fr*, February 15, 2017.
Untersinger, Martin . “Les preuves de l’ingérence russe dans la campagne de Macron en 2017.” *Le Monde.fr*, December 6, 2019.
“Update on Results of Retrospective Review of Russian-Related Election Activity,” January 19, 2019.
U.S. Department of Homeland Security. “Foreign Interference Taxonomy. Mis-, Dis-, and Malinformation Resource Library.” Cybersecurity and Infrastructure Security Agency, July 2018.
U.S. Department of Justice. National Security Strategy (2010).

U.S. Senate Committee on Foreign Relations. “Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security.” Government. Washington D.C.: Congress, January 10, 2018.
U.S. Senate Select Committee on Intelligence. “Assessing Russian Activities and Intentions in Recent US Elections.” Office of the Director of National Intelligence, January 6, 2017.
U.S. Senate Select Committee on Intelligence. “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution.” Office of the Director of National Intelligence, January 6, 2017.
U.S. Senate Select Committee on Intelligence. “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V.” U.S. Senate Select Committee on Intelligence, 2020 2019.
U.S. Strategic Command. “The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities.” U.S. Strategic Command, January 5, 2009. National Security Archive.
Van De Velde, Jacqueline. “The Law of Cyber Interference in Elections.” *Social Science Research Network*, SSRN Scholarly Paper, May 15, 2017.
Varol, Onur, Emilio Ferrara, Clayton Davis, Filippo Menczer, and Alessandro Flammini. “Online Human-Bot Interactions: Detection, Estimation, and Characterization,” March 8, 2017.
Vazquez, Coline. “Pourquoi la loi contre les fake news suscite une levée de boucliers.” *Franceinfo*, June 8, 2018.
Secrétariat général de la défense et de la sécurité nationale. “Viginum, Vigilance et Protection Contre Les Ingérences Numériques Étrangères.” Accessed September 6, 2022. http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/le-service-de-vigilance-et-de-protection-contre-les-ingerences-numeriques-etrangeres-viginum/.
Vigour, Cécile. *La comparaison dans les sciences sociales. Pratiques et méthodes*. Repères. Paris: La Découverte, 2005.
Vogels, Emily a, Risa Gelles-Watnick, and Navid Massarat. “Teens, Social Media and Technology 2022.” Pew Research Center: Internet, Science & Tech, August 10, 2022.
Walker, Mason, and Katerina Eva Matsa. “News Consumption Across Social Media in 2021.” Pew Research Center, September 2021.
Walker, Shawn, Dan Mercea, and Marco Bastos. “The Disinformation Landscape and the Lockdown of Social Platforms.” *Information, Communication & Society* 22 (September 19, 2019): 1531–43.
Wardle, Claire, and Hossein Derakhshan. “Information disorder: Toward an interdisciplinary framework for research and policy making.” Council of Europe, September 27, 2017.
Weedon, Jen, William Nuland, and Alex Stamos. “Information Operations and Facebook.” Facebook Security, 2017.
Wike, Richard, Janell Fetterolf, Shannon Schumacher, and J. j Moncus. “Citizens in Advanced Economies Want Significant Changes to Their Political Systems.” Pew Research Center’s Global Attitudes Project. Pew Research Center, October 21, 2021.
Wilson, Clay. “Information Operations and Cyberwar: Capabilities and Related Policy Issues.” Congressional Research Service, September 14, 2006.
Wohlforth, William C., and Alexandra Gheciu. *The Oxford Handbook of International Security*. *The Oxford Handbook of International Security*. Oxford University Press, 2018.
Wollebæk, Dag, Rune Karlsen, Kari Steen-Johnsen, and Bernard Enjolras. “Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior.” *Social Media + Society* 5 (April 1, 2019).
Woolley, Samuel C., and Philip N. Howard, eds. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford Studies in Digital Politics. New York: Oxford University Press, 2018.

TABLE OF APPENDICES

Appendix 1: Figure 1

Figure 1 :

Figure 23: Rewards for Justice – Reward Offer for Information on Russian Interference in U.S. Elections" (U.S. Department of State - Office of the Spokesperson, July 28, 2022)

Appendix 2: Figure 2

Figure 2:

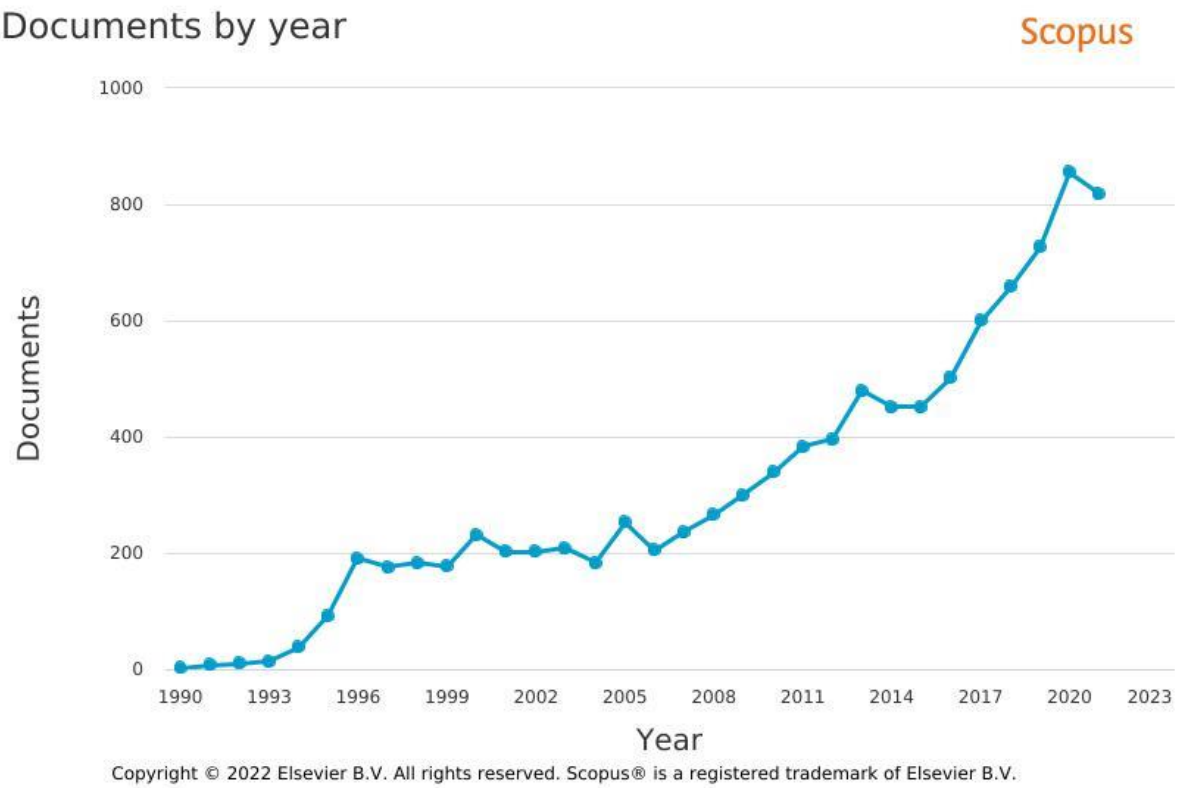

Figure 24: Documents including the term "cyberspace" in their title, abstract or keywords. Scopus data, Elsevier B.V., 2022.

Appendix 3: Figure 3

Figure 3:

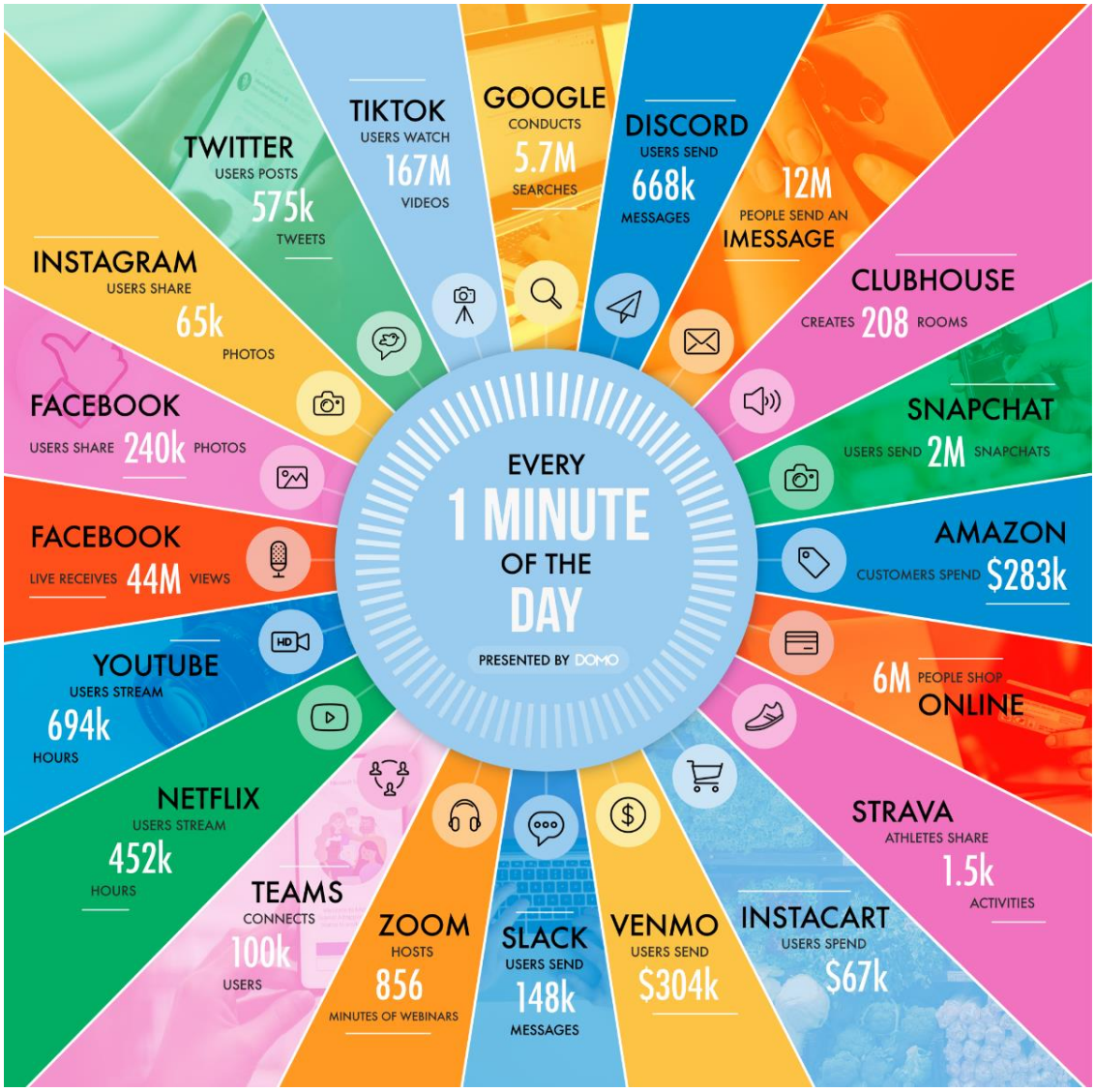

Figure 25: "Data Never Sleeps 9.0". *Domo*. 2021.

Appendix 4: Figure 4

Figure 4:

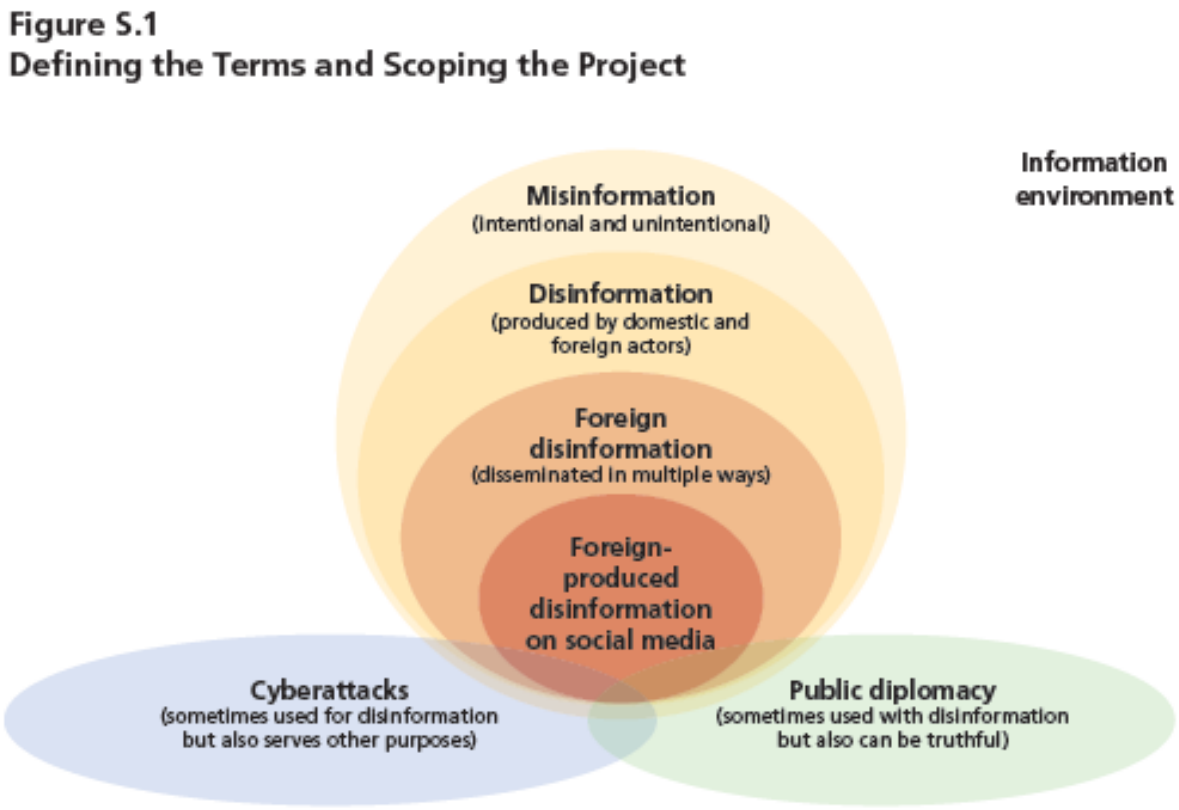

Figure 26: Defining the Terms and Scoping the Project. RAND Corporation. 2021

Appendix 5: Figure 5

Figure 5:

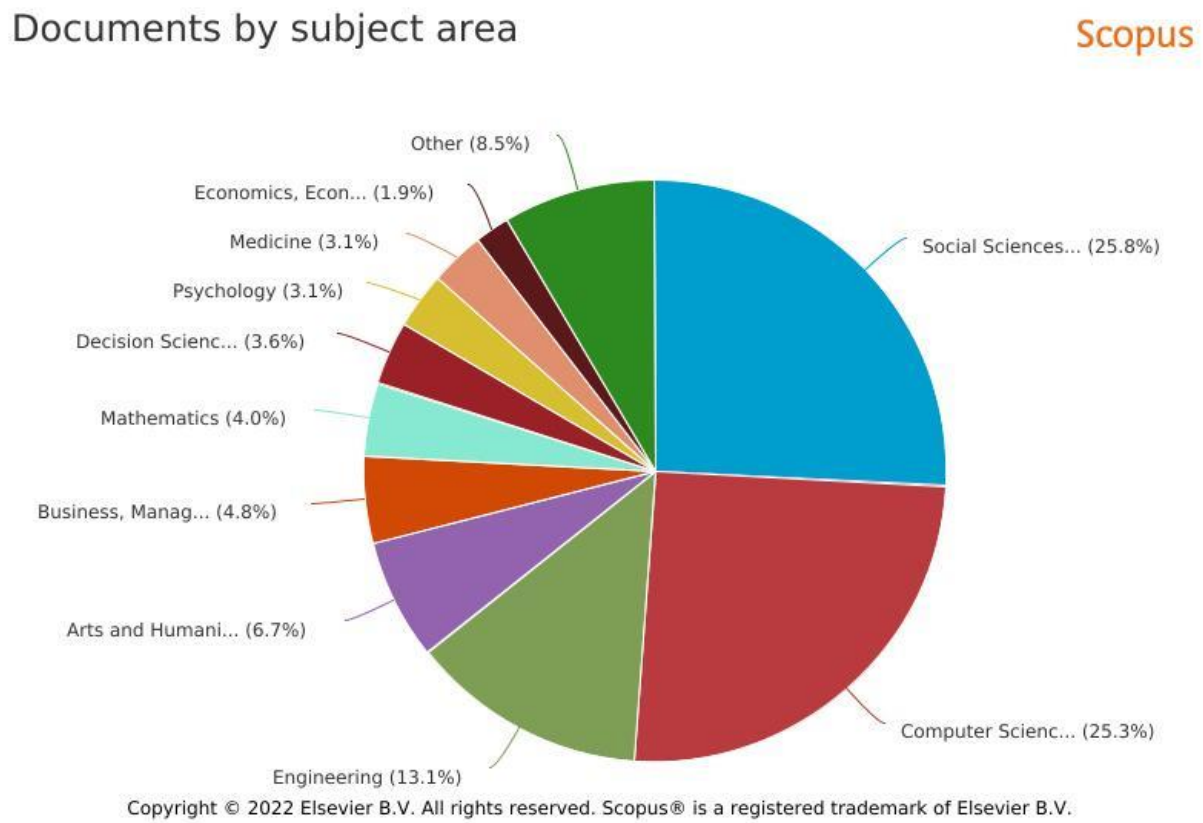

Figure 27: Scopus search on "cyberspace", by subject area. Scopus data, Elsevier B.V., 2022

Appendix 6: Figure 6 and 7

Figure 6 and 7:

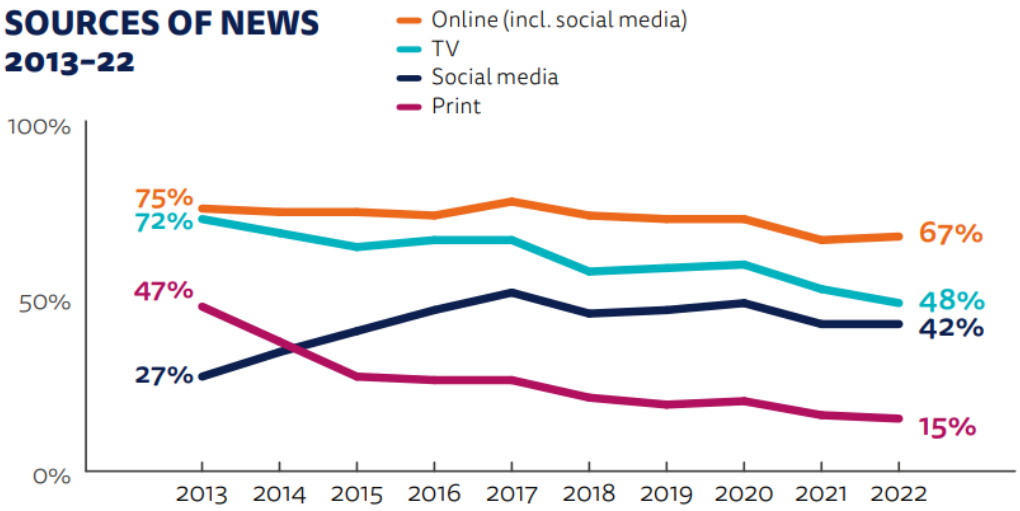

Figure 28: "Sources of news in the United-States (2013-2022)". Digital News Report 2022. *Reuters Institute for the Study of Journalism*. June 2022.

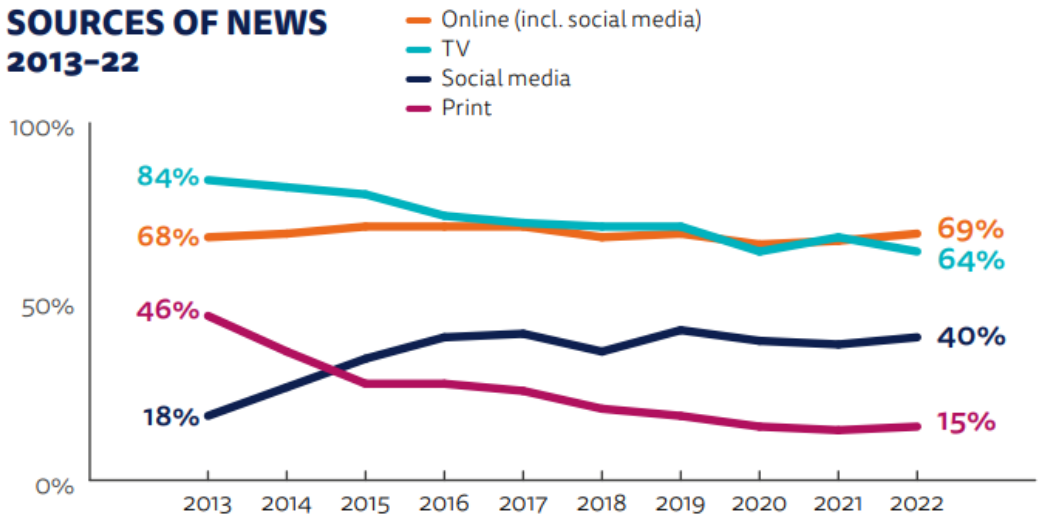

Figure 29: "Sources of news in France (2013-2022)". Digital News Report 2022. *Reuters Institute for the Study of Journalism*. June 2022

Appendix 7: Figure 8

Figure 8:

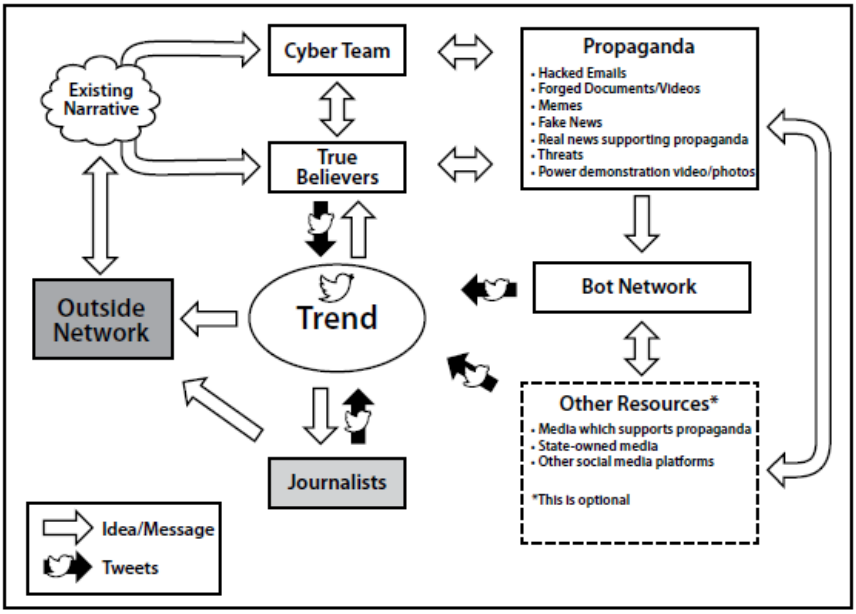

Figure 30: Process map of how propaganda spreads via the trend, Jarred Prier, 2017.

Appendix 8: Figure 9

Figure 9:

Figure 31: IRA-related content on Twitter. Renee DiResta et al., "The Tactics & Tropes of the Internet Research Agency", *U.S. Senate Documents*, 2019.

Appendix 9: Figure 10

Figure 10:

Date	Organization	Phishing Domain
04/01/16	Democratic Party US	myaccount.google.com-changepasswordmyaccount-idx8jxcn4ufdmncudd.gq
04/22/16	CDU	webmail-cdu.de
05/06/16	CDU	support-cdu.de
06/06/16	Democratic Party US	actblues.com
10/20/16	Parliament Montenegro	mail-skupstina.me
03/15/17	Emmanuel Macron campaign	onedrive-en-marche.fr
04/05/17	Konrad Adenauer Stiftung	kasapp.de

Figure 32: Extract from Feike Hacquebord, "Two Years Of Pawn Storm: Examining An Increasingly Relevant Threat", *Trend Micro*, 2018.

Appendix 10: Figure 11

Figure 11:

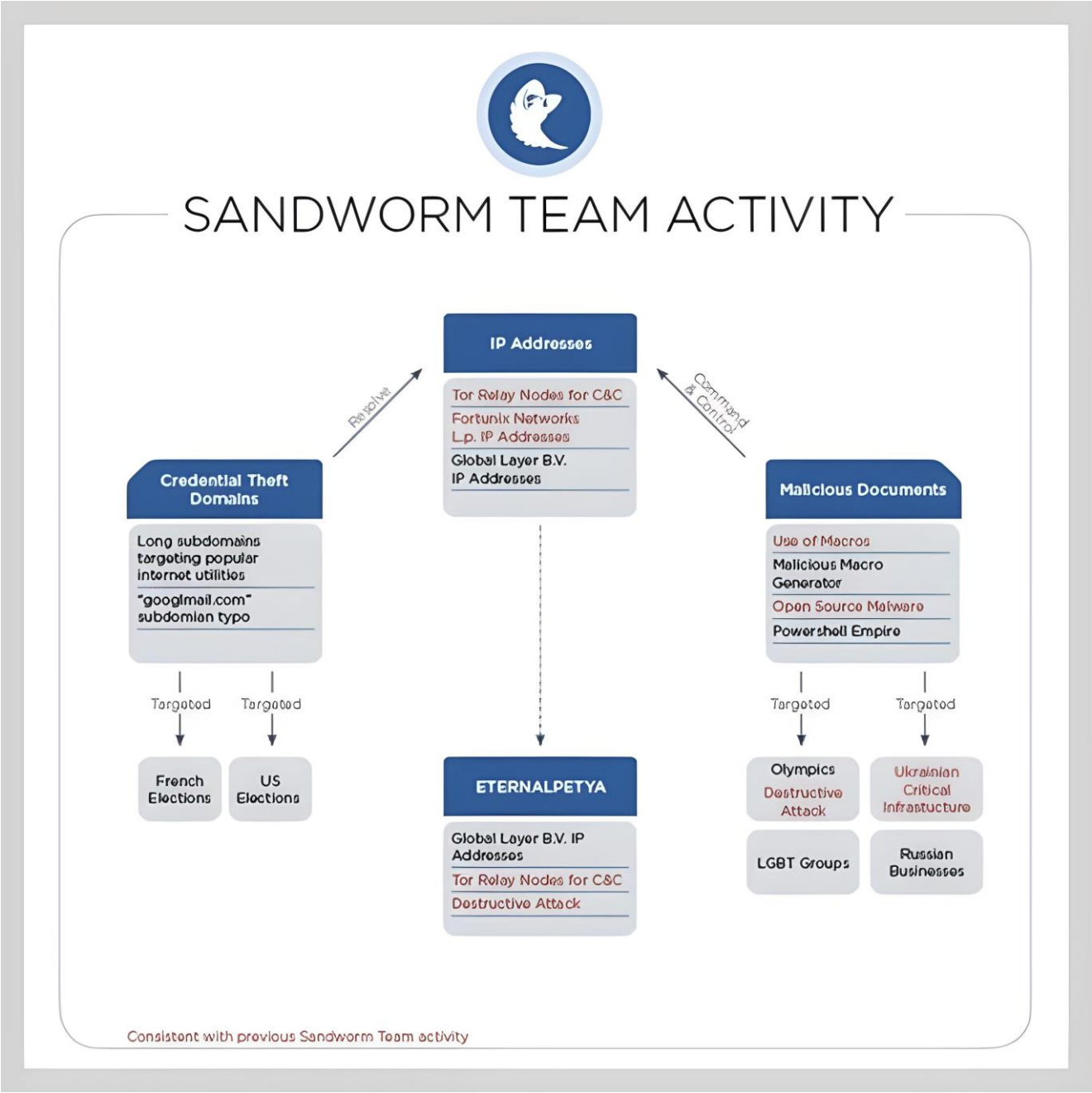

Figure 33: Andy Greenberg, "Here's The Evidence That Links Russia's Most Brazen Hacking Efforts," *Wired*, November 15, 2019.

Appendix 11: Figure 12

Figure 12:

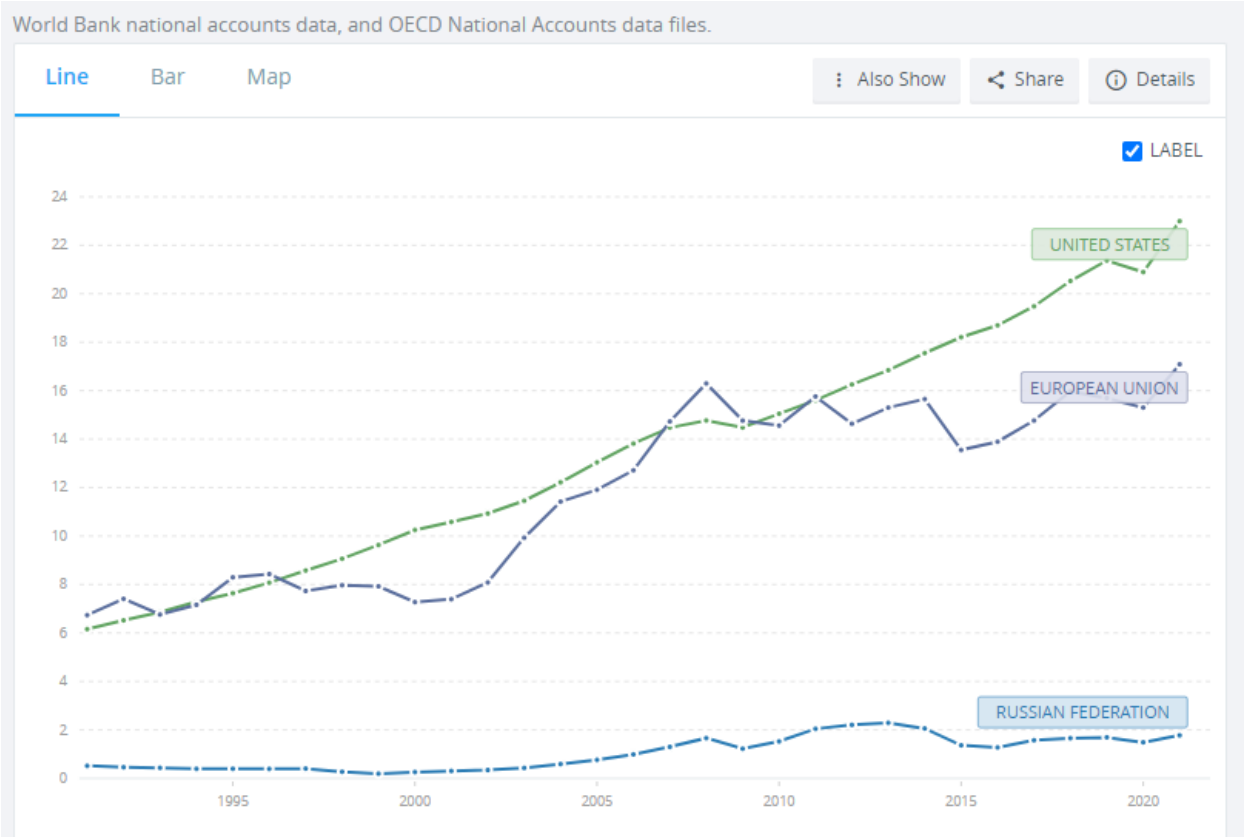

Figure 34: "GDP (current US$) - Russian Federation, United States, European Union" (1991-2021), World Bank, 2021.

Appendix 12: Figure 13 and 14

Figure 13 and 14:

Figure 35: Left to right: Profiles of @euyy450, @meqypiwute, and @vriwyt, all archived on July 19, 2018. (Source: Twitter)

Figure 36: Tweets by @DaWash3241 in August 2016, archived on July 19, 2018. (Source: Twitter / @DaWash3241).

Appendix 13: Figure 15

Figure 15:

Figure 37: "We beat'em before... We'll beat'em again !", David Chavalarias, Toxic Data: Comment les réseaux manipulent nos opinions, 2022.

Appendix 14: Figure 16

Figure 16:

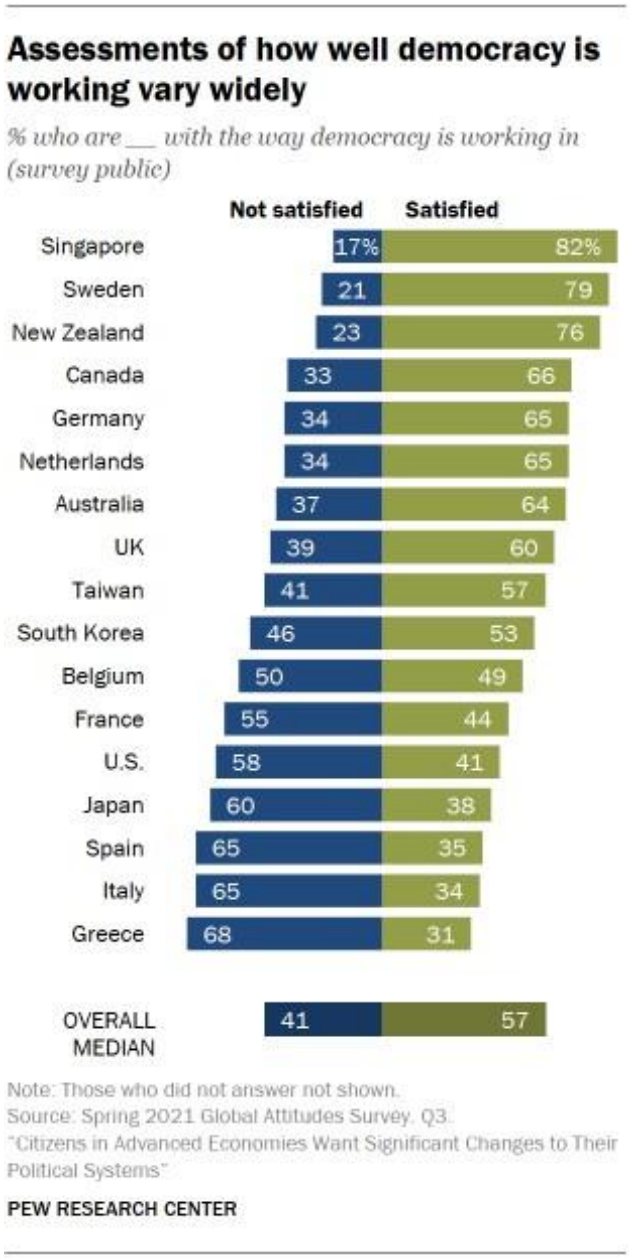

Figure 38: "Assessments of how well democracy is working vary widely". *Pew Research Center*. 2021

Appendix 15: Figure 17

Figure 17:

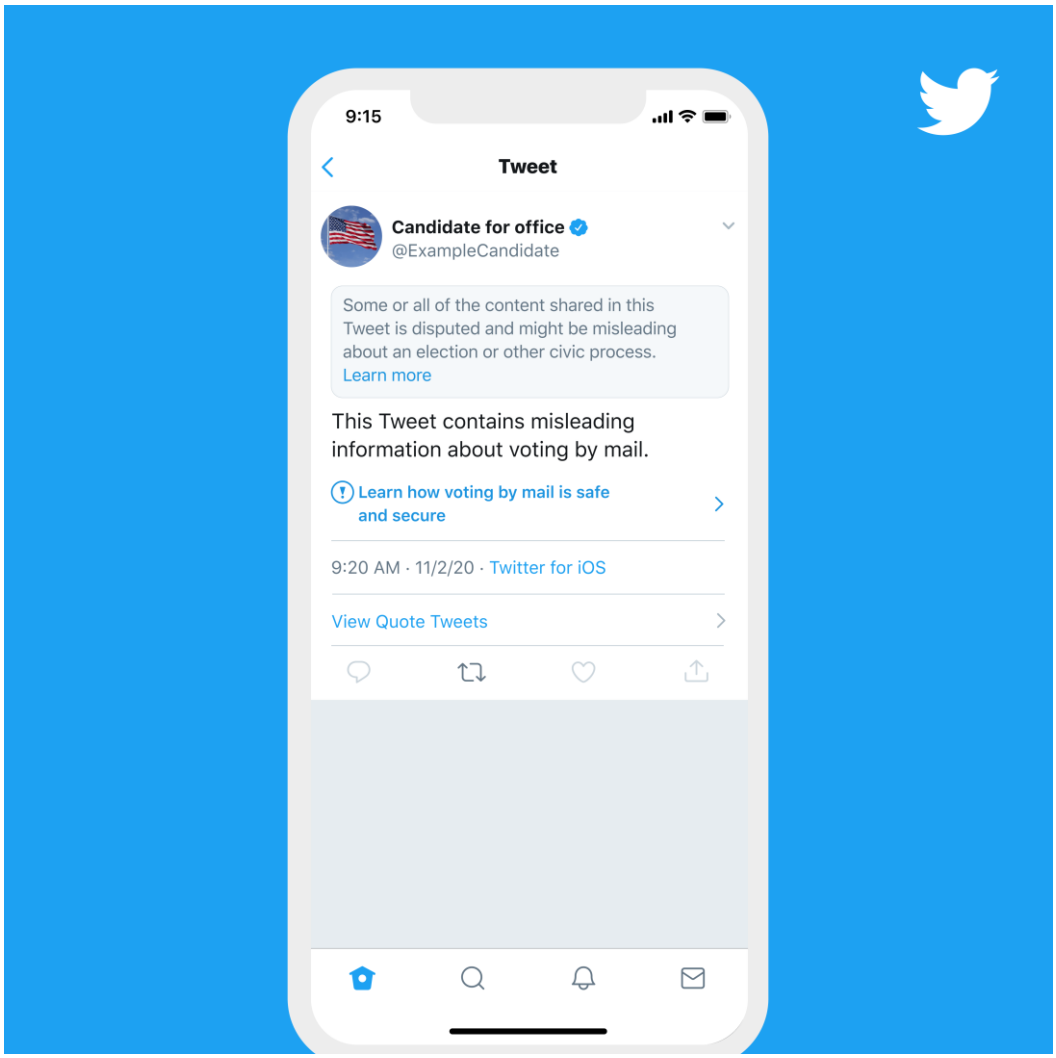

Figure 39: Twitter label. Kayvon Beykpour and Vijaya Gadde, "Additional Steps We're Taking Ahead of the 2020 US Election," Twitter Blog, October 9, 2020.

Appendix 16: Figure 18

Figure 18:

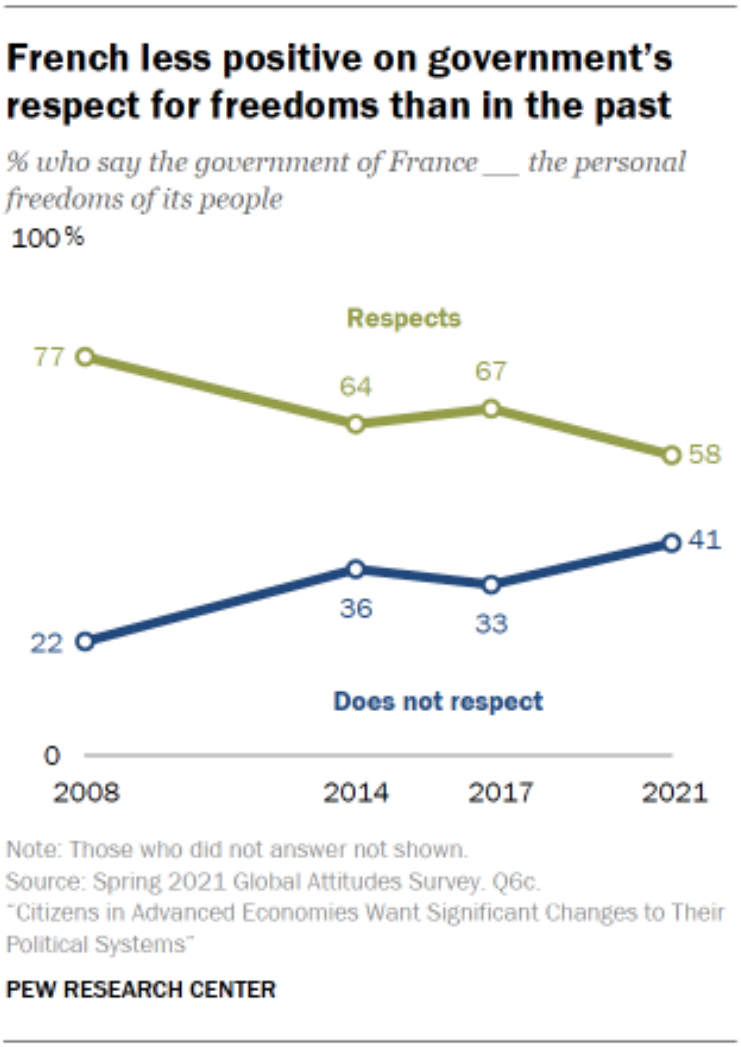

Figure 40: French vision of their government's respect for freedoms (2008-2021). In: Wike et.al., "Citizens in advanced economies want significant changes to their political systems", *Pew Research Center*, 2021.

Appendix 17: Figure 19

Figure 19:

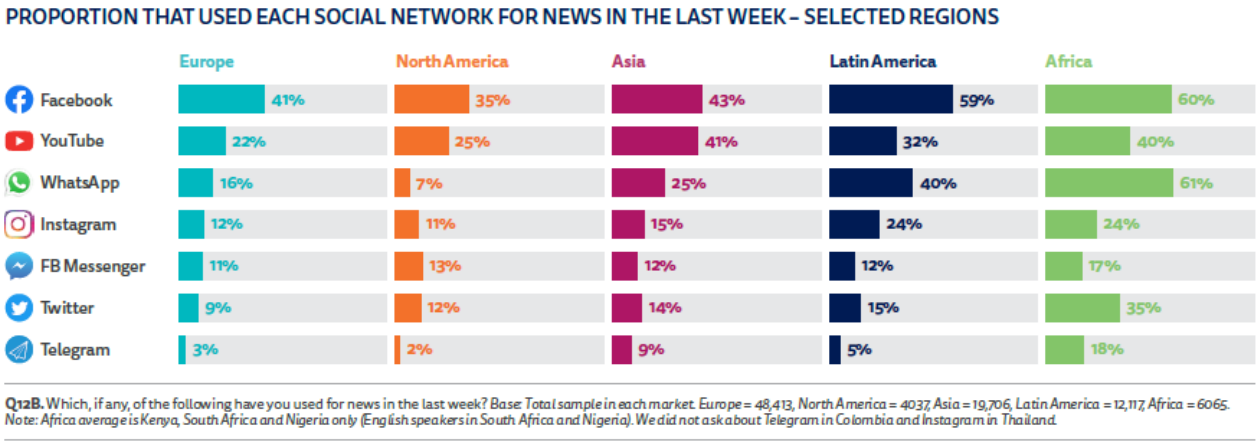

Figure 41: Proportion that used each social network for news in the last week - selected regions. Digital News Report 2022. *Reuters Institute*. June 2022.

Appendix 18: Figure 20

Figure 20:

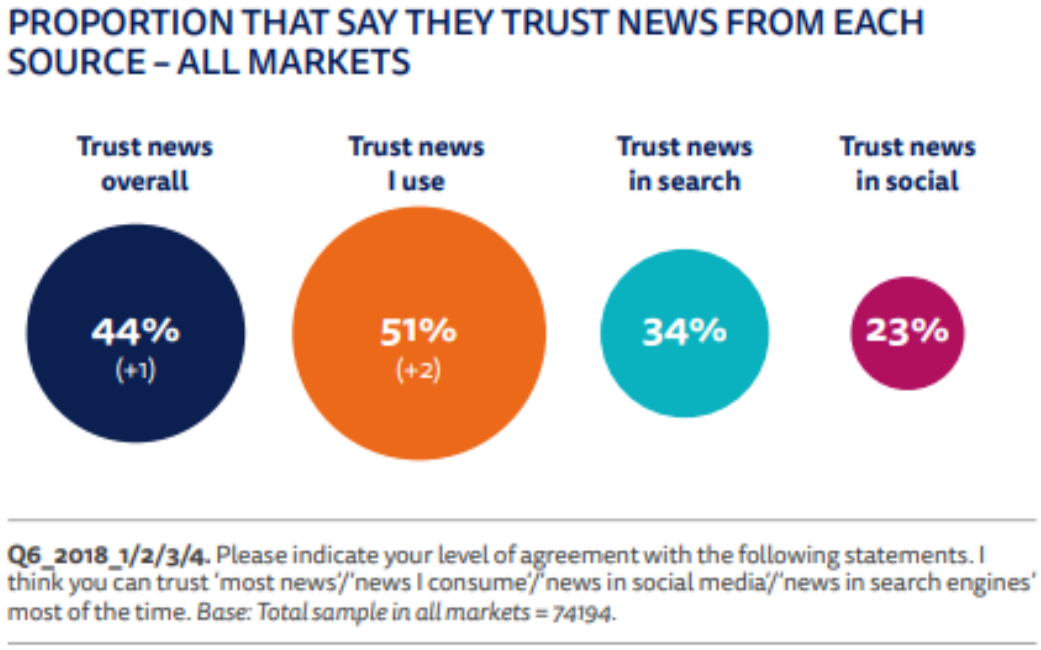

Figure 42: Trust in the news. Newman et.al., "Digital News Report 2018", 2018.

Appendix 19: Figure 21

Figure 21:

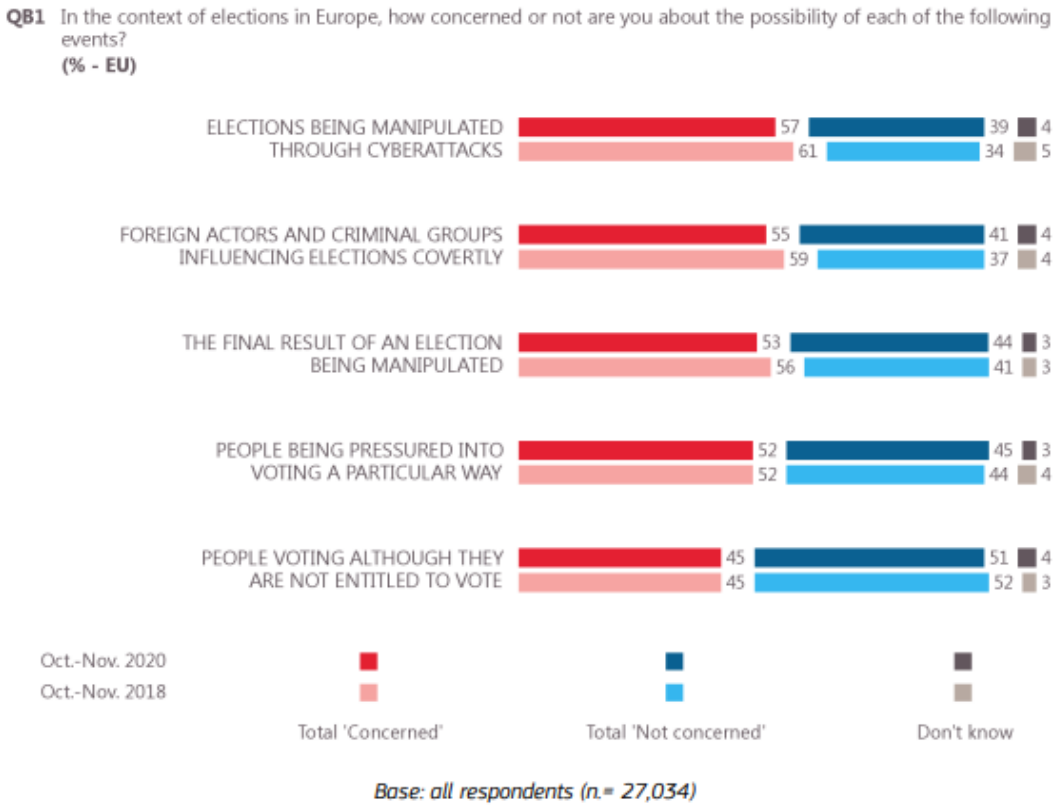

Figure 43: Europeans concerned about particular events in elections. "Democracy in the EU - Eurobarometer Survey 507", *European Commission*, March 2021.

Appendix 20: Figure 22

Figure 22:

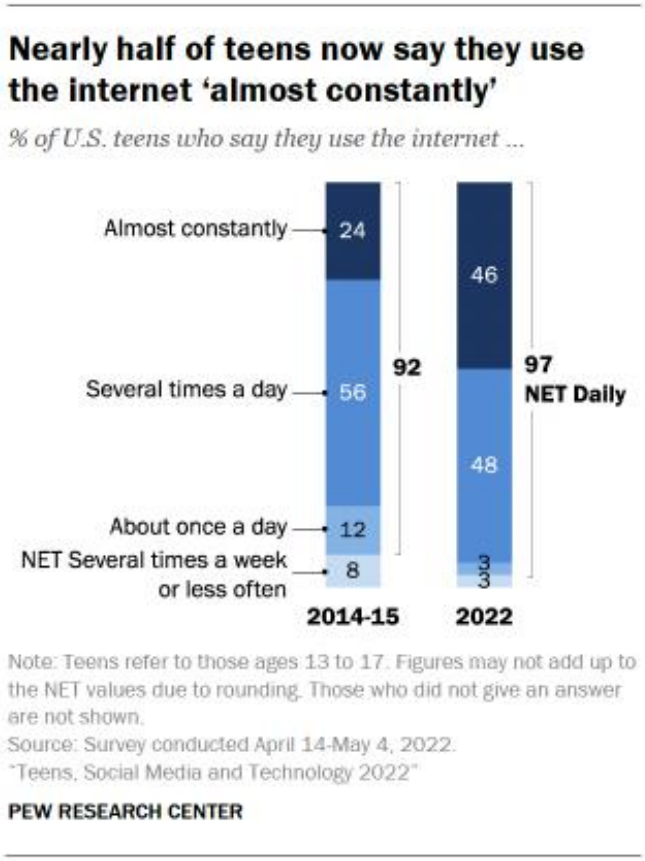

Figure 44: Use of Internet by U.S. teens. "Teens, Social Media and Technology 2022", *Pew Research Center*, 2022.

Appendix 21: Summary of the thesis

Since the first accusations of Russia interfering in U.S. elections emerged in 2016, states have kept a close eye on foreign interference and feared information manipulation campaigns. Similar accusations followed regarding the French presidential elections of 2017, and in other countries. Discussions about this topic emerged in the academic sector as well as in the media or the political sphere, generating a general confusion about the terms used to describe different situations. Framing the debate with clear definitions is therefore necessary in order to avoid confusions and discuss the topic on the same grounds. Here we will provide elements of definition for a few essential notions of our research such as social media, and backdoor (as referring to the title), as well as more complex and debated notions such as information manipulation and foreign interference in elections. Although the first social media in the broad sense emerged at the end of the 1990s, such as SixDegrees.com in 1997, social media as we know them today started developing only in 2004 with the creation of Facebook. The use of these platforms has exploded since the introduction of Instagram in 2010 and Snapchat in 2011. The number of social media users is difficult to evaluate since not all platforms grant access to these data, however, diverse studies agree on the fact that more than half of the world population today are active social media users, a number that is expected to grow. Social media can be defined as forms of Internet-based media that allow groups or individuals to communicate and share information in real time. Important features of social media are the instantaneity of the information, the lack of regulation and national boundaries, as well as possibility of access by every individual. Social media are based on individuals and their interactions, which are different from one society to another. In this respect, since our study focuses mainly on the U.S. and France, we will study the main social media platforms used in these societies, which are mainly Facebook, Twitter, YouTube and Instagram. On social media, as well as on most of the software applications and systems, backdoors can be identified. Backdoors in computer science can be defined as a means to access the computer system or the data of a program, through a security bias. These backdoors are usually meant for legitimate purposes such as maintenance operations carried out remotely, or to leave access for the government. However, when discovered and used by malicious actors, they can represent dangerous vulnerabilities through which malwares can be inserted. In our title, backdoor is used as a metaphor from the cybersecurity world to show how social media's legitimate uses can be deviated and become a window open for malicious actors to cause harm. Through social media, malicious actors can interfere in the electoral process, in several ways such as cyberattacks or information manipulation. The definition of foreign interference is not clear and has been attributed different meanings by scholars, governments, or private companies. In the United States, 'foreign interference' has been defined by the Department of

Homeland Security (DHS) as "*malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies*."[367]. Social media companies also provide us with definitions, such as Facebook that defined 'foreign interference' as "*Coordinated Inauthentic Behavior conducted on behalf of a foreign or government actor*"[368]. If foreign interference is meant to '*influence'* others in the sense that the means used are not coercive, several dimensions need to be added to better understand the concept and to distinguish foreign interference from foreign influence. While public diplomacy through open communication is considered as a legitimate aspect of influence, interference is characterized by a pejorative meaning and considered as neither legitimate nor acceptable according to Kristine Berzina and Etienne Soula[369]. They underline two major dimensions that they consider essential in order to grab the notion of 'foreign interference', which are intent and transparency. Several factors can help determine the intent of these actions such as timing, coordination of behaviors and scale of effect. Transparency relates to the covert and opaque nature of foreign interference. It is important to notice that when we talk about foreign interference in the electoral process, not only we refer to the vote itself but first and foremost to the whole political campaign taking place before, for a period of time more or less extended depending on the country. The political campaign as we know, takes place everywhere, in private conversations, meetings, traditional media but also more and more on social media, which can allow foreign interference. A report conducted by French scholars[370] highlighted three main aspects of information manipulation: it represents a coordinated campaign (not isolated individual messages), which main tool is to spread false or consciously distorted information, with the political intention to cause harm. For the authors, manipulation is more satisfying than influence in the sense that they consider influence as too broad and not necessarily problematic. Information manipulation can therefore take different forms: spread of false or distorted information through bots or trolls, targeting individuals relying on personal information (micro-targeting), hack-and-leak operations against public personalities, and many others. Information manipulation operations therefore use the information environment on social media to manipulate opinions, using and exploiting digital tools and vulnerabilities to achieve their goals. The fact that these operations are launched by a government or non-state actors depends on the definition. However, we will focus here on state-sponsored interference on social media, although it is difficult to prove the role of the government and to distinguish it from actions taken at the individual level.

Foreign interference in elections is considered as a major threat for democracies, since it obstructs the democratic electoral process. The fact, for the people, to not believe in the integrity of their electoral

[367] U.S. Department of Homeland Security, "Foreign Interference Taxonomy. Mis-, Dis-, and Malinformation Resource Library."
[368] Berzina and Soula, "Conceptualizing Foreign Interference in Europe."
[369] Berzina and Soula.
[370] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."

process delegitimizes all the democratic institutions. By manipulating information, foreign actors can also divide the population and increase political tensions. This topic is therefore of great interest since only a thorough understanding can help assess and frame the threat to then propose adapted solutions. Election interference and information manipulation largely predate social media. However, we saw with the 2016 American presidential elections, and later with the 2017 French presidential elections, that it took a different form, more difficult to apprehend, and larger in scale, which at the time generated huge debates and fears due to its unknown and unpredictable character. If today, research permitted a better understanding of the threat, it is still evolving and solutions are still either not adapted or applied unequally. Throughout our research we will therefore try to respond to these questions: how have social media opened up potential opportunities for electoral interference by foreign actors and how can the cases of American presidential elections in 2016 and French presidential elections in 2017 bring insights on this phenomenon? How do states and other actors respond to such threats and to what extent is there room for improvement? Our main hypotheses are first that social media's characteristics and vulnerabilities are used by foreign actors as new tools to interfere in elections and favor one candidate. Another sub-hypothesis is that the U.S. and France both took significant measures to respond to these threats. This work seeks to provide a detailed analysis tackling these hypotheses and the questions raised, through a multidisciplinary and comparatist approach, which will be detailed in the first chapter, along with a state of the art on the topic including the broader literature on cyberspace. The second chapter will study the mechanisms and objectives of foreign election interference through social media, while the third chapter will analyze the response from the measures that are already undertaken to those potentially applicable.

Chapter 1:

Interfering in elections through social media is considered as an emerging hybrid threat for democracies. The cyber dimension of the topic will be underlined since social media emerged as part of cyberspace, that represents a flourishing and constantly evolving literature. Other aspects of the topic will be analyzed emphasizing on the variety of research fields feeding this literature, leading to our final section on the value added by the comparative method. The emergence of cyberspace has rapidly fascinated or worried the world, from researchers, who have seized the opportunity to engage in numerous works providing tools for a better understanding, to states that have shown a significant interest in integrating the cyber domain to their policies. If the birth of cyberspace was accompanied with fantasies and various interpretations of cyber threats, the development of cyberspace literature has progressively framed the topic for a better understanding. These emerging threats have generated a great deal of interest from states, as they understood that they could pose a crucial danger to their security. However, while the cyber world has received significant consideration, hybrid threats related to social media have often been left out of cyber issues, to be analyzed through a separate approach.

The difficulty of the topic resides in the fact that it is composed of three main subtopics (social media, foreign electoral interference, information manipulation), that can be analyzed through the prism of

many research sectors, multiplying the possible approaches. If we tried to present the literature on cyberspace – the main concept encompassing our topic – with an eye of international relations scholars, it is equally crucial to provide an overview of all the different approaches of the topic, so as to widen our view for a more complete understanding. Particular attention will be given to information studies, which, while long established, are experiencing a revival with the emergence of social media. While we chose to focus our study under the prism of cyberspace first, since information manipulation on social media takes place in an online environment, election interference through social media is also extensively analyzed as part of studies on information, reshaping an old strategy in international relations of influencing and controlling the information. In fact, in the post-World War II and Cold War eras, the United States and Russia (or USSR) regularly intervened in other countries' elections: not less than 117 times between 1946 and 2000, according to Dov H. Levin[371]. And information manipulation is not a new phenomenon either: "*the disruption of another country's public opinion and decision-making dates back decades, if not centuries*"[372]. If controlling information is still considered as necessary to uphold national security and preserve sovereignty[373], social media have made it significantly more challenging for states to operate in interconnected networks of several flows and actors.Through the use of automation or Big Data, social media technologies shaped the way information is transmitted significantly, in its scale, scope, and precision, especially for disinformation[374]. Information manipulation on social media therefore seems a relatively new field of study, that we saw stems from the whole literature on cyberspace, but is also of interest to researchers working on information. This subject is at the crossroads of a large number of research sectors, which contributes to its richness. The multidisciplinary aspect of this subject represents a precious strength that it is essential to take into account to understand all its implications.

The comparative method provides some insights on the phenomenon of foreign interference in elections on social media and will represent the core of our analysis, while incorporating multidisciplinary sources. The construction of the thesis will be explained through a quick methodological review of how the research was built, and through a more deepened analysis on the relevance of the French-American comparison. First, it is important to present the methodology used in undertaking this research work, from the reason why it was adopted to the tools and methodology employed. In this research work, we used a large variety of sources from different disciplinary backgrounds, including primary sources (such as official reports and news articles), and secondary sources. The choice of the paired-comparison can be summarized as follows. France and the United

[371] Dov H. Levin, "Should We Worry about Partisan Electoral Interventions? The Nature, History, and Known Effects of Foreign Interference in Elections," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, Oxford University Press, 2021.
[372] James Pamment et al., "Countering Information Influence Activities: The State of the Art: Research Report." (Lund University, July 1, 2018).
[373] Eriksson and Giacomello, *International Relations and Security in the Digital Age*.

States, if they differ in size since the U.S. is 18 times bigger than France, are relatively similar in that they both are well-established democracies and are considered as influential countries at the international level (although France to a lesser extent). Studying their democratic elections is consequently relevant, all the more so since both are presidential elections. Their use of social media is also similar in the sense that they use more or less the same social media and that the social media environment is generally open.

Chapter 2:

Social media being born relatively recently, there is no clear legal framework regulating it, and their functioning today, when associated with human brain characteristics, is an element that facilitates foreign interference, especially when the targeted regime is democratic. The 'democratic disadvantage' on social media leaves democracies more vulnerable to foreign interference in their elections, while authoritarian regimes are somewhat protected by their closed media environment. A democratic regime, by definition, needs to guarantee pluralism and freedom of speech. With an independent and free press in democracies, the state has no direct control on what is published. On social media, it is particularly striking since every individual can express their opinion, and social media companies are the regulators of what can or cannot be said on their platforms. The open media environment is an open gate for false information to spread, since no censorship is organized to remove this type of content[375]. Democracies indeed face a dilemma in countering foreign interference in elections on social media. A solution would be to operate a stricter control on online content, but this would appear as a slide towards authoritarianism. The easiest way for authoritarian regimes to avoid electoral interference through social media is obviously to ban social media. That is why traditional social media that we know today that are born in the U.S. such as Facebook, Instagram, Whatsapp or Twitter, are not available in China. In response, China has built its own social media, such as WeChat, Weibo etc. Similarly, recently, the Kremlin has restricted access to Facebook, Instagram and Twitter, mainly in order to control the narratives around the war in Ukraine[376]. Russians are now compelled to use domestic social media platforms, such as Vkontakte or Odnoklassniki, that are deeply scrutinized by the government.

At the international level, no legal framework has been set up to regulate social media companies' behavior which means that they are often responsible for establishing the rules that will regulate their own content. As Ronald Deibert claimed, social media and private companies on cyberspace operate in legal gray areas with "relative impunity"[377]. Today, the main point of agreement refers to the fact that international law indeed applies to cyberspace, as it was claimed by international organizations

[374] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," Computational Propaganda Research Project (Oxford Internet Institute - University of Oxford, September 26, 2019).
[375] Kreps, *Social Media and International Relations*.
[376] Dan Milmo, "Russia Blocks Access to Facebook and Twitter," *The Guardian*, March 4, 2022.
[377] Deibert, "Trajectories for Future Cybersecurity Research."

such as NATO or the UN. However, key challenges remain, that are grouped into five main categories by Duncan B. Hollis[378]: silence, existential disagreements, interpretative challenges, attribution, and accountability. With billions of subscribers and huge profit margins, social media companies are becoming extremely powerful, challenging states' regulation.

The social media environment is particularly prone to the spread of false or distorted information for several reasons. First, content filtering as operated on traditional media by editors, does not exist on social media, and every individual can publish a message without having to respond to intermediaries. Second, studies have shown that false news spreads faster and at a larger extent on social media. One particularly prominent study by MIT researchers published in 2018[379] showed that "*false news spread farther, faster, deeper and more broadly than the truth in every category of information*", especially regarding political information. Malicious actors can therefore use bots to amplify a movement and make it appear as wide and consensual when it is actually not representative of reality. In a study by Onur Varol et al., over Twitter data[380], authors estimated the percentage of bots in all Twitter accounts to 9% to 15%, while Woolley and Howard estimate it to about a third of all Twitter users[381].

Malicious actors can easily take advantage of social media to manipulate information, due to the vulnerabilities of the human brain, associated with the algorithms designed by these platforms. In order to understand cognitive biases, it is helpful to provide insights on the brain's functioning. Two main systems are at play in the human brain when processing information: the first is fast and instinctive while the second is slower and reflexive. The first is used to make rapid decisions and is mostly controlled by emotions, while the second takes more time since it analyzes the first evaluation and adds other factors to form a reasoning. On social media, the balance between the two systems is altered and the first system that engages emotions takes precedence over the more reflexive system[382], due to the short messages, images and videos online. This superficial processing of information is adequate for everyday tasks, but should be substituted by reasoning for online content that requires a deeper analysis[383]. Our brain reacts in different ways to different messages, in the sense that they can trigger emotions that will lead to various reactions. There are factors that have been highlighted by Claire Wardle and Hossein Derakhshan[384] that increase a message's attractiveness including the fact that it has a powerful visual component, a strong narrative, and is repeated. The visual component is extensively used to spread disinformation through images, videos, and often memes. While Facebook algorithms tend to favor videos and images over text only, the human brain is also more reactive to

[378] Duncan Hollis, "A Brief Primer on International Law and Cyberspace," *Carnegie Endowment for International Peace*, June 2021.
[379] Aral, Vosoughi, and Roy, "The Spread of True and False News Online."
[380] Varol et al., "Online Human-Bot Interactions."
[381] Woolley and Howard, *Computational Propaganda*.Op.Cit.
[382] Chavalarias, *Toxic Data*.
[383] Herbert Lin, "Conclusion: An Outsider Looks In," in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Jens David Ohlin and Duncan B. Hollis, Ethics National Security Rule Law Series (New York: Oxford University Press, 2021).
[384] Wardle and Derakhshan, "Information disorder."

this type of content. Memes are therefore a powerful tool for foreign actors to engage in political debates and banks of memes are established to produce a large number of memes by choosing a picture and replacing the text to make humorous content that will be spread at a wider scale after.

The role of bots can be crucial in repeating a message, using what we call the repetition bias. The more one piece of information is repeated, the more the brain will tend to believe that it is true[385]. Moreover, due to the validation bias, we tend to believe this story even more if it was shared by a close relative. The confirmation bias, also called congeniality bias leads us to remain consistent with our preconceived ideas[386]. This means that we tend to be less critical regarding information that confirms our viewpoint. This confirmation bias is reinforced by algorithms that are designed in a way to suggest content in line with what the user has previously 'liked' or shared.

Algorithms are characterized by technological biases that go hand in hand with cognitive biases, and are even often designed to reinforce the latter. We mentioned that algorithms tend to suggest content that confirms individuals' viewpoints. This leads to the creation of 'filter bubbles', a term that was popularized by Eli Pariser[387]. Many studies after him confirmed that, since algorithms of social media and the Internet tend to deliver content that is linked to our interests and viewpoints, we become trapped in a social media environment that reflects our worldviews excluding alternative perspectives, leading us to a distorted vision of the society we live in. However, this is not representative of the reality and it tends to favor polarization of the society since less and less debate occurs between opposite opinions. A study by Stanford scholars showed that both France and the U.S. were experiencing greater polarization since the 1980s, with the U.S. being the most polarized of the studied countries[388]. Several studies have shown that algorithms also tend to show more extreme or violent content, since they produce more 'engagement'. A study by Norwegian scholars[389] found that some emotions were overrepresented on social media content, such as anger. This means that, while algorithms tend to suggest content that supports our viewpoints, they will also show us some opposite content, but tinged with anger or violence that might be susceptible to engage us, which will further distort our view of alternative opinions, as only extreme and angry ones are represented. Furthermore, algorithms tend to favor violent content. One study showed that Youtube's algorithms favor more extreme content, and even tend to favor far-right extremist content and conspiracy theories[390].

In the same way, algorithms tend to favor more conservative than liberal parties, as found by a study on 9,3 million Twitter users in seven countries (including the U.S. and France). In all countries,

[385] Gérald Bronner, "Les lumières à l'ère numérique," Rapport officiel de la Commission (Présidence de la République, January 2022).
[386] Chavalarias, *Toxic Data*; Bronner, "Les lumières à l'ère numérique."
[387] Pariser, *The Filter Bubble*.
[388] Boxell, Gentzkow, and Shapiro, "Cross-Country Trends in Affective Polarization."
[389] Dag Wollebæk et al., "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior," *Social Media + Society* 5 (April 1, 2019).
[390] Max Fisher and Katrin Bennhold, "As Germans Seek News, YouTube Delivers Far-Right Tirades," *The New York Times*, September 7, 2018.

conservative discourse was amplified by algorithms[391]. False information is also favored by social media algorithms, since they favor engagement by arousing strong emotions such as outrage and anger, as we analyzed previously.

Although social media are well aware of these phenomena, their algorithms keep favoring these types of content and create filter bubbles, because of their need to foster 'engagement'. Engagement is what makes users spend more time on social media, and is the basis of social media's business model.

Technological biases of algorithms, along with cognitive biases therefore form an environment that is particularly vulnerable to information manipulation. Coupled to a particular societal context, malicious foreign actors can use countless techniques to interfere in the political debate during elections, that play on these pitfalls for greater efficiency. After having analyzed different possible methods of information manipulation on social media, we will analyze similar methods that were employed in the U.S. and France, underlining the *modus operandi* of one particular actor: Russia. However, we will see that the scale of these operations was different in the U.S. and France, along with the level of available proof of the intervening actors. Actors that want to manipulate information have a wide range of opportunities to exploit social media vulnerabilities and achieve their ends. These techniques can be grouped into main interrelated categories: microtargeting, disinformation, amplification of the information, or personal attacks, usually cyberattacks (such as theft of personal information) associated with communication on this attack (disclosure of personal information). Trolls and sock puppets are massively used for information manipulation campaigns. Their institutionalization is facilitated through troll farms, which organize and pay people to carry out coordinated actions online[392]. Foreign actors, when trying to penetrate a national political debate through social media, must coordinate their actions between automated and human accounts.

Both in the U.S. and France, claims were made about a foreign actor interfering in presidential elections (in both cases, Russia was at the center of accusations). In the presidential elections in the U.S. and France of 2016 and 2017, the same pattern of information manipulation can be evidenced, despite some discrepancies. For both campaigns, a high impact operation was launched, characterized by what we call a 'hack-and-leak' operation, i.e., the unauthorized intrusion in private computers of one candidate or political party members, stealing of private data and release of these information, generally followed by a campaign of amplification to give visibility to these documents[393]. The most used technique by hackers for accessing confidential data and documents is through *phishing*: they send an email pretending to be a trustful company, person or institution and include a link on which a click by the target will grant access to personal data. This technique was used both in the U.S. and France. In the U.S., private files, emails and documents were stolen to the Clinton campaign through the intrusion in the Democratic Congressional Campaign Committee (DCCC) and the Democratic

[391] Cited in: Chavalarias, *Toxic Data*. Op.Cit.

[392] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."

National Committee (DNC) computer networks, around April 2016[394]. The documents were released by purposefully created websites "DCLeaks" and "Guccifer 2.0", along with the organization WikiLeaks later. A second round of email leaks were linked to John Podesta's, after being victim of a phishing operation also. In February 2017[395], Emmanuel Macron's campaign team in France observed numerous attempts to penetrate their networks, coming from tens of thousands different computers simultaneously, which suggested an organized operation. In May 2017, at 8:35pm, a few hours before the end of the official political campaign[396], more than 150,000 documents were published on the website "4chan" and spread on social media with the hashtag #Macronleaks (first used by Jack Posobiec). In France also, WikiLeaks has largely participated in the diffusion of the hashtag and the leaks[397].

Moreover, both campaigns were characterized by a large diffusion of false and distorted information. From precise and elaborate conspiracy theories to simple false facts, disinformation has infiltrated the electoral campaign. All the stories were spread through memes, false articles or cut video extracts, to stain the candidate's image. Both in the U.S. and in France, foreign actors were involved in some ways in national elections, in the U.S., largely Russia and in France both Russia and some alt-right American citizens, as we will see later. In both countries, documents' leaks and the spread of false information was deeply amplified by bots. As an example, leaks were spread in a short lapse of time, which can make us think that they benefited from amplification tools. The main difference in analyzing tools and techniques that were employed in election disruption was the use of psychographic targeting, through microtargeting. In France, no evidence of microtargeting was found, although it remains very likely, the scale to which it was used might not be meaningful. In the U.S. microtargeting was used by the The U.S. Senate Select Committee on Intelligence found that Russia's Internet Research Agency (IRA), a company considered as a 'troll farm', and linked to Russian officials, funded targeted political advertising on social media and had an interest in favoring Donald Trump[398].

The main differences in the two elections depend on the scale to which information manipulation was undertaken, and their success. France is often considered as a 'success story' in terms of mitigating negative effects of information manipulation operations. In France in 2017, Emmanuel Macron eventually won the presidential elections by far (66,10% for Emmanuel Macron *versus* 33,90% for Marine Le Pen), which can make us think that the overall impact of this anti-Macron information manipulation campaign was low. For Jean-Baptiste Jeangène Vilmer, they "*neither succeeded in interfering with the election nor in antagonizing French society*"[399]. Conversely, in the U.S., several

---

[393] Susan Davis, "Russian Meddling in Elections and Referenda in the Alliance," Science and Technology Committee (USA: NATO Parliamentary Assembly, November 18, 2018).
[394] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."
[395] Jeangène Vilmer, "The 'Macron Leaks' Operation: A Post-Mortem."
[396] Cf the next section for more information on the French official campaign.
[397] Naz Durakoglu, "Hashtag Campaign: #MacronLeaks," *DFR Lab - Atlantic Council*, May 8, 2017.
[398] U.S. Senate Select Committee on Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections."
[399] Jeangène Vilmer et al., "Information Manipulation: A Challenge for Our Democracies."

official reports showed the scale of election interference through information manipulation *via* social media, and how they favored candidate Donald Trump. Several studies even showed that these operations of information manipulation might have cost the election to Hillary Clinton. Studies have shown that disinformation posts linked to Russia on Facebook were seen by roughly 126 million Americans over the period of the electoral campaign, 20 million on Instagram and 1,5 million on Twitter[400]. It only takes a small percentage of those people to have been misled about Clinton and voted for Trump, or more likely, ended up not voting when they would have voted for Clinton otherwise, to change the outcome of the election.

These two operations have, hence, been more or less successful depending on the country, which can be explained by different factors. Main differences in political and electoral systems, foreign actors' campaign sophistication or anticipation of the threat, can help explain why the information manipulation campaign was more successful in the U.S. than in France.

If we can highlight similar Russian techniques and tools employed for interfering in elections, the attribution of cyberattacks in general, and information manipulation operations on social media, is often delicate, and if the U.S. officially attributed it to Russia, the French government never explicitly accused the Russian government of such information manipulation operation. Russia's interference in the U.S. presidential election of 2016, has been proven by several official reports, such as the U.S. Senate Select Committee on Intelligence reports in five volumes[401] for a total of 1313 pages with more than 200 witnesses and a million documents reviewed[402] published between 2019 and 2020. Another important report is the so-called 'Mueller report'[403]. Robert S. Mueller, former FBI Director, was commissioned by the U.S. executive to investigate Russian interference in the 2016 presidential elections, and the potential links with the Trump administration.

In France, it was found that first hacking attempts against Emmanuel Macron and his relatives or collaborators were operated by APT-28, a Russian hacker group linked to the GRU. The link used for Macron's phishing operation was also found in GRU communications[404]. APT-28 is also considered to have conducted the phishing operation against Clinton's team in the DNC Leaks[405]. In addition to the hack and leak operations in the U.S. and France, a similar pattern of information manipulation on social media through disinformation and the use of amplification techniques tend to point at Russia, as instigator of this campaign, through the IRA. Many official reports were published in the U.S. recognizing through official institutions such as the Senate or Intelligence services, the role of Russia in interfering in the 2016 elections (cf Chapter 3). Intelligence officials' testimonies to the Senate had a great impact in recognizing the role of Russia in election interference. Of all the six Intelligence

[400] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements."
[401] U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volumes I-V."
[402] "Press Release of Intelligence Committee: Senate Intel Releases Volume 5 of Bipartisan Russia Report."
[403] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."
[404] Andy Greenberg, "Hackers Hit Macron With Huge Email Leak Ahead of French Election," *Wired*, May 5, 2017.

leaders interrogated, none refuted the Kremlin's role in interfering in U.S. elections (including some of Donald Trump's close allies, Mike Pompeo and Dan Coats). Conversely, France was reluctant in attributing the information manipulation campaign during the 2017 presidential elections to Russia, and although some comments were made implying Russian interference in elections[406], no official statement was made accusing the Russian government of these operations. While several factors explain these differences in attribution, they are essentially linked to the fact that, although the U.S. succeeded in finding clear evidence of Russian interference in elections, attribution of foreign interference in elections and cyberattacks in general are extremely rare and remain a sensitive issue. Attribution of election interference through cyberspace (in this case, cyberattacks and social media), is extremely difficult, because of the multiplicity and anonymity of actors, and the unavailability of social media data.

After analyzing the means employed to interfere in elections through social media and which actors were at the origins of such attacks, especially in the cases of the U.S. and France, it is necessary to understand the motives of such interference. The first explicative factor for initiating information manipulation operations in order to interfere in elections is simply that it does not require much resources. As we saw earlier, social media represents a fairly open environment, accessible to everyone. Therefore, manipulating information on social media does not necessarily require advanced digital skills and the barriers to entry are low. According to Samuel C. Woolley and Philip N. Howard, political bots are developing and becoming even cheaper, with "*armies of bots built to like particular content or send message "bombs" costing less than 100 US dollars*"[407]. Russia has a particular interest in launching information manipulation operations, "*as a way to offset conventional disadvantages*"[408].

The second reason of foreign interference in elections through social media is the most straightforward, that is to say, to favor one candidate. Both in the U.S. and France, identifying one candidate that was favored, or conversely, reviled, is relatively straightforward. Russia, for example, considered more favorable – and did not hide it – to see Donald Trump become President instead of Hillary Clinton. In a similar way in France, Emmanuel Macron was the target of information manipulation and hack and leak operations. The candidate, known for his positions not favorable to Russia, such as the continuation and reinforcing of the sanctions against Moscow, or his strong liberal and European perspectives, was considered to represent a danger for Russian interests. Conversely, Marine Le Pen is considered to share more interests with Russia, as she supported lifting the economic sanctions against the country.

---

[405] Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election."

[406] A tense first meeting between Emmanuel Macron and Vladimir Putin took place at Versailles on May 29th 2017, in which the French President told his Russian counterpart that he knew what Russia did and could do in terms of election interference. Meeting Macron-Putin, France 24. https://www.youtube.com/watch?v=QV_mwKoAHtU

[407] Woolley and Howard, *Computational Propaganda*.

[408] Kremer and Müller, *Cyberspace and International Relations*.

However, if supporting one candidate is often an objective of interfering in elections, the main driver behind election interference through social media is generally to disrupt the democratic process and affect the society as a whole. The primary way to manipulate information on social media is by exploiting pre-existing tensions so as to fuel the conflict and polarize society. The goal is to foster extreme positions in order to shape the public debate. In doing so, extreme positions become normalized and polarization deepens, resulting in a lack of cohesion and common points of reference[409]. Moreover, disturbing the electoral process amounts to questioning the legitimacy of leaders and institutions themselves.

Chapter 3:

Claims and evidence of foreign interference in elections through social media raised awareness and generated various responses by the United States and France, as well as other non-state actors, to counter those threats. However, these responses triggered reactions and debates and their efficiency is often disputed, which brings us to discuss potential solutions and improvements for countering foreign interference in elections through social media.

The U.S. and France both took the threat seriously and implemented various measures in order to try to fight it, in generally similar ways, although some different steps ought to be highlighted. One major difference between the U.S. and France in fighting foreign information manipulation operations lies in France's membership to the European Union, whose role in this respect is worth mentioning. Other similarities and differences in responses by non-state actors will also be highlighted.

If similar responses regarding administrative agencies were implemented, approaches regarding regulation and official positions through works of investigation and official statements, differed in some ways. France's action is more covert, while the U.S.' more frontal, and includes important works of investigation. One main difference between the American and French response is their vision of the state's role in regulation. This is partly due to differences in their political systems with federal versus centralized political systems. Regulation regarding social media companies remains quite low in the U.S. compared to France, especially if we take into account other rules that apply to France, as part of the European Union (EU) that provides a major regulatory framework and other measures for European countries. States are not the only actors that responded to election interference and information manipulation in the U.S. and France. Private companies and civil society also played a role in the post-election interference. In combating fake news, democratic states have little room for maneuver if they do not want to appear as authoritarian states that censor what they consider as untrue. In this sense, it is generally agreed that states should be involved as little as possible in debunking fake news. Civil society therefore filled that void in taking initiatives to debunk fake news on social media and try to counter these disinformation campaigns. Efforts were also made by social

[409] Kreps, *Social Media and International Relations*; Davis, "Russian Meddling in Elections and Referenda in the Alliance."

media companies after being pressured to counter information manipulation. However, these efforts are still insufficient in preventing election interference, and could benefit from several improvements.

As stated by Myriam Dunn Cavelty and Florian J. Egloff: "*a satisfactory level of cybersecurity can only be achieved by government, business, and society together*". This applies to the specific threat of election interference through social media. These actors must work together and bring changes in education, coordination, and regulation, which could significantly improve the prevention and response to the threat. Education is essential in order to respond through a whole-society approach. First, education is need to raise awareness among the general public and help identify information manipulation operations from the younger age. Then, education through research is also essential and helps deepen the topic through all its aspects, useful for citizens, private companies and last but not least, governments to design their policies. However, one key obstacle regarding research on social media remains, and has to be addressed, that is the fact that most social media data are not accessible and kept secret by the companies. These data are considered as essential in order to produce evidence-based policies, as underlined by the Council of the EU in a 2019 report[410], and further regulation must therefore be established to compel social media companies to publicize these data or facilitate their accessibility for researchers. If cooperation is essential to share knowledge and improve the threat's understanding, it must be further developed to achieve a satisfying coordinated governance, at all levels. Building a strong cooperation between actors and structures is essential in order to avoid a counterproductive effect, as highlighted by the last INGE report[411]. One crucial element in countering information manipulation operations is in providing the necessary legal framework to address the issue. From national to regional and international regulation, along with working with actors concerned by the regulation, designing an adapted legal framework is not an easy task and there is still room for improvement. States, social media companies, but also civil society and experts could work together in building the appropriate legal framework. If the fact that international law applies to cyberspace is largely consensual, how it applies and how it can be implemented remain widely debated issues. No internationally accepted sanction is provided for election interference through social media. However, implementing laws and sanctions raises critical questions on the necessary balance between regulation and liberty that will be addressed in the next part.

The last part aims at responding to legitimate questions on the necessity and utility to act, when looking at some particularly controversial aspects of the issue. Controversial issues ranging from countermeasures' drawbacks to the functioning of social media and their role in a broader context makes us wonder if action is really needed and desirable. The issue of regulation has already triggered huge reactions and debates both in the U.S. and France, so to avoid any accusation towards states going too far in restricting individual liberties, they must be really careful in choosing the best suited

[410] "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions."
[411] INGE Special Committee, "Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation."

regulation and build that regulation along with civil society and private companies. It is essential to remember that one crucial recommendation is to always bear in mind democratic values, and not use the same techniques as authoritarian regimes. Another stance taken in criticizing countermeasures to respond to information manipulation through social media, is to claim that small changes will be inefficient in the sense that the social media system is inherently prone to information manipulation, and is not likely to change. Unless a profound transformation of their financial model is imposed on social media, companies will keep hosting and encouraging all types of content on their platforms. Nevertheless, we argue that change is possible in diverse manners. If more incentive is given to social media to change their algorithms and to rely on experts' knowledge with an ethical perspective to design them, our online environment could be safer and less prone to information manipulation by foreign actors. Beyond those who think that foreign interference in elections through social media manipulation cannot or should not be addressed for several reasons, there are those who believe that this threat might actually be as important as we think. First, because social media are not used by everybody and might not have a crucial impact on society and then, because it seems unlikely that social media can really change the outcome of the election. As a counterargument, we claim that through traditional media, information manipulation campaigns have an impact even on those who do not use it, and that it can change the outcome of the election in case of a tight battle as it was the case in 2016. Overall, despite all interrogations, we argue that the potential consequences of these operations are too risky not to try to act. questioning whether information manipulation campaigns changed the outcome of the elections diverts us from the real focus: the disruption of democracy in general. As Jens David Ohlin put it: "*The danger posed by a particular threat is measured not by the actual damage caused but rather by the potential disruption it represents*"[412]. Information manipulation operations might have several negative impacts on the society as a whole. They disrupt democracies by eroding trust in institutions, elected leaders, and the media; along with polarizing societies. Moreover, the reach of the threat (France and the U.S. are not isolated cases), and its constant evolution make us think that it is not ready to fade, and we should therefore be prepared to either counter it or live with it in a more adapted manner.

Conclusion:

All in all, social media represent a backdoor for foreign interference in elections. Our first hypothesis was that social media's characteristics and vulnerabilities are used by foreign actors as new tools to interfere in elections and favor one candidate. Throughout this research, our hypothesis is partially corroborated, since we indeed found that foreign actors can weigh in the political debate and favor one candidate over another. However, we saw that the main consequence of these operations is not primarily that one candidate might be elected in lieu of another, but mainly the fact that they disrupt the democratic electoral process, leading to an erosion of trust in political institutions, elected

[412] Ohlin, "A Roadmap for Fighting Election Interference."

representatives and the media. If the U.S. and France have faced similar campaigns of interference in their 2016 and 2017 presidential elections, through social media, including hack-and-leak operations and disinformation campaigns, the scale of the operation differed as well as the states' response. The U.S. faced a more developed and pugnacious campaign, considered as relatively successful, whereas for France, the operation was considered a failure and less elaborated. Mainly due to the scale of the attack, the U.S. and France had different responses, with the U.S. attributing this attack to Russia after thorough investigations while France was said to respond by more covert diplomatic means, only evocating the possibility of a Russian-related campaign. Since 2016, countries and international organizations and institutions have shown the will to take this threat seriously and build more resilient societies to election interference through social media. From regulation, to education and cooperation, various significant measures have been undertaken. However, they should still be constantly reviewed and improved, in light of this rapidly evolving, multifaceted threat. In this respect, our research has permitted a better understanding of two important operations of election interference through social media, underlying similarities and differences both in the tools employed and in the response to these operations. Keeping in mind the necessity to adopt a multidisciplinary approach when tackling this topic, has allowed us to present interconnected issues and solutions, sometimes lacking in the present literature. This research has therefore tried to bring insights for an assessment of the threat in two diverse but similar countries, and potential recommendations to tackle the issue at multiple levels. However, for material purposes the research focused on 2016 and 2017 elections, while more recent elections that took place in the U.S. and France might bring further details on the countermeasures' efficiency and the evolution of the threat. Presidential elections in 2020 in the U.S. and 2022 in France, have shown that this threat is still a source of concern in our societies, although occurring under different forms. Therefore, it is crucial to remain persistently vigilant and keep analyzing potential evolutions of this threat, and share this knowledge to the population and decision-makers for a whole-of-society response.