INFORMATION MANIPULATION

A Challenge for Our Democracies

A report by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

MINISTÈRE
DES ARMÉES

AUTHORS

Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera.

ABOUT CAPS AND IRSEM

The Policy Planning Staff (Centre d'analyse, de prévision et de stratégie), known as CAPS, created in 1973, reports to the Minister for Europe and Foreign Affairs. Composed of around twenty experts, diplomats and academics, CAPS produces trans-disciplinary and forward-looking analyses of medium- and long-term developments in the international arena for the benefit of the French Foreign Minister and French authorities. It also proposes foreign policy recommendations and strategic options drawn from its own analysis and interactions with the world of think tanks and academic research in the field of international relations.

The Institute for Strategic Research (Institut de recherche stratégique de l'École militaire), known as IRSEM, created in 2009, is the research institute of the Ministry for the Armed Forces. Composed of around forty people, including both civilians and military personnel, the majority of whom hold doctoral degrees, IRSEM's primary mission is to promote French research on defense and security issues. In addition to conducting research internally (for the benefit of the Ministry) and externally (for the wider strategic community), the IRSEM also encourages the emergence of a new generation of researchers (*la relève stratégique*), contributes to higher military education and engages in public debate on questions related to defense and security.

To cite this report
J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the 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, Paris, August 2018.

This report is available in French and in English (this is an English translation of the original French document).

Printed in Paris, August 2018.

ISBN: 978-2-11-152607-5

Cover © Antonio/Getty Images.

INFORMATION MANIPULATION

A Challenge for Our Democracies

A report by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Rechearch (IRSEM, Ministry for the Armed Forces)

CONTENTS

FOREWORD

Our Study

Our investigation is the product of an awareness of the existential danger that information manipulation poses to our democracies. This awareness was generated by two series of events: first, the repeated interferences that have occurred since 2014 (Ukraine, Bundestag, Dutch referendum, Brexit, US election) have shown that even the largest Western democracies are not immune. Second, the attempted interference in the 2017 French presidential election, culminating with the so-called "Macron Leaks" incident, captured French attention and demonstrated to us the importance of studying this subject.

In September 2017, acting on our own initiative, we decided to set up a joint working group bringing together members of the 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. Initially, the purpose of this working group was to explore the possibility of creating an inter-agency task force to combat information manipulation. But, above all, this group gave itself the task studying the underlying problem, its causes, its consequences and the solutions that can be brought to bear.

This working group was intended to be inter-agency in order to respond to the inherently interdisciplinary nature of information manipulation, which lies at the crossroads between international relations, war studies,

intelligence studies, media studies, sociology and social psychology. Consequently, our subject concerns several different administrations.

This working group was designed to study the problem from an international perspective, taking into account not only our national interests, but also the transnational nature of information manipulation, which transcends sovereignty and individual State legal systems. While certain cases are more well-known than others, the issue of information manipulation is universal. It is an issue that affects civil society as well as the governments of many States, not only in Europe and North America, but also in Asia, in the Middle East, in Africa and in Latin America. However, information manipulation is also diverse in nature and each case is different and is tailored to fit different target audiences.

It is important to distinguish between exogenous manipulations, which originate from outside the targeted State, and endogenous manipulations, which originate from within a State. We must also distinguish between attempts that are caused by state actors and those that are caused by non-state actors. Given that it was impossible to cover everything, and given our particular focus on foreign affairs and defense, we chose to limit the scope of this report to the study of information manipulation orchestrated by foreign States, or in other words, foreign interferences.

Over the last few months, we visited twenty countries (Austria, Belgium, Canada, Czech Republic, Denmark, Estonia, Finland, Germany, Italy, Japan, Latvia, the Netherlands, Poland, Russia, Singapore, Spain, Sweden, the United Kingdom, the United States and Ukraine) and three organizations (the EU, NATO, the OSCE). We have conducted about 100 interviews with national authorities (Foreign Affairs and Defense Ministries, intelligence agencies, national Parliaments) and representatives of civil society (academics, think-tanks, NGOs, journalists) to find out their perceptions of the existing threats and the countermeasures put in place. We also conducted interviews in France with national authorities, members of civil society and private actors, basing our research on the scientific literature on the subject (see the bibliography for an overview).

We produced a dozen internal memos within the relevant ministries and departments, a published research paper[1] and organized several public events including a seminar cycle at the IRSEM on "Information Warfare" and an international symposium organized by the CAPS on 4 April 2018, which had opening remarks given by the Minister for Culture and closing

1. Maud Quessard, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information?,* IRSEM Research Note, 54, 30 April 2018.

remarks by the Minister for Europe and Foreign Affairs. The Foreign Minister's closing speech is the longest and most detailed French official statement on the subject of information manipulation to date.

In his speech, the Minister mentioned the present report, which was then in the making, and is the principal result of our research. He expressed his hope to be able to "draw lessons from it."[2] This is also what we hope to accomplish. It must be noted however that this report does not and should not be considered as reflecting an official position of the French government. CAPS and IRSEM enjoy a degree of autonomy within their respective ministries. Within this report, our team of researchers and diplomats express their independent opinions.

Nor should this report be considered as our final position: we will continue to explore the subject in the future, within our respective remits, particulary to try and keep an updaded view of the latest developments in this phenomenon, whose impact will continue to be felt within our democracies in ever-changing ways.

2. "The Policy Planning Staff of my Ministry, along with the Institute for Strategic Research, is currently finalizing a report that assembles the analyses and best practices of our partners, researchers, media and civil society organizations from around the globe. I hope that we may draw lessons from it" (Jean-Yves Le Drian, *Discours de clôture de la conférence internationale "Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information,"* Paris, 4 April 2018).

SUMMARY

Information manipulation is not a new phenomenon. The attention that it has recently attracted is tied to a combination of two factors: on the one hand, the unprecedented capacity of the internet and social networks to rapidly, even 'virally,' spread information; on the other hand, the crisis of confidence that our democracies are experiencing, which devalues public speech and goes so far as to relativize the very notion of truth.

The 2016 US and 2017 French elections have shed a critical light on this phenomenon, its mechanisms and consequences. Yet, the impact of information manipulation—and, in some cases, its very existence—is sometimes called into question. Are we not in the context of democratic debate, whose excesses can be corrected by existing legislation? Is the emphasis numerous governments place on "fake news" not a suspiciously convenient way to clear themselves of blame or point fingers at the alleged enemies of democracy, including those abroad, in order to consolidate power? Could it even be an insidious pretext by which to challenge civil liberties and, above all, freedom of expression?

These objections are serious. They require in-depth examination in order to identify as clearly as possible what actually constitutes information manipulation. Therefore, this report proposes a definition of the problem by substituting the vague and controversial notion of "fake news" for the more precise term, "information manipulation." The latter term is

understood as the intentional and massive dissemination of false or biased news for hostile political purposes. This report focuses on a specific kind of information manipulation: those which are orchestrated by States, and whose purpose is to weaken or destabilize democratic debate in other States.

Working off of this definition of information manipulation and drawing on our numerous interviews and a thorough review of the abundant literature on the subject, this report proceeds as follows. Firstly, the report explores the causes of information manipulation, which exist partly at the level of the individual. After all, information manipulation is tied to human nature and arguably finds its roots in psychology and epistemology (cognitive weaknesses and a crisis of knowledge). Causes also exist at the collective level as information manipulation is linked to our social lives (a crisis of trust in institutions, a crisis of the press and disillusionment with the digital world). After having analyzed each of these causes, we then proceed to identify the beneficiaries of these activities, i.e. the actors carrying out information manipulation. We focus specifically on States that manipulate information outside their territory or, in other words, who interfere in the internal affairs of other States.

Secondly, this report highlights the distinctive features of recent information manipulation campaigns in order to identify some common characteristics—both in terms of vulnerability factors (the presence of minorities, internal divisions, external divisions, a vulnerable media ecosystem, contested institutions) and in terms of the means (multiform levers and vectors, calibrated narratives, privileged places and mechanisms, massive data leaks, the falsification of documents, direct interference in democratic processes). We also explore information manipulation in regions other than the post-Soviet space, Europe and North America—which are the best known—by turning our attention to several case studies in the Middle East, Africa and Latin America.

In the third part, which is devoted to the responses to information manipulation, we summarize the countermeasures adopted by all actors: States, international organizations, civil society and private actors. We start with a case study on the "Macron Leaks," which stand apart from the recent history of election meddling precisely because they failed to achieve their intended purpose. It is, therefore, important to understand why and to draw lessons from this isolated incident.

To conclude, we identify future challenges—technological challenges, future trends in Russian "information warfare" and possible future

scenarios. Lastly, we propose 50 recommendations operating on the assumption that information manipulation will remain a problem in the future and that it will constitute a long-term challenge for our democracies. In the face of this challenge, democracies must provide a participatory, liberal response that respects fundamental rights. In closing, we anticipate some of the criticism that our recommendations will receive and note some of our responses to these objections.

Information is increasingly seen as a common good, the protection of which falls into all citizens concerned with the quality of public debate. Above all, it is the duty of civil society to develop its own resilience. Governments can and should come to the aid of civil society. They should not be in the lead, but their role is nonetheless crucial, for they cannot afford to ignore a threat that undermines the foundations of democracy and national security.

INTRODUCTION

Information manipulation—be it by production, retention or distortion—is as old as information itself and has always been ingrained in social life. It is indeed one of the many timeless ruses of war[1]. Consider one early example: before the Battle of Qadesh in 1274 B.C., it is believed that the Hittites transmitted false information to the Egyptians to influence the outcome of the conflict. Scholars have been theorizing the use of information manipulation since antiquity, through works such as *The Arthashstra* of the 4th century B.C., Plato's *Dialogues*, Aristotle's *Rhetoric*,[2] and more recently, Pascal's *Art of Persuasion* (1660) or Arthur Schopenhauer's *The Art of Being Right* (1830). Historian Robert Darnton has shown how fake news benefited from the development of print media, including French and English sensationalist pamphlets (known in France as Parisian *canards*) of the seventeenth and eighteenth centuries.[3]

Disinformation has a long legacy in the twentieth century as well.[4] *The Protocols of the Elders of Zion* (1901) constitutes one of the first famous examples. The rise of totalitarianism served as a catalyst and the Cold War, too, had its share of well-known episodes. Two infamous examples were

1. Jean-Vincent Holeindre, *La Ruse et la Force, Une autre histoire de la stratégie*, Perrin, 2017.

2. Alexandre Koyré, *Réflexions sur le mensonge*, Paris, Allia, 2004.

3. Robert Darnton, "The True History of Fake News," *The New York Review of Books*, 13 February 2017.

4. Vladimir Volkoff, *Petite Histoire de la désinformation*, Éd. du Rocher, 1999.

the Soviet propaganda campaigns which sought to blame the CIA for the assassination of Kennedy (in 1963) and the AIDS epidemic (Operation *Infektion*, 1983-1987).[5] In 1962, jurist and sociologist Jacques Ellul argued that propaganda had "become a very general phenomenon in the modern world."[6]

Despite—or perhaps because of—this lengthy history, the subject suffers from a great deal of confusion as far as terminology is concerned. There are a profusion of words that are used as synonyms or without being properly defined: "propaganda," "disinformation," "fake news," "post-truth," and various types of "warfare" (information, psychological, political, ideological, subversive, hybrid, etc.) This confusion has led some to equate RT with the BBC or France 24 or to minimize the entire problem by claiming that "everything is propaganda." For this reason, clarifying the terminology is an essential prerequisite to our analysis. In this introduction, we will review the existing terminology and then justify our decision to use the term "information manipulation," which we believe is best suited to the context. Our goal is to both to define the terms of the debate and to demonstrate the importance of this issue, bearing in mind the effectiveness of and the challenges posed by these kinds of manipulation.

I. What are we talking about?

The subject is riddled with an abundance of imprecise terms, mixing classical notions (influence, propaganda, disinformation) with neologisms (fake news, post-truth, fact-checking), whose multiplication "signals the inability for the existing vocabulary to describe a social world that is completely transforming."[7] To ensure the study had solid foundations, it was imperative first of all to identify and set aside the most vague and ambiguous of them and find a more precise definition of the phenomenon under consideration.

— "Fake news" is the most commonly used expression, even in French, where it is sometimes translated into "*fausses informations*" (false information) although it might be more accurate to speak of falsified, counterfeit,

5. Thomas Boghardt, "Operation Infektion: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, 53:4, 2009, p. 1-24.

6. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes,* Random House, 1965, p. ix.

7. Jayson Harsin, "Un guide critique des *Fake News* : de la comédie à la tragédie," *Pouvoirs*, 164, 2018/1, p. 99.

or forged information. The term was popularized in 1999 by *The Daily Show*, a satirical American show that tampers with information and news for comedic purposes, much like *The Onion* news journal. This first generation of fake news, a humoristic one, lasted for around fifteen years. Since the 2016 American presidential campaign, the usage of the term literally exploded (+ 365% in 2017 according to the Collins Dictionary, who named it "word of the year") however its connotation became negative, going "from comedy to tragedy."[8] Following the lead of the European High Level Group on Fake News and Online Disinformation,[9] we reject this term for two reasons: firstly, because it is too vague and does not account for the fact that part of the problem arises from information that is not, strictly speaking, "false." Secondly, the term has become so overused that it is not uncommon, even for certain heads of State, to use it for all news that they dislike, ultimately enabling a form of populism that is hostile to the freedom of the press.

— The notion of "political warfare," which applies to all non-military and non-lethal operations, and even the sub-field of "information warfare," are simply too broad. Furthermore, these terms entail a militarization of information and of the academic literature devoted to this phenomenon. This critique also extends to "hybrid warfare," a widespread but confusing notion, which in reality refers to war waged across the full spectrum—from conventional means to information and cyber means, from clandestine operations to nuclear intimidation.[10] It is, therefore, even broader than the preceding two categories, because hybrid warfare associates non-kinetic elements (such as information) with kinetic ones.

— "Propaganda," defined as "an attempt to influence the opinion and behavior of society in order for people to adopt a particular opinion and behavior,"[11] is also too vague. Above all, it does not apply to our subject because the term propaganda implies the defense of an alternative world view. This is an element that the current observed phenomena—essentially centered on the denigration of others—appear to lack.

— "Influence" and "public diplomacy" are also very broad and, above all, they are not in themselves problematic. All States who possess the

8. *Ibid.*

9. European Commission, *A Multi-Dimensional Approach to Disinformation, Report of the Independent High Level Group on Fake News and Online Disinformation*, March 2018, p. 10.

10. For a critique of the vocabulary of hybrid warfare and its alleged novelty, see Joseph Henrotin, *Techno-guérilla et guerre hybride : le pire des deux mondes*, Nuvis, 2014 and Elie Tenenbaum, *Le piège de la guerre hybride*, Focus stratégique 63, IFRI, October 2015.

11. Jean-Marie Domenach, *La Propagande politique,* Paris, PUF, 1965, p. 8.

means to do so implement strategies of influence that involve public diplomacy. The distinction proves useful when responding to the line of argument that views RT and Sputnik as merely the Russian equivalents of mainstream media. As the RT chief editor repeatedly states, "We do not give the Kremlin's point of view, but that of Russia, like France 24 or the BBC, which present the values of France and Great Britain or Al-Jazeera for the Arab world."[12] However, RT and Sputnik are not criticized for carrying out public diplomacy, but for manipulating information, which is not the same thing.

— "Disinformation" is the intentional dissemination of information that is wholly or partly false. It differs from "misinformation," which is unintentional. The problem, of course, remains that the intention is rarely clear,[13] and can only be assumed. This definition of the subject is probably the least bad from among the most commonly used terms. Still, it is both too broad and too narrow. It is too broad in the sense that it includes benign information that lacks a hostile intention. Needless to say, such benign information can have dire consequences: for example, in 1938, Orson Welles sowed panic in the United States with his radio adaptation of *The War of the Worlds* because the population came to believe in the possibility of an extraterrestrial attack. But intentionally disseminating false information is not in itself problematic: the focus should be on false information that has a negative effect or that is at least spread with a hostile intent. At the same time, the concept of disinformation is too narrow because the problems that we encounter are not all, strictly speaking, forms of disinformation. Sometimes information is not false, but simply exaggerated, biased or presented in a very emotional way, such as in a tabloid. Information can be manipulated in many ways: through the production, dissemination and even retention. These processes do not all imply a dichotomy between truth and falsehood. Most of the time, the manipulator does not position himself relative to the truth; he or she is simply trying to produce an effect. For this reason, reducing the problem to disinformation is misleading.

To account for this complexity, some experts, including the European Group of Experts, define disinformation as "false, inaccurate, or

12. Margarita Simonian, then the Editor-in-Chief of Russia Today and Sputnik, cited by Isabelle Mandraud, "Les médias, machine de guerre du Kremlin," *Le Monde*, 25 November 2015, p. 2.

13. Caroline Jack, *Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute, 2017, p. 4.

misleading information designed, presented and promoted to intentionally cause public harm or for profit"[14]— a definition that has been reused in various publications, including a report by the Irish government and a report from the Belgian Group of Experts.[15]

To us, it seems preferable to use the generic term, "manipulation," because it is more inclusive. Manipulation is intentional (its purpose is to cause harm) and clandestine (victims do not know they are being manipulated). We have chosen to focus our attention on "information manipulation" encompassing three criteria: a coordinated campaign, the diffusion of false information or information that is consciously distorted, and the political intention to cause harm.

The notion of a "coordinated campaign" refers less to the idea of an orchestrated operation with certain actors giving orders and others carrying them out. It refers more to a range of indicators pointing to the diffusion, through various media, of problematic content, by both human and non-human sources (Twitter, Facebook, bloggers, shared by institutional actors such as embassies, and by transmitters like RT, Sputnik, WikiLeaks, etc.)

By selecting this definition, we have chosen to highlight the political intent behind information manipulation campaigns as a defining criterion of the phenomenon. The political intent to harm is understood in a broad sense. It does not mean that the field is limited to political or national affairs. The campaign may seek to undermine the legitimacy of an electoral process, ruin the reputation of a large corporation abroad or create a hostile environment for an external military operation.

We are *de facto* excluding the numerous information manipulation attempts whose intention is neither political nor hostile from the scope of this study.

However, we must not overemphasize the distinction, as we sometimes do, between commercial manipulation, whose intention is to turn a profit and is thus often depoliticized by those who analyze it, and political manipulation, which is of interest to us here. Not only can the former have real political consequences, whether intended or not, but the latter may also be used to make money, for the media, digital platforms and even

14. European Commission, *A Multi-Dimensional Approach to Disinformation, op. cit.*, p. 10.

15. Government of Ireland, *First Report of the Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation*, prepared by the Department of the Taoiseach, June 2018 and Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, July 2018.

Macedonian adolescents.[16] In other words, there is an overlap between political and economic interests.

We have been advocating for the use of the expression "information manipulation" in our internal memoranda since the beginning of 2018. Minister for Europe and Foreign Affairs Jean-Yves Le Drian publically advocated for it in his speech on April 4 and, in May, an amendment was made to the proposed bill currently under consideration before the Parliament which allowed its name to be changed from "Against false information" (*contre les fausses informations*) to a law "relating to the fight against information manipulation" (*relative à la lutte contre la manipulation de l'information*). The French terminology is therefore coherent on this matter.

II. Is information manipulation a minor issue?

In 2013, the World Economic Forum listed online "misinformation" as one of the ten trends to watch in 2014[17]—which proved to be premonitory, given the non-negligible role that information manipulation played in the Ukrainian crisis. The subject has since only grown in popularity. All the polls confirm that it is now a major concern for populations, journalists, NGOs and governments around the world, who recognize the damages these types of manipulations can cause to society.[18] Moreover, awareness of this issue continues to grow, both in terms of scope (more and more countries are interested) as well as in depth (analyses are increasingly thorough).

However, there is also a common tendency to underestimate the effectiveness of information manipulation, and thus the importance of the subject. This tendency is less pronounced in countries that are traditionally more aware of the issue (Central, Eastern and Northern

16. One investigation revealed how the city of Veles, in Macedonia, had become a breeding ground for fake news and how the youth had, sometimes without any political motivation, *de facto* supported Trump in the American campaign, simply after having observed it was that most profitable choice (the pro-Trump content was shared more times, and therefore generated more publicity revenue. Some of them earned around US$5,000 per month, in a country where the average salary was less than 400 euros. (Craig Silverman and Lawrence Alexander, "How Teens in the Balkans are Duping Trump Suppporters with Fake News," *BuzzFeed News*, 4 November 2016). Today, some of them continue to mass produce fake news, but they earn much less because after the whole operation was discovered they were no longer able to sell to Google.

17. World Economic Forum, *Outlook on the Global Agenda 2014*, 2013, p. 28-29.

18. See for example the latest online public consultation conducted by the European Commission on fake news and disinformation online from November 2017 to February 2018 (*Synopsis report*, 26 April 2018) and *Reuters Institute Digital News Report 2018*, which surveyed over 74,000 people in 37 States.

Europe), or countries that were the most evidently targeted and whose ongoing parliamentary inquiries discuss this subject on a daily basis (the United States and the United Kingdom). However, countries who believe they are insulated, or who know they are targeted but have succeeded in fending off past attempts—such as France in the so-called "Macron Leaks" affair (see below)—are susceptible to underestimating the threat. Strong persuasion is then necessary, sometimes within government itself, and in public debates, to bring about the realization that this is no minor issue.

In order to do so, it could be helpful to state as a reminder, that information manipulation, although appearing virtual, has numerous, very real effects. In the last few years alone, it has interfered in the democratic processes of multiple states, including the presidential elections of the world's major powers, and destabilized large digital companies. Information manipulation has divided public opinion, and sowed doubt as to the veracity of the information provided by the media and reinforced a rejection of traditional media. It played a role in various diplomatic crises (Ukraine, Syria, the Gulf), and has also contributed to the saturation of digital spaces with troll communities that harass and intimidate internet users. Sometimes, information manipulation has gruesome consequences: information manipulation on Facebook, through false rumors and retouched photos, played a non-negligible role in the persecution of the Rohingya in Burma, which has since been described as "ethnic cleansing"[19] and possibly even genocide[20] by the United Nations. On a smaller scale, in only two months (May-June 2018) in India, dozens of people were lynched after having false information circulated about them. As a result, authorities decided to temporarily cut access to some online platforms.[21] The fact that many States are mobilizing and civil society is launching numerous initiatives to protect itself, as the disinformation economy continues to develop in parallel, with its troll factories, click farms and millionaire entrepreneurs,[22] is an indication of both the gravity and the effectiveness of information manipulation.

19. Annie Gowen and Max Bearak, "Fake News on Facebook Fans the Flames of Hate Against the Rohingya in Burma," *The Washington Post*, 8 December 2017.

20. UN Doc. A/HRC/39/64 (24 August 2018).

21. Shweta Ganjoo, "Hindustan or lynchistan? May be Indians should not be allowed to use WhatsApp," *India Today*, 2 July 2018.

22. See for example the case of Mexican Carlos Merlo, who claims to control millions of bots and dozens of sites. His entreprise, Victory Lab provides services such as "managing bots, containment, cyberattacks, and the creation of fake news sites" at prices ranging from 49,000 pesos (€2,256 at the time of writing) to a six-month contract at one million pesos (€46,000) per. See Ben

Nevertheless, the assessment of the effectiveness of information manipulation remains a challenge. No method is entirely satisfactory. During and after the Cold War, US intelligence agencies commissioned meticulous surveys in an attempt to accurately measure the permeability of targeted groups to Moscow's disinformation campaigns.[23] Today, the analysis of social networks provides valuable insights: it allows investigators to detect artificial and coordinated movements, to measure the number of viewers reached or the "infected tissue," after taking into consideration the automated accounts (bots). However, the number of viewers does not indicate whether those viewers are convinced by the false information or whether the information is going to have a behavioral effect (persuade someone to give their contact information or to give money, to protest, etc.) Furthermore, the number of viewers does not take into account the nature of those viewers: a message that reaches only 2% of the population could have a significant effect if those 2% are violent and ready to act.

Another limitation on the methodology is the reliance on textual analysis, whereas information manipulation can also occur through images, which are much more difficult to analyze automatically. Therefore, while it is crucial that attention be drawn to the role of platforms like Facebook, other networks (Instagram, WhatsApp) must also be examined. Disinformation through images also raises the issue of manipulation aimed at children.

Measuring the effectiveness of information manipulation is almost impossible because the link between a broadcast message and subsequent behavior involves too many other variables. However, we can distinguish the *impact* in the digital environment, which is relatively measurable and quantifiable (that is, if we manage to separate the real accounts from increasingly sophisticated bots), from the broader *effect,* which can merely be hypothesized. We can distinguish several effects.

Nimmo *et al.*, "#ElectionWatch: Trending Beyond Borders in Mexico," Atlantic Council's Digital Forensic Research Lab, Medium.com, 28 June 2018.

23. The Special Reports S issued by the intelligence community by the US Information Agency. The Department of Defense (via the Defense Intelligence Agency), the State Department and the CIA, like the USIA previously, consider social science studies an essential tool for the implementation of their respective strategies. The Office of Research and Intelligence (INR) produces dozens of "Special S reports," (surveys, case studies, impact assessment) and collaborates with many departments and academic research laboratories. These reports, once they are declassified, are available at the US National Archives: "Special 'S' Reports," Entry 1009, Record Group 306, Box 17, National Archives II, College Park, MD.

"We must not kid ourselves that it does not work. We know that it works, we have seen it at work abroad and also in France. Democratic process is thus profoundly distorted because the indignation that stems from this fake news is explosive and prevails over reflection. And that is the somewhat anthropological gamble made by those who manipulate these channels. […] Barriers have been raised but presidential campaigns in nearly all contemporary democracies have shown their weakness and our collective inability to bring responses equal to the scale of today's threats."

(Emmanuel Macron, President of France, New Year's Address to the Press, 4 January 2018.)

On the one hand, there is a direct effect. The question is whether information manipulation can succeed in generating new opinions or merely reinforce existing ones. From our investigation, it appears that manipulation does not generate new opinions, but sows doubt and confusion and, sometimes, facilitates action. In other words, sometimes information manipulation transforms a passive conviction into an active conviction—in a way that is similar to the process of radicalization. The act in question may be a vote.

On the other hand, there is an indirect effect. Information manipulation may tempt heads of government to infringe upon civil liberties. This could very well be the true end goal of the foreign powers behind information manipulation: not so much to convince a population of this or that story as to lead governments to take measures that are contrary to their democratic, liberal values, which, in turn, will provoke a reaction (from a different part of the political class and civil society). This ultimately contributes to the deepening of divisions within society. Therefore, it is important for the State to properly monitor its efforts against disinformation so as to respect civil liberties.

It appears, therefore, essential to have the means to conduct independent research into the science of information and communication, which will allow for the evaluation of the reception of information manipulation campaigns. In the meantime, immediate action is necessary, given the very real effect of these phenomena.

Part One

WHY?

Fighting effectively against information manipulation requires first and foremost to identify the roots of the problem. These roots are multiple and identifying them is a challenge of its own: there are individual causes, linked to human nature and thus tied to psychology and epistemology. There are cognitive weaknesses and a crisis of knowledge that makes us particularly vulnerable to information manipulation. There are also collective causes, related to the dynamics of social life, a crisis of trust in institutions, a crisis of the press and disillusionment with the digital world. Indeed, although the internet was supposed to liberate us, we instead find ourselves confined by it. After analyzing each of these causes, we will identify the beneficiaries, i.e. the actors conducting information manipulation, focusing in particular on state actors.

Information manipulation is particularly prolific in times of war—and thus benefits all the more from the "despecification" of war, that is, from the increasing ambiguity between times of war and times of peace. As French historian Marc Bloch noted in 1921 in an article analyzing the proliferation of fake news during the First World War, "emotion and fatigue destroy the critical faculty."[1] Censorship also plays a role, because it is more intense in moments of crises and it feeds into paranoia and delusions.

1. Marc Bloch, "Reflections of a Historian on the False News of the War", *Michigan War Studies Review*, 2013-051, translation by James P. Holoka, Eastern Michigan University, 1 July 2013, p. 10.

Marc Bloch on the causes of fake news (1921)

"The masses are aroused by false stories. Items of false news, in all the multiplicity of their forms—simple gossip, deceptions, legends—have filled the life of humanity. How are they born? From what elements do they take shape? How do they propagate themselves, gaining strength as they pass from mouth to mouth or writing to writing? […]

The historian who seeks to understand the origin and development of false news, disappointed by the reading of documents, will naturally think of turning to the laboratories of psychologists. […]

The error propagates itself, grows, and ultimately survives only on one condition—that it finds a favorable cultural broth in the society where it is spreading. Through it, people unconsciously express all their prejudices, hatreds, fears, all their strong emotions. Only great collective states of mind—I will have occasion to return to this later—have the power to transform a misperception into a legend.

[…] among the questions of social psychology that the events of the last few years can elucidate, those relating to false news are at the forefront. False news reports! For four and a half years, everywhere, in every country, at the front as in the rear, we saw them being born and proliferating. They troubled minds, sometimes overstimulating them and sometimes sapping them of their courage. Their variety, their strangeness, and their strength still astonish anyone who can remember and remembers having believed them.

[…] more often, false news in the press is simply a fabrication, crafted by the hand of a worker in a predetermined plan—to affect opinion or to obey an order—or simply to embellish a story with those curious literary precepts that impose themselves so strongly on modest publicists or with recollections of texts lying around: Cicero and Quintilian have more disciples in editorial bureaux than we commonly believe.

[…] an item of false news always arises from preexisting collective representations. It is fortuitous only in appearance, or, more correctly, all that is fortuitous about it is the initial incident, something that sets the imagination in motion. But this setting in motion occurs only because imaginations have already been prepared and are secretly fermenting. An event or misperception, for example, that does not go in the direction where all minds are already tending can at most constitute the origin of an individual error, not a popular and widespread instance of false news. If I may use a term which sociologists have given, for my liking, a too metaphysical value but which is convenient and, after all, rich in meaning, false news is a mirror wherein the 'collective consciousness' contemplates its own features."

(Marc Bloch, "Reflections of a Historian on the False News of the War, *Michigan War Studies Review*, 2013-051, translation by James P. Holoka, Eastern Michigan University, 2013, p. 2-10.)

Bloch cites a humorist from that era, writing that "The opinion prevailed in the trenches that anything could be true except what was allowed in print."[2] This same conviction is held today by a number of conspiracy backers. Indeed, Bloch's text is worth revisiting because it shows the extent to which the fundamental elements of the "fake news" debate have not changed.

I. Causes at the individual level

Targeting the individual and the collective at the same time, "modern propaganda is based on scientific analyses of psychology and sociology. Step by step, the propagandist builds his techniques on the basis of his knowledge of man, his tendencies, his desires, his needs, his psychic mechanisms, his conditioning—and as much on social psychology as on depth psychology."[3]

A. Cognitive failings

Disinformation exploits a natural intellectual laziness, characterized by the failure to systematically exercise critical thinking and choosing to relay information naively without looking for evidence to support that information. Conspiracy theorists demand that we provide evidence that their theories are incorrect and far-fetched, which is contrary to journalistic standards. As Emmanuel Macron reminds us, "The burden of proof has been reversed: while journalists constantly have to prove what they say—in accordance with the ethics of their profession, they must show what they say or write to be true—, those spreading fake news shout out: "It is your responsibility to prove that we are wrong!""[4]

We tend to favor information that confirms our preexisting assumptions, supports our positions and does not offend our sensibilities. This psychological phenomenon is commonly referred to as "confirmation bias." In the field of advertising, this weakness is well known and exploited: the success of an advertising campaign can be based on the commitment and constancy of an individual, that is to say his or her tendency to remain faithful to an opinion that is already formed.[5]

2. *Ibid.*
3. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes, op. cit.*, p. 4.
4. Emmanuel Macron, New Year's Address to the Press, 4 January 2018.
5. Joel J. Davis, *Advertising Research: Theory and* Practice, 2nd ed., Pearson, 2011.

Furthermore, all humans have the tendency to overestimate "their own memory and reasoning capacities, and to believe that they are more rational and more intelligent than they really are."[6] In this context "the widespread idea that reasoning works to seek out truth, good decisions, and must be impartial and objective" is false.[7] As Pascal Engel writes, "reasoning has not evolved in order to establish reality, but only as a means to win against our adversaries. We only reason for the purposes of competing in a social game, in which we systematically favor our own point of view and interests."[8] Information manipulation is just as natural as our own vulnerabilities in this regard.

A recent study showed that fake news spreads faster than accurate news for psychological reasons.[9] Real news is often not that new; it is often merely a confirmation of what we already know or suspect. It merely adds to the accumulation of knowledge, and is quickly forgotten. By contrast, fake news surprises; fake news is written to surprise and to go against the *doxa*. The novelty of fake news not only arouses greater interest, but also explains its greater diffusion by those who want to instruct others (a reputational dimension, social status, etc.). Furthermore, fake news is specifically tailored to go viral. It is written in a spectacular, emotional and often alarmist style, playing on fear and anxiety, elements that are generally not as prioritized in the realm of real news. It is therefore our cognitive biases that contribute in large part to the spread of fake news.

Advertising research has already identified several cognitive failures that a skilled advertiser can exploit: the consistency of an individual (confirmation bias); validation by social interaction (the individual will do what he thinks others do); the authority argument (the individual tends to obey authority figures, even when they demand the accomplishment of reprehensible acts); the illusion of correlation, as the individual perceives a connection between two events occurring within a similar timeframe; or preferences, as individuals are easily convinced by people they admire.

6. Pascal Engel, "Vous pensez être capable de détecter des 'fake news'… N'en soyez pas si sûrs" (interview), *Atlantico*, 7 January 2017.

7. Hugo Mercier and Dan Sperber, *The Enigma of Reason*, Harvard University Press, 2017, p. 129.

8. Pascal Engel, "Si on ne peut pas prouver que le monstre du Loch Ness n'existe pas, c'est qu'il existe…," *Libération*, 19 February 2018.

9. Soroush Vosoughi, Deb Roy and Sinan Aral, "The Spread of true and false news online," *Science*, 9 March 2018, p. 1146-1151.

B. An epistemological crisis

Information manipulation is only one of the manifestations of a much larger phenomenon that integrates pseudoscience—particularly in the fields of medicine and biology—, historical revisionism, and conspiracy theories. In the academic world, we are equally witnessing an upsurge in counterfeiting: there are thousands[10] of fake scientific journals and publishing houses who publish articles and books without evaluating them first and charge researchers to be published. Researchers receive more and more spam from these "editorial predators." Some countries have been particularly affected, such as Kazakhstan and Indonesia. The phenomenon was studied by a coalition of international media corps, who dubbed it "Fake Science."[11]

In 2008, British writer and journalist Damian Thompson already alerted the public of a "pandemic of credulous thinking" and the decline of Enlightenment values in the face of "counterknowledge."[12] The fact is that "We are now facing a situation in which a large share of the populace is living in an epistemic space that has abandoned conventional criteria of evidence, internal consistency, and fact-seeking. It follows that the current state of public discourse can no longer be examined through the lens of misinformation that can be debunked, but as an alternative reality that is shared by millions."[13]

In 2013, sociologist Gerald Bronner wrote a book on the growing gullibility of our democracies, describing it as the "soft stomach of our contemporary rationalism in which irrationalism effortlessly carves itself out a very consequential and paradoxical place."[14] He views this development as the result of a combination of two elements: on the one hand, the liberalization of the information market in which rational sources must compete with irrational sources, as well as the fact that this competition favors the "believers" who are "generally more motivated than the non-believers to defend their point of view and dedicate their

10. American documentarian Jeffrey Beall counted 11,000 fake scientific journals (beallslist.weebly.com).

11. Stéphane Foucart and David Larousserie, "Alerte mondiale à la fausse science," *Le Monde*, 19 July 2018.

12. Damian Thompson, *Counter-Knowledge: How we surrendered to conspiracy theories, quack medicine, bogus science and fake history*, Atlantic, 2008.

13. Stephan Lewandowsky, Ullrich Ecker and John Cook, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," *Journal of Applied Research in Memory and Cognition* 6:4, 2017, p. 360.

14. Gérald Bronner, *La Démocratie des crédules*, PUF, 2013, p. 86.

time to it."[15] On the other hand, he notes the intellectual laziness of media users, who easily succumb to various cognitive biases, including confirmation bias.

For Olivier Schmitt, the current epistemological crisis stems from "the intertwining, in the public space, of adulterated versions of three epistemological approaches."[16] The first is the Cartesian doubt which is turned into a systematic doubt that can feed conspiracy theories. The second is the relationship between knowledge and power: loosely quoting Foucault, one can state that "all manufactured knowledge inherently benefits to the most powerful." The third is deconstructionism, an approach which, according to the writings of Derrida, seeks to unveil unsaid things. In its adulterated version, deconstructionism aims to systematically deconstruct a "dominant speech." All in all, the contemporary epistemological crisis lies in the wrong interpretation, the diversion and the simplification of otherwise legitimate approaches.

A phenomenon from the Right or the Left?

If the majority of studies, in the United States at least, show that the right-wing is most often—but of course not exclusively—the source of fake and biased news, it is due to the fact that progressive citizens generally consult a larger variety of sources of information and are more trusting towards professional journalism, while conservatives have a stronger tendency to consult sources and networks that conform with their political opinions, and tend to maintain an anti-media, anti-intellectual bias. This equally holds true for European right-wing populism. Because of these vulnerabilities, people holding right-wing convictions seems more susceptible to fall victim to fabricated information "because they seem to be more systematically targeted by those looking to strategically exploit them."[17]

15. *Ibid.*, p. 76. See also Dominique Cardon, *La Démocratie Internet. Promesses et limites*, Seuil, 2010.

16. Olivier Schmitt, "'Je ne fais que poser des questions'. La Crise épistémologique, le doute systématique et leurs conséquences politiques," *Temps présents,* 15 June 2018.

17. Jayson Harsin, "Un guide critique des *Fake News* : de la comédie à la tragédie," *op. cit.,* p. 116.

In the early 1960s, philosopher Karl Popper outlined his "conspiracy theory of society." According to this theory, "there is a view, which I shall call the conspiracy theory, which holds that the explanation of any social phenomenon consists in finding out who is interested in the occurrence of this phenomenon. This view arises, of course, from the mistaken theory that, whatever happens in society—especially happenings such as war, unemployment, poverty, shortages, which people as a rule dislike—is the direct design by some powerful individuals and groups."[18]

Conspiracy theories amplify a natural tendency we harbor, namely to believe that every effect is caused by intentional action, especially those effects that benefit certain people. For this reason, conspiracy theories are inevitable and feed mostly on crises and violent events. Fortunately, not all are dangerous. Some are harmless. But others can have destabilizing effects, even if they are only shared by a very small percentage of the population, as long as that small minority is ready to take violent action. Radicalism and world views fueled by conspiracy theories often go hand-in-hand.

Most conspiracy theorists are neither foolish nor irrational but simply lack good sources of information. The theories they defend are unjustified in light of *all* the information available, but not according to the sources they consult, which make these arguments seem plausible. The cause of the problem is the epistemic poverty of their environments. To a certain extent, this is also true of extremism, in general, which some authors say suffers from a "crippled epistemology."[19] Therefore, one of the solutions is the "cognitive infiltration of extremist groups" using physical or virtual means to sow doubt and distrust in their minds by the introduction of explanatory diversity.[20]

Conspiracy theorists pose a particular difficulty because they are highly resistant to debunking, especially if attempted by the State. As conspiracy theories hold that certain people have disproportionate power with which to conceal their actions, these attempts can become absorbed into the narrative of the plot.

Hence, we are experiencing a crisis of knowledge, an epistemological crisis—although this is nothing new. It was already present during Plato's

18. Karl Popper, *Open Society and Its Enemies, Vol. II: The High Tide of Prophecy* (5th ed.), Princeton University Press, 1966, p. 306.

19. Russell Hardin, "The Crippled Epistemology of Extremism," in A. Breton, G. Galeotti, P. Salmon & R. Wintrobe (eds.), *Political Extremism and Rationality*, Cambridge University Press, 2002, p. 3-22.

20. Cass R. Sunstein and Adrian Vermeule, "Conspiracy Theories: Causes and Cures," *The Journal of Political Philosophy*, 17:2, 2009, p. 219.

fight with the sophists, whom he reproached for not being interested in the truth, but only in conviction. They did not aim for knowledge (*episteme*), only for opinion (*doxa*). Never before today has the distinction between *episteme* and *doxa* been so threatened—and through it, the very possibility of knowledge. The era in which we currently live is very different from the epistemological crises of the past. We find ourselves not in an ideological era, in which we replace one truth with another, but rather in a skeptical or relativist era, where we question the very existence of truth.

On 16 November 2016, the Oxford dictionaries declared the term "post-truth" to be the word of the year. Between 2015 and 2016, its usage increased by 2000%.[21] "Instead of undermining truth at its very core by trying laboriously to replace that truth with another through a massive effort of manipulation and surveillance, [the post-truth] disqualifies truth at its outset and upstream. The post-truth imposes no particular truth and it is precisely in this way that it sows confusion and doubt. In this respect, the post-truth expertly accommodates dissension and criticism by not allowing 'alternative facts' to multiply, even when they contradict one another."[22]

II. Causes at the collective level

A. The crisis of confidence in institutions

A survey of more than 33,000 people in 28 countries in November 2017 showed that distrust of institutions was on the rise, with the media ranking first in terms of the least trusted institution, while trust in social media platforms was decreasing, but trust in journalism was increasing. In addition, almost 70% of the population reported feeling worried about the weaponization of fake news. This percentage was highest in Mexico, Argentina, Spain and Indonesia (76-80%) and lowest—though still significant—in France, Sweden and the Netherlands (55-60%).[23] "What is the fake news in circulation telling us? It speaks of the treachery of elected officials, the media's appropriation of public discourse and a number of

21. Sabrina Tanquerel, "Quand l'exigence de vérité devient secondaire," *The Conversation*, 12 February 2017.

22. Sebastian Dieguez, *Total Bullshit ! Au cœur de la post-vérité*, *op. cit.*, p. 307. See also Julien Nocetti, "La guerre de l'information. Comment l'information recompose les relations internationales. La faute à Internet ?" IFRI (ed.), *RAMSES 2018. La guerre de l'information aura-t-elle lieu ?,* Dunod, 2018.

23. 2018 Edelman Trust Barometer, Global Report.

anxieties tied to globalization. In this sense, fake news is an expression of a virulent defiance towards the political and intellectual elite."[24]

Information manipulation is both a cause and a symptom of the crisis of democracy, which is evidenced by the growing abstention in elections, distrust towards elected officials and even questioning of democratic and liberal values. The depreciation of the truth is one of the manifestations of this crisis of confidence—but at the same time, the devaluation of truth propagates the crisis of confidence. This crisis is due to circumstantial factors, including the financial crisis of 2008-2009, as well as root causes:

1. The rejection of the elites. From the United States to the Philippines to Hungary, hatred for the establishment seems to be a passion that is shared by all populist outsiders, real or purported.

2. The polarization of identity. In response to the porous borders and the cultural blending that globalization engenders, there is an increasing demand for the reaffirmation of "us" against "them." This tendency includes phenomena such as the erection of walls (Israel, the United States, Hungary), the expansion of gated urban communities, the imposition of refugee quotas, etc.

3. The subversion and diversion of democratic institutions. Governing parties tend to transform the nature of the rule of law that they inherit from within (subjugation of the judiciary in Poland, strengthening of police powers through special laws in Turkey, criminalization of the opposition and certain NGOs in Russia and Israel). The use of the plebiscite makes it possible to legitimize continued rule by the executive beyond the time allowed under the constitution (third terms in Venezuela, Burundi and the Congo).

4. The "barbarization of the bourgeois" in times of crisis.[25] Populist leaders or "new demagogues" most often position themselves as the champions of middle-classes driven by growth (in emerging countries) or terrified of losing their status (in OECD countries).

5. A global crisis of political communication. The explanation for this crisis of *logos* that deeply endangers the public space is twofold: the development of a conspiracy-driven, transnational blogosphere that plays into the hands of propaganda and the spread of disinformation by certain anti-liberal regimes and movements.

---

24. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, FYP editions, 2017, p. 44.

25. Pierre Hassner, "Le Barbare et le Bourgeois," *Politique internationale*, 84, Summer 1999, p. 90-91.

B. The crisis of the press

The phenomenon commonly referred to as "the crisis of the press" generally manifests itself in two ways: through a crisis of the economic model and a crisis of norms.[26] The crisis of the economic model is not new and is largely the result of the decrease in press advertising revenues, due to the competition it first faced from the advent of television, and then later on with the invention of the internet. The shift over to digital media hardly provided compensation: digital publicity is less lucrative than both print and television. Many agencies and news organizations have had to lay off journalists, doll out severance payments and terminate certain news outlets. This precarious situation renders the press even more vulnerable to information manipulation, because there are less people and less time to detect them and because of the premium placed on quantity rather than quality.

Nevertheless, new economic models are constantly cropping up, and are paid for by subscriptions and the diversification of revenue sources (with expansions in event planning, for example)—sometimes with such success that one might even say the press is "in a state of reinvention, rather than crisis."[27] *The New York Times* is a perfect example of this: the newspaper made over a billion dollars in annual revenue from 2017, thanks to subscriptions.[28]

As for the crisis of norms, this challenge is largely a result of the rise of social media (see below), whose equalizing power allows anyone to spread information without respecting journalistic standards or spread discourses that are sometimes extremist and hateful, much like trolls do (see below). Nevertheless, there is room for hope in this case too, namely because these excesses generate fatigue within the population, which prompts more serious media outlets, eager to demonstrate their added value, to strengthen journalistic norms and to value investigative journalism, which produces papers that are longer and more complex, and sometimes collaborative.

26. Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," Alliance for Securing Democracy (GMF) Brief 2018 No. 009, March 2018, p. 2.

27. Intreview with Jean-Marie Charon, *Télérama*, 18 March 2017.

28. Sydney Ember, "New York Times Co. Subscription Revenue Surpassed $1 Billion in 2017," *The New York Times*, 8 February 2018.

C. Digital disillusionment

Information manipulation has always existed but was accelerated by three technical innovations: print, mass media, and the internet. The internet, in particular, became even more of an accelerant in the last decade with the rise of social media.

The digital revolution—in particular, the accessibility of broadband in the last fifteen years—and the subsequent development of social media (MySpace in 2003, Facebook in 2004, Twitter in 2006) have changed the playing field. Social media has become omnipresent in the lives of billions of individuals. (As of June 2017, Facebook has more than 2 billion active users, Youtube 1.5 billion, Instagram 700 million and Twitter 328 million.) Social networks are used as a source of information by 62% of American adults and 48% of Europeans.[29] Google and Facebook now account for more than 70% of web traffic, which means that other sites, including news organizations, get most of their audience from these platforms. These platforms have become the gatekeepers of the web. At the same time, they generate massive advertising revenues.

Initially, the dramatic growth of social networks—and in particular, the Web 2.0, blogs and citizen journalism—has brought many to believe in the emancipation of the people from their States.[30] The Arab Spring exemplifies this idea, albeit at the risk of exaggeration (many spoke at the time of a "Facebook revolution" or a "Twitter revolution"). This optimism was followed by disappointment several years later, beginning with the Snowden Affair (2013) which revealed (or rather confirmed) that States had not renounced their strong grip over society. Beginning in 2016, there was also a series of interferences in democratic processes (the Dutch referendum on the association agreement between Ukraine and the European Union, Brexit, the American presidential election, the French presidential election).

The exponential development of digital platforms has considerably increased the risk of information manipulation in several ways:

- the overabundance of information, a phenomenon known as "infosaturation" or "infobesity." "[T]he average American is exposed to about five times as much information [as] in 1986."[31] In turn, information

29. *Reuters Institute Digital News Report 2016*.

30. François-Bernard Huyghe, "Que changent les *fake news* ?," *La Revue internationale et stratégique*, 110, February 2018, p. 79.

31. Daniel Levitin, Author of *Weaponized Lies: How to Think Critically in the Post-Truth Era*, cited in Eoin O'Carroll, "How information overload helps spread fake news," *The Christian Science*

overload contributes to disinformation because it leads to decreased concentration, which weakens our vigilance and our ability to process counter-arguments.[32] This assertion is nothing more than the application of a well-known truth from the field of psychology to the digital realm: too much information is detrimental to decision-making.

• the number of vectors available to diffuse false information (potentially as many as there are users of these networks or, in other words, billions);

• the increased precision with which the population is segmented and targeted (micro-targeting)—the most vulnerable targets are the youngest populations (17-25 years of age);

• the low cost of this diffusion (a few clicks, a few minutes) and the facility with which one can create a seemingly reputable website (the ease with which one can make a blog, a webpage or a website look professional);

• the horizontality of social media, which allows anyone to broadcast content to others without passing through an editorial control body;

• the fact that the internet has no borders and, therefore, foreign powers can easily infiltrate communities and spread fake news;

• the technical progress in tailoring photo, video and audio content to look increasingly like reality, which in turn makes it harder to detect modifications.

As Ben Nimmo concludes, "the spread of digital publishing technologies has made it easier to *create* false stories. The internet has made it easier to *publish* fake stories, and social media have made it easier to *spread* false stories."[33] In 2005, before the rise of the main social network platforms, one could already write that "everyone's a reporter."[34] This trend has only intensified.

The speed of propagation has thus considerably increased. It took the KGB nearly four years to spread the rumor that the AIDS virus was created by the Pentagon. (This fake story was planted in an Indian newspaper in

Monitor, 27 June 2017.

32. Xiaoyan Qiu *et al.*, "Limited individual attention and online virality of low-quality information," *Nature Human Behaviour* 1, article number 0132, 2017.

33. Ben Nimmo, for his hearing before the Singaporean Parliament (Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures, written representation 26, 22 February 2018).

34. Lucas Grave, "Everyone's a reporter," *Wired Magazine*, 9 January 2005.

1983 but only reached the Soviet press in 1985 and the Western media in 1987.) Today's social networks have succeeded in reducing this time to a few minutes or hours, as demonstrated by the "Macron Leaks" incident (see below). One might think that it is only a change of level. However, as stated by the Minister for Europe and Foreign Affairs Jean-Yves Le Drian, "there are spheres—such as the informational domain—in which the change of level is actually a change of nature."[35]

To increase the time that users spend online, platforms have developed technologies that, for example, match us with the sponsored content that is most likely to make us react and click to continue browsing (matching technique). This poses several problems:[36]

1. This encloses internet users in "filter bubbles." Search engines and social networks use personalization algorithms. As of 2010, the search results in Google are not the same for all users; they depend on the preferences of the user as deduced from his or her search history and geolocation. Originally, these algorithms served a commercial purpose by offering the user results as close (in every sense of the term) to their expectations as possible. But this practice also had the perverse effect of cocooning internet users "in closed cognitive spaces where they were only exposed to content that supported their beliefs. The engine would become a tool of confirmation rather than information."[37] It was in the context of denouncing this kind of confinement that Eli Pariser coined the term "filter bubble" in 2011.[38] Facebook and other social networks do the same thing. The problem is that for most users, these platforms are the "gatekeepers" of the web, the access routes to the rest of the internet. These personalization algorithms close people in cocoons, comfortable cognitive spaces that confirm prejudices rather than confront them with the prejudices of others. This problem of "filter bubbles" amplifies our sociological and cognitive biases, in particular our "confirmation bias." As already stated, we do not like to be contradicted, and these platforms' content-creating algorithms ensure that we are not, by providing us with information that bolsters our opinions. Paradoxically, the digital revolution may actually be pushing us to close us back in on ourselves.

35. Jean-Yves Le Drian, Speech of 4 April 2018.

36. We thank the General Secretariat of the French Digital Council for its contribution to the following analysis.

37. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 33.

38. Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2011.

This phenomenon has contributed to the political "surprises" of 2016, such as the fact that almost no one seems to have anticipated Brexit and Trump's election. In a famous article entitled "How technology disrupted the truth," Katharine Viner, the Editor-in-Chief of the *Guardian*, demonstrated how this occurred in the case of Brexit.[39] A few months later, in an article with an evocative title—"There are 58 million pro-Trump voters and I have not seen any of them"—Julien Cadot produced a similar analysis of the election of Trump.[40]

2. This also creates the phenomenon of "cascading information:" users relay information posted by their close contacts without necessarily checking or even considering whether that information is true. The more the information is shared, the more we tend to trust it and the less we use critical thinking to assess it.

3. This phenomenon favors the most interesting or scandalous content because that is most likely to make us react, regardless of truth or accuracy. This model contributes to the polarization of public opinion by reducing the visibility of nuanced content, which is considered to be less engaging. This business model is optimized for profit rather than truth: it valorizes "fake news."

4. This setup triggers a race to capture users' attention. Platforms invest huge amounts of money in studies of what it is that attracts our attention and produces weaknesses of will.

For all of these reasons, journalistic ethics, the traceability of sources and the verification of facts are sacrificed in order to make something go viral. This race to the number of page views, to increase advertising revenues and to attract investors corrupts press companies at the expense of serious journalism. It encourages lurid titles, sensationalism, clickbait to the detriment of the truth.

III. Who manipulates information and why?

The vulnerabilities identified in the previous pages constitute fertile ground for information manipulation. On their own, however, they do not explain the current situation. These vulnerabilities are used by actors who perceive them as opportunities to defend their strategic interests.

39. Katharine Viner, "How technology disrupted the truth," *The Guardian*, 12 July 2016.

40. Julien Cadot, "Bulles de filtrage : il y a 58 millions d'électeurs pro-Trump et je n'en ai vu aucun," numerama.com, 9 November 2016. See also Matthew Hughes, "How the Internet tricked you into thinking Trump wouldn't win," *The Next Web*, 9 November 2016.

Who are these actors? They are diverse: ranging from the more or less lone individual to states and non-state groups and corporations. All types of actors manipulate information. This report focuses on a particular type of manipulation conducted by a particular actor: information manipulation of state origin targeting the population of another State, or in other words, interference. However, we will begin by examining other scenarios of information manipulation.

A. Non-state actors

The report concerns itself with non-state actors primarily in their role as a relay, or sometimes a stimulus, of information manipulation by States. However, information manipulation techniques are also used by non-state actors acting on their own behalf to promote their own agendas. Two case studies can provide interesting insight in this regard: jihadist groups, which testify to the role of information manipulation in terrorism; and ethnic and/or religious communities that, when used and/or manipulated, weaken some States, particularly in Asia or Africa. The case of nationalist and/or populist movements within our Western democracies, which played a role in Brexit, the election of Donald Trump and the recent French presidential election, are a separate category. Those efforts stemmed from a different logic as the agenda of these movements overlapped with those of state actors. As the so-called "Macron Leaks" will be the subject of a separate chapter (see below), we will first consider the examples of the first two instances.

1. Jihadist groups: the case of ISIS

Al Qaeda had already recognized the opportunities to carry out terrorist operations in the virtual sphere. In 2005, Ayman al-Zawahiri said, "we are in a battle and more than half of this battle is in the media. In this media battle we are in the race for the hearts and minds of our Umma [the Muslim community]."[41] Ten years later, the Geneva Center for Security Policy estimated that ISIS' campaign on social media had attracted more than 18,000 foreign soldiers from more than 90 countries.[42] The groups'

41. Christina Schori Liang, *Cyber Jihad: Understanding and Countering Islamic State Propaganda,* The Geneva Centre for Security Policy, Policy Paper 2015/2, February 2015, p. 2.

42. *Ibid.*

jihadist propaganda apparatus is one of its major forces at a time when its armed forces are being defeated in Syria and in Iraq.

The propaganda used by ISIS is multidimensional, multi-vectored and carefully targeted. It is multidimensional firstly because it is based on a simple, conspiratorial vision of a Manichean world to explain our social lives. Media content includes history lessons (rewriting the Sykes-Picot agreement,[43] colonization, the 2003 Iraq intervention) and news articles (on coalition action, Iran). It also involves BBC-type reports presented by John Cantlie, a hostage-reporter, speaking about such things as the good living conditions in Mosul.[44] It further includes theology courses, based on extremist readings of religious texts. The broadcasts serve as attractive reading and viewing material for the main targets of this group: young people in the midst of an identity crisies.[45] ISIS propaganda pairs speeches that are supposedly truth-oriented with more emotional elements—a combination which allows the group to acquire discourse credibility and conquer "the hearts and minds" of their disciples.[46]

ISIS propaganda is also multi-vectored. ISIS' communication agency, AMAQ, is highly active. The group communicates through its media center Al-Hayat[47] and the "jihadosphere" has experienced significant development since the official proclamation of the caliphate in 2014. Henceforth, the so-called Islamic State not only has websites, chat rooms and online journals, but it also makes extensive use of social networks, blogs, instant messengers, video sharing sites, Twitter, Facebook, Instagram, WhatsApp, Tumblr, etc. The group is also active on Telegram and on specialized forums (terror forums) as well as on the Darknet, where terrorist operations can be organized and coordinated. This diversity of the means of dissemination also makes use of a variety of formats: videos, articles, songs, reports, memes, etc. ISIS claimed responsibility for the attacks of November 2015 in Paris via an official written statement, which was also repeated in song to a much younger audience. In doing so,

43. James Renton, "Décrypter Daech : le califat et le spectre des accords Sykes-Picot," *The Conversation*, 4 March 2016.

44. In a video published by the Islamic State in January 2015, the reporter proposed a tour of the city. The video appeared to be a direct response to an article by *The Guardian*, which stated that the residents of Mosul lacked water, food and electricity. John Cantlie presented the city as pleasant despite the conflict, repeating that there were no power outages in the area.

45. Xavier Crettiez and Romain Sèze, *Saisir les mécanismes de la radicalisation violente : pour une analyse processuelle et biographique des engagements violents,* Research Report Rapport for the *Mission de recherche Droit et Justice*, April 2017.

46. Kierat Ranautta-Sambhi, in NATO Stratcom COE and the King's College London, *Fake News. A Roadmap,* January 2018, p. 51.

47. Christina Schori Liang, *Cyber Jihad*, *op. cit.*, p. 2.

the Islamic State is building a propaganda apparatus capable of attracting diverse audiences.

These audiences are subject to meticulous targeting that seeks primarily to exploit the social, economic, political and cultural vulnerabilities of certain communities. The multiplication of memes and terrorist videos suggests that young people are the principal target of the conspiracy theories spun by the so-called Islamic State. ISIS offers these vulnerable young people answers to the challenges that come with entering the professional world and building an adult identity.[48] ISIS uses individualized targeting at an unprecedented level.

2. Ethnic and/or religious communities: the Indonesian case

The Indonesian case seems fairly representative of the way in which information manipulation targeting ethnic and/or religious communities occurs. In Indonesia, disinformation generally focuses on such topics as the increase in the number of Chinese immigrants (which has actually increased but not by nearly as much as this false information claims it has). It also focuses on the ethnic and religious origins of leaders (such as during the 2014 presidential election, when Jokowi was accused of hiding his Chinese origins and of being a Christian). The problem also arose in 2012 and more recently in 2017, during the gubernatorial elections in Jakarta, which sparked numerous disinformation campaigns attempting to set Muslims against Indonesians of Chinese origin—an old antagonism in the country. One of the main targets was the then governor, Basuki Tjahaja Purnama (the first Christian of Chinese origin to hold this post), who was accused of blasphemy. The campaign had serious consequences: hundreds of thousands of Muslims took to the streets to protest and Basuki Tjahaja Purnama was sentenced to two years in prison.

Disinformation also pollutes daily life with tangible problems: several temples and pagodas were destroyed in 2016 in North Sumatra following the spread of a false rumor on social networks that a Chinese woman complained about the call for morning prayer. The following year, in West Kalimantan, an innocent man was beaten to death by a mob following a false rumor—but a more sophisticated one as it used the police logo—that a child kidnapping scheme had taken place. A

48. Xavier Crettiez and Romain Sèze, *Saisir les mécanismes de la radicalisation violente : pour une analyse processuelle et biographique des engagements violents, op. cit.*

group called *Saracen* had been paid to conduct online campaigns against different ethnic and religious groups. By the time the group was arrested in August 2017, its members had already succeeded in exacerbating anti-Chinese sentiment. The group controlled 800,000 accounts on social networks.

Indonesia's vulnerability stems from a population that is poorly educated and highly polarized (along ethnic and religious lines). Indonesian disinformation, however, remains domestic: the ecosystem is largely isolated from the rest of the world by its language, Bahasa, and thus remains relatively sheltered from foreign attempts at interference.

The president has since declared "war" on fake news and civil society has launched a number of initiatives to detect fake news, such as *TurnBackHoax*. The government has also created a National Cyber Encryption Agency to counter religious extremism and fake news online.

B. States

In the face of the social movements launched by or with the aid of digital platforms, in particular Twitter and Facebook, authoritarian governments have had two successive reactions. They initially reacted with a strategy of information scarcity, by censuring content and blocking access, as was witnessed in numerous examples from the early 2000s in China, North Africa and the Middle East. These authoritarian governments nevertheless quickly became aware of the potential for these technologies to surveil and influence their own citizens. Therefore, the second generation in internet control of the population, in contrast to the first, actually benefitted from the overabundance of information. Today, these States find themselves in the paradoxical position of using "the same tools they once perceived as a threat to deploy information technology as a means for power consolidation and social control, fueling disinformation operations and disseminating government propaganda at a greater scale than ever before."[49]

The latest annual report from Freedom House on online freedom[50] shows that more and more States are manipulating information on social media, using trolls, bots or fake sites. The NGO denounced the actions of 30 governments (compared to only 23 countries denounced in the

49. Carly Nyst and Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, Institute for the Future, 2018, p. 8.

50. Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, November 2017.

previous year) and stated that, in 2016, manipulation and disinformation online played an important role in the elections of at least 18 States. The case of the United States was peculiar in that it revealed that another State, Russia, had used manipulation to advance its interests and influence abroad. In reality, there are two kinds of manipulation by States: the most common which is manipulation directed at a State's own population in order to control it; and manipulation directed at the population of another State, which constitutes interference, and is the focus of this report.

1. Manipulation targeting the local population

In most cases, governments manipulate the information given to their own people in order to strengthen and solidify their power. They use control techniques such as those developed by China and Russia which have become a "global phenomenon," according to the President of Freedom House.[51]

"Trolling" is one of these techniques, and its usage is growing increasingly common. There is increasing reference to a "new phenomenon," defined as "the State use of targeted hate campaigns and online harassment to intimidate and silence individuals who criticize the State."[52] There is no shortage of case studies—not only in Russia and China (the famous "50 cent army," composed of more than 2 million people, posting nearly 450 million comments per year)[53] but also in Iran (where the intelligence services and the Revolutionary Guard draw support from a network of 18,000 "volunteers" to surveil social networks);[54] in Mexico (where "Peñabots" refers to bots serving President Enrique Peña Nieto);[55] in India (the BJP, currently in power, supposedly has an "IT Cell");[56] in Vietnam (in December 2017, the government launched a

51. "De plus en plus de gouvernements manipulent les réseaux sociaux," AFP, 14 November 2017.

52. Carly Nyst and Nick Monaco, *State-Sponsored Trolling*, *op. cit.*, p. 1. See also Michael Riley, Lauren Etter and Bibhudatta Pradhan, *A Global Guide to State-Sponsored Trolling*, Bloomberg, 19 July 2018.

53. 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*, 111:3, 2017, p. 484-501.

54. RSF, *Online Harassment of Journalists: Attack of the trolls*, 2018, p. 27.

55. Erin Gallagher, "Mexican Botnet Dirt Wars: Bots are waging a dirty war in Mexican Social media," media.ccc.de, August 2015.

56. Swati Chaturvedi, *I am a Troll: Inside the Secret World of the BJP's Digital Army*, Juggernaut Publication, 2016.

brigade known as the "Force 47" composed of 10,000 cyber-inspectors);[57] in Argentina (President Mauricio Macri is also said to have access to an "army of trolls");[58] in South Korea (where a psychological war unit in the National Intelligence Service supposedly paid millions of citizens to denigrate the liberal candidate and support the conservative candidate in the presidential campaign of 2012);[59] in Turkey (where an army of 6,000 "AK Trolls"—named after the party—were trained by the regime in response to the protests of 2013);[60] as well as in the Philippines, where the campaign that led to the election of Rodrigo Duterte was described as a prime example of "patriotic trolling," in which "government-backed actors fuel existing social media campaigns, manipulate public biases, and leverage online abuse for offline intimidation."[61] Duterte's team attacked anyone who criticized them: "By making an example of one citizen, one politician, one journalist, all brutally attacked online, it created a chilling effect that made many others afraid to speak out"—what is known in communications theory as a "spiral of silence."[62]

The practice of trolling—which can be more or less state-led depending on the degree of control the State has on trolls—is but only one of many tools at the disposal of "cybertroops," defined as "teams belonging to the government, the army, or political parties, whose mission is to manipulate public opinion via social media."[63] Many States, including democratic ones, have made use of these tactics, although it is quite obvious that all these structures do not have comparable activities.

The object of this report is not to identify all the information manipulation implemented by States against their own population—that falls to the lot of human rights NGOs—but to analyze those attempts aimed at foreign populations (attempts at interference) targeted, above all, at our democracies.

57. RSF, *Online Harassment of Journalists: Attack of the trolls*, *op. cit.*, p. 28.

58. "Trolls: cómo funciona el ejército de perfiles macristas truchos que denuncian Tinelli y la oposición," politicaargentina.com, 15 July 2016.

59. "Ex-intelligence official arrested for 2012 election-meddling," *Korea Herald*, 19 September 2017.

60. RSF, *Online Harassment of Journalists: Attack of the trolls*, *op. cit.*, p. 25.

61. Carly Nyst, "Patriotic Trolling: How governments endorse hate campaigns against critics," *The Guardian*, 12 July 2017.

62. CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, Ottawa, February 2018, p. 84-85.

63. Samantha Bradshaw and Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Working paper no. 2017.12, University of Oxford, July 2017, p. 3.

2. Manipulation targeted at a foreign population

This category concerns far fewer States. In the following section, we will only look at the two most important ones: firstly, Russia and, to a lesser extent, China. This does not mean, of course, that only these two States manipulate information outside of their borders. Other States also do it, or attempt to do it, but with much less success and far fewer means in the international arena than the two mentioned above.

a. Russia

There is no "Russophobia" in the observation that all recent interference attempts in referenda (the Netherlands, Brexit, Catalonia) and elections (the United States, France, Germany) are tied, directly or indirectly, to Russia. Our interlocutors among European authorities attribute 80% of influence efforts in Europe to Russia. The remaining percentage comes from other States (mainly China and Iran) and non-state actors (Jihadist groups, in particular ISIS).[64] Consider the example of the 2017 French presidential election. An analysis of the 800 most visited sites during the campaign and the nearly 8 million links shared between November 2016 and April 2017 "only identified foreign influence connected with Russia. No other foreign source of influence was detected."[65] The practice was even recognized by numerous Russian officials and theorists, who have underlined how information is being used as a means to politically intimidate or destabilize, in order to fulfill strategic objectives (see below).

For a number of countries that have been exposed for many years—Baltic and Scandinavian countries, Central and Eastern European countries—this trend is nothing new. These States have long been the targets of information manipulation campaigns. However, until 2014, their concerns were not heard, as attempts to bring attention to this phenomenon were only met with indifference and even irritation from the "great" powers of Western Europe. Their attempts were even described as anti-Russian "hysteria." Everything has changed since then.

Western political leaders no longer hesitate to call out Russia actions. In her annual speech before the Lord Mayor of London in November 2017, Theresa May took direct aim at Russia: "I have a very simple message for Russia. We know what you are doing. And you will not succeed. Because you

64. Interview in Brussels, 26 September 2017.

65. Bakamo, *2017 French Election Social Media Landscape: The Role and Impact of Non-Traditional Publishers in the French Elections 2017*, 19 April 2017, p. 18.

underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us."[66] She accused Russia of multiple wrongdoings, including the annexation of Crimea, the conflict in the Donbass, several violations of European countries' airspace, cyberattacks and election interference. The 2017 Swedish National Security Strategy also accused Russia of waging, in Sweden and in several other Western countries, influence operations "to sow discord, create uncertainty and influence political decision-making processes and choices."[67] Defense Minister Peter Hultqvist adopted the same position, denouncing "the Russian aggression in eastern Ukraine," and the fact that Russia uses "disinformation and propaganda operations."[68]

When the head of the German domestic intelligence service (*Bundesamt für Verfassungsschutz)* identified other oncoming attacks a few days before the 2017 federal elections, he immediately pointed the finger at Moscow: "We recognize this as a campaign being directed from Russia. Our counterpart is trying to generate information that can be used for disinformation or for influencing operations."[69] In its report on disinformation, the Canadian Security Intelligence Service (CSIS) considered that Russia is "the most skillful national purveyor of falsehoods."[70] The French Minister for Europe and Foreign Affairs has also mentioned "the campaigns orchestrated from Russia against Emmanuel Macron."[71]

Moscow is certainly not the only state actor to use these tactics, but it is the only one to use them so well and for so long. These tactics have been integrated into Russian official doctrine, whose strategy is to weaken the West as will be demonstrated in the subsequent pages.

To be exact, and as recommended by the CSIS, we should speak about the "Kremlin" rather than "Russia" so as not to conflate the governing power with its people. Russians are the first victims of information manipulation. "Virtually every type of action it has undertaken against the West was first implemented in Russia, against the Russian people, and

66. PM speech to the Lord Mayor's Banquet 2017 (https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017).

67. Sweden, Price Minister's office, *National Security Strategy*, 2017, p. 12.

68. Peter Hultqvist, speech in Tbilissi, 6 March 2018.

69. Andrea Shalal, "Germany Challenges Russia over alleged cyberattacks," Reuters, 4 May 2017.

70. CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, *op. cit.*, p. 6.

71. Jean-Yves Le Drian, Speech of 4 April, 2018.

against Russia's many ethnic, national and religious minorities."[72] It should be further added that "many Russians are perfectly aware that the news is faked: the Kremlin's power is entrenched not by trying to persuade people that it is telling the truth, but by making it clear that it can dictate the terms of the 'truth' and thus enhance its aura of power."[73]

In this report, we limit ourselves to influence through information, which is only one element of the Kremlin's tools of influence. The other elements are of a political, diplomatic, military, economic and cultural nature. In particular, the Kremlin has "weaponized" four spheres of activity: "traditional and social media, ideology and culture, crime and corruption, and energy."[74] Russian influence, particularly in France, is already well studied.[75] The following pages focus on its informational component.

A Soviet tradition

Russian disinformation—including interviews with fake experts, counterfeit documents, and retouched photos and videos—has a long tradition dating back to the Soviet period. The word itself comes from the Russian word *dezinformatzia*.[76] Disinformation as a weapon of war was first systematized in 1923 with the creation of a special unit within the GPU. The first significant operation was Operation Trust (1923-1927), which targeted White Russians in exile. The use of disinformation became more sophisticated in the late 1960s under the leadership of KGB Director Yuri Andropov.[77] The most famous

72. CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, *op. cit.*, p. 25.

73. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Interpreter, a project of the Institute of Modern Russia, 2014, p. 10.

74. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, A Minority Staff Report prepared for the use of the Committee on Foreign Relations, United States Senate, 10 January 2018, p. 37. This expression was popularized by Pomerantsev and Weiss who, in a report in 2014, argued that the Kremlin "arsenalized" information, money and culture (*The Menace of Unreality*, *op. cit.*).

75. See notably Cécile Vaissié, *Les Réseaux du Kremlin en France*, Les Petits Matins, 2016; Nicolas Hénin, *La France russe*, Fayard, 2016; Olivier Schmitt, *Pourquoi Poutine est notre allié ? Anatomie d'une passion française*, Hikari, 2016; Céline Marangé, *Les Stratégies et les pratiques d'influence de la Russie*, IRSEM *Étude* 49, March 2017.

76. On the history of Soviet disinformation operations, see the notes of Vasili Mitrokhim, who was an archivist for the KGB for thirty years before going to the West in 1992. Christopher Andrew has notably written two books from Mitrokhim's notes (*The Mitrokhin Archive: The KGB in Europe and the West*, Allen Lane, 1999 and *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB*, Basic Books, 1999). See also General Ion Mihai Pacepa, *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, 2013.

77. Cited in CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, *op. cit.*, p. 26-27.

Soviet attempt at disinformation of this period is certainly the rumor that JFK was assassinated by the CIA. This Soviet rumor remains popular today and is used by the Kremlin to defend itself from certain accusations, namely by claiming that these accusations are merely false flag operations. Among other famous fake news of the Soviet era were stories alleging American responsibility for the 1961 putsch of French generals, the assassination attempt on Pope John Paul II in 1981, and the "creation" of the AIDS virus. Interference in democratic processes is nothing new either.

"Active measures" refers to all the overt or covert strategies and techniques implemented by the Kremlin to influence the opinions and actions of the foreign public. These strategies include disinformation, infiltration or manipulation of youth organizations or trade unions, the use of agents of influence, and the use of pro-Russian or mainstream foreign media to disseminate information. For a time, the White House refused to respond directly to these operations. It was only in 1981 that the Reagan Administration created an inter-agency group (bringing together the CIA, USIA, FBI and the State Department) to analyze and organize a means of response in the form of reports presented before Congress and briefings to major media outlets. This is the sole example of a coordinated and effective response by the American institutional apparatus to the threat of Soviet influence.

On April 12, 1982, KGB Director Yuri Andropov ordered all agents to take "active measures" to prevent Ronald Reagan from being reelected.[78] Moscow also launched a "massive propaganda campaign" to see Helmut Kohl defeated in the 1983 federal election in Germany, but to no avail.[79]

In fine, even if today's Russia is no longer the USSR, the continuity is striking: the means have occasionally changed, but the doctrine remains the same as does the use of "old methods (sabotage, diversion tactics, disinformation, state terror, manipulation, aggressive propaganda, exploitating the potential for protest among the local population)."[80]

Contemporary Russian information operations are a skilled mix of traditional Soviet propaganda and American entertainment. There is a mimetic component to the Russian approach, which draws inspiration from the latest Western communication and public relations techniques.

78. Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB*, *op. cit.*, p. 242.

79. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 37.

80. Jolanta Darczewska, "The Devil is in the details: Information warfare in the light of Russia's Military Doctrine", *Point of View*, 50, OSW, May 2015, p. 7.

The Kremlin additionally benefits from the help of certain societies, such as Ketchum, an American public relations company, whose most impressive "coup" was to place an op-ed from Putin in *The New York Times* on 11 September 2013, a highly symbolic date.[81]

The evolution of the Russian approach

One major difference with the Soviet period is that contemporary Russian interferences have given up any pretense of ideology. The objective of information manipulation is no longer to convert people to an ideology—which the Russian authorities willingly admit was the case in years prior ("in contrast with the USSR, Russia has renounced the exportation of any given ideology").[82] This does not signify, naturally, that Russia has renounced its exertion of influence, but simply that the intended effect is no longer the same; it is less a matter of conversion than of weakening and dividing. In this respect, the Soviet techniques remain quite useful.

The continuation and adaptation of Soviet techniques occurred in several stages. Moscow observed that its narrative of the Chechnya War, from 1999 onward, was not adopted by international public opinion, even as the majority of the Russian population rallied around the new President Putin and his stated desire to exterminate Chechen terrorism.

Following the "color revolutions" in Georgia (2003) and in Ukraine (2004), the Kremlin was able to measure the power of attraction of a democratic narrative that was widely circulated at the time by Western-backed media aimed at its "near abroad." Russia then worked to strengthen and redefine its tools of international influence. First, it attempted a classic approach to soft power, based on attraction, by creating the Valdai club and by recruiting communicators.[83] It was to this end that Russia Today was created in December 2005 with the aim of improving Russia's image abroad.

But the fruits of these efforts took time and the 2008 Georgian War confirmed the weaknesses of the Russian information system. Despite its efforts, Russia Today failed to influence the international public's perception of the conflict. Russia has since changed its strategy, renaming

81. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 18.

82. Commission for defending sovereignty and protecting against interferences in the internal affairs of the Russian Federation Council (the upper chamber of Parliament), Report published on 5 March 2018 (http://council.gov.ru/media/files/BX3FqMRAl7ykAmPLRl4cR1ju4RaswiKN.pdf).

83. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 12.

the outlet "RT" the following year, a more neutral title that does not immediately reveal its Russian origin. The outlet has also shifted from a positive approach (promoting Russia), which was unsuccessful, to a negative approach aimed at discrediting the adversary, through for example, the recruitment of Western voices (journalists, experts, activists, personalities).[84]

An important turning point came in 2011: the Arab Spring, which was perceived in Moscow as having been inspired and supported by the West; and the contestation of the Russian legislative elections in December 2011, which mobilized over ten thousand people in several Russian cities. Putin still believes that the West is trying to overthrow him. It was after this episode that the Kremlin incorporated "the protest potential of the population" into its military doctrine, perceiving it as one of the most important variables in armed conflict. This policy advocates targeting Russians first in order to quell protests through the repression of NGOs under the law on foreign agents and through purges in the media; in September 2012, the Kremlin closed USAID, which it described as an agent of influence. At the same time, the troll factory in St. Petersburg, which later became famous (see below), was created. Its initial purpose was to control the Russian population.

The Kremlin perceived both Euromaidan and the fall of the Yanukovych regime as serious setbacks. They were, for Moscow, a worrying signal of the success of the regime change approach, i.e. a Western-led idea. Adding to the anxiety, these events took place near Russian borders, and more importantly, in Ukraine. This trauma partly explains Russia's subsequent military intervention in Ukraine—first in Crimea and later in the Donbass. It also explains the intensity of the information war waged by Russia from the start of the Ukrainian crisis.

After having implemented a series of measures aimed at curbing the protest potential of the Russian population, the Kremlin has, since the Ukrainian crisis in particular, strengthened its information offensive both towards the States of the "near abroad" and Western States. Since 2016, the sophistication of these techniques has advanced with the adoption of a new information doctrine and, in 2017, a strategy for the development of the information society and the creation of "cyberbrigades," the extension of the National Guard's jurisdiction over informational and cyber fields, etc.[85]

84. *Ibid.*, p. 15.
85. CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, *op. cit.*, p. 35.

Moscow considers its actions to be defensive. It considers itself the victim of an information war waged by the West, especially by the United States. The defense of democratic and liberal values and support for civil society are seen as subversive acts whose purpose is regime change. The perception of Western dominance in the information field (based on the observation that major American and British media have much larger audiences than RT, for example) puts Russia on the defensive. In Russian state doctrine, it is written that the "US and its allies […] seek to conserve domination over international affairs" by "containing" Russia through "political, economic, military and informational pressure."[86]

Moscow also responded in kind to the Western accusations of interfering in democratic processes: on 30 May 2018, the Commission for the Protection of State Sovereignty and the Prevention of Interference in the Internal Affairs of the Russian Federation (with the Parliament's upper chamber), published a *Special Report on the attacks on electoral sovereignty during the presidential elections of the Russian Federation*, which accuses the United States, NATO, the EU, Australia and several post-Soviet States such as Ukraine to have launched "massive attacks" throughout the 2018 presidential elections, including both cyberattacks and influence operations through the vector of civil society. The report concludes by noting the failure of this initiative. It will however be noted that no proof was provided in support of this claim and that, if the central electoral commission observed these cyberattacks on the day of the vote, they did not identify any perpetrators.

The "new generation warfare"

The Russian strategic community speaks of a "new generation warfare" in reference to the growing use of non-military and non-lethal means (what Americans refer to as "political warfare"). The term "Gerasimov doctrine" is common in the West, named after the Chief of the General Staff of the Russian Armed Forces. In reality, the "doctrine" is mainly drawn from extracts of one of his articles, published in 2013 in a weekly military journal, in which he affirms:

> In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. […] The role of nonmilitary means of achieving political and strategic goals has grown, and, in

86. National Security Strategy of 31 December 2015.

> many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces.[87]

This is not exactly a doctrine nor is it new: the same idea was formulated several times in Russian military journals a decade earlier. In 2003, Makhmut Gareev, former Deputy Chief of the General Staff and current President of the Academy of Military Sciences, noted that "the importance and the proportional share of non-military means have increased considerably."[88] In 2010, Chekinov and Bogdanov restated this conclusion.[89] Admiral Pirumov writes that "[i]nformation warfare consists in securing national policy objectives both in war time and in peace time through means and techniques of influencing the information resources of the opposing side... and includes influences on an enemy's information system and psychic condition… disinformation (deception), manipulation (situational or societal), propaganda (conversion, separation, demoralization, desertion, captivity), lobbying, crisis control and blackmail."[90]

Above all, Gerasimov's speech is supposed to describe the supposed actions of Westerners in the Arab Spring. In Ukraine in 2014, Russia reproduced what it thought Westerners had done during the color revolutions, the Arab Spring and Euromaidan. Gerasimov likes to recall that the concept of "hybrid warfare" was first written in 2005 in the United States from the pen of a certain General James Mattis, now Secretary of Defense.[91]

87. Valery Gerasimov, "The Value of Science Is in the Foresight", originally published in *Military-Industrial Kurier*, 27 February 2013, translated from Russian by Robert Coalson and republished in the US *Army Military Review*, January-February 2016, p. 24.

88. Makhmut Gareev, "If There Were War Tomorrow," Armeyskiy Sbornik, 1 April 2003, cited in Linda Robinson *et al.*, *Modern Political Warfare. Current Practices and Possible Responses,* Rand Corporation, 2018, p. 43.

89. Sergei Chekinov and Sergei Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought*, Vol. 1, 2010, p. 17-22.

90. V.S. Pirumov, *Informatsionnoe Protivoborstvo*. 3. Moscow, 2010, quote in Peter Pomerantsev and Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 12.

91. James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings Magazine* (U.S. Naval Institute), 131:11, November 2005, p. 18-19.

"Information warfare"

In this new generation warfare, the role of information is of central importance now that "the main battlefield is consciousness, perception, and strategic calculus of the adversary."[92] The goal is to achieve "informational superiority."[93]

The Russian political and military elite do not hesitate to use the term "information warfare" (*informatsionaya voyna*), while maintaining a defensive posture. In other words, they continue to accuse the West, and above all the United States, of launching an informational war against Moscow and elsewhere (the Arab Spring of 2011 is frequently cited as an example). They understand the expression broadly: cyber-operations, for example, are only one subset of information warfare.[94] The Military Academy of the General Staff of the Armed Forces of Russia devotes an entry to this term in a glossary, with the purpose to distinguish the Russian meaning, applicable at all times, from the Western meaning, which limits informational operations to a period of hostilities.[95] This confirms the Russian continuum between war and peace and the conviction, on the Russian side, of their difference (and perceived advantage), compared to the Western approach.

In March 2018, several members of the Duma evoked the possibility of introducing the concept of "information war" into Russian legislation. Mikhail Degtyarev, for example, declared that "it is the continuation of the information war launched against Russia. We should take a firmer position and begin with the legislative consolidation of the notion of a 'war of information.'"[96]

In spite of the devices deployed, whose capabilities are often exaggerated, Russian "information warfare" faces several structural limitations. First, the democratization of information through the internet, especially in democratic countries, creates fierce competition for major Russian media. In terms of the number of viewers, on television and even on social networks, RT remains well below BBC, CNN and

92. Dima Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, IFRI, Proliferation Papers, 54, November 2015, p. 26.

93. Sergei Chekinov and Sergei Bogdanov, "Asymmetrical Actions to Maintain Russia's Military Security," *op. cit.*

94. Keir Giles, *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, 2016, p. 4.

95. Cited by Keir Giles, *The Next Phase of Russian Information Warfare*, *op. cit.*, p. 2.

96. Dar'ja Rynochnova, "Дегтярев предложил внести в законодательство понятие 'информационной Войны,'" *Parlamentskaja Gazeta*, 13 March 2018.

Al-Jazeera. However, this same process of democratizing information is also ambivalent and creates more relays and means of reaching certain audiences. This makes disinformation easier.

In addition, the Kremlin does not create crises so much as it exploits existing vulnerabilities, divisions, and political or inter-community tensions. Essentially, it blows on the embers. The Kremlin's logic is reactive rather than active.

Finally, it is also necessary to relativize the capacities of the Russian secret services and explore other, often endogenous, causes of the crises that exist right now in Western democracies because "not everything that happens in Russia's favor is necessarily initiated by Russia, just as the United States is not responsible for everything that happens in its favor."[97] It is important to resist the temptation to use Russia to explain every hardship encountered, from the election of Trump to Brexit, while minimizing the responsibility that falls upon our liberal democracies for a trust crisis among our public.

b. China

The People's Republic of China (PRC) has a long history of ideological struggle and the use of propaganda. Today, this know-how is at the service of Chinese interests on a global scale. Beyond the maintenance and improvement of its image, Beijing develops tools of influence and interference that are specifically geared towards offensive intentions.

In China, the fabrication of propaganda and ideological indoctrination are two key prerogatives of the Chinese Communist Party (CCP). The Party has a large bureaucratic structure for information control that has now been adapted to match the status of the PRC on the international stage. Effort on the ideological front has two objectives: first, to shape the internal political space and maintain the Party's legitimacy (through censorship and disinformation); second, to influence international opinion and wage the "information war" in favor of Chinese interests.

The organs of propaganda and influence are placed high up in the political hierarchy. The regime's number five, Wang Huning, heads the "Central Guidance Commission on Building Spiritual Civilization," which determines ideological content and manages its dissemination at the national and international level. The commission oversees the Central Propaganda Department (Publicity Department of the Communist Party

97. Linda Robinson *et al., Modern Political Warfare*, *op. cit.,* p. 56.

of China, *zhongxuanbu*), headed by Huang Kunming, a member of the CCP Political Bureau, whose activities focus mainly on the internal aspects of the Party and the use of propaganda at the national level.[98]

Chinese propaganda is a critical part of its public diplomacy. Beijing manages content and deploys a number of vectors to further its slogans, which are intended to guide intellectual debate on China ("peaceful rise," "harmonious world") and to disseminate positive information to the public, such as about its current Belt and Road Initiative (BRI). Today, China controls more than 3,000 public television channels in the world, over 150 pay TV channels, around 2,500 radio stations, about 2,000 newspapers and 10,000 magazines and more than three million internet sites. In addition, the regime has published nearly 250,000 books.[99] These vectors are complemented by networks that broadcast cultural content for educational and academic purposes, such as the Confucius Institutes, which are the preferred relays of influence and propagation of official messages.

In the media field, China created a state-owned global broadcasting group called the China Global Television Network in 2016. It was the product of a merger involving several channels of the China Central Television Network (CCTV). The programs broadcast content in a coordinated manner that was, for the most part, provided by the Xinhua State News Agency. The Xinhua State News Agency is intended to compete with international agencies (like AP, UPI, Bloomberg, Reuters) and broadcasts on all media (internet and mobile phone providers). In pursuit of these same objectives, the main English-language Chinese newspapers, the *People's Daily*, the *China Daily* and the *Global Times*, are similarly distributed through digital media.

In recent years, the nature of the content broadcast by these media has changed dramatically. In the context of China's rise to the rank of superpower and its involvement in the strategic and security issues of the day, Chinese critiques of Western powers—the United States, in particular—have become more regular and more elaborate. In China, many stories simply recycle the content published by Russian news agencies (like RT or Sputnik). This is the case, for example, with the media's treatment of the Syrian crisis. However, some specific content,

98. At the international level, these two bodies rely on a dense network of broadcasters and operators whose supervision is essentially shared by the Information Office of the State Council and the Ministry of Foreign Affairs.

99. David Shambaugh, *China goes Global. The Partial Power,* Oxford University Press, 2013, p. 227-228.

such as criticism directed at French action in Africa, or the position on the South China Sea issue and the "warmongering" of Japan and India, are subject to a regular and strictly planned schedule of diffusion. This is part of a counter-influence attempt aimed primarily at Eastern European and African audiences. These operations are part of a global propaganda campaign that seeks to counter and reduce the influence of democratic, liberal values and messages. The establishment of the Belt and Road Media Community contributes not only to promoting Chinese interests, but also to countering or extinguishing the influence of external media.[100]

The PRC's influence on information is global in scope. The ideological content is not only used to seduce or influence, but also to guide public opinion and interfere if needed. This proactive dimension is less aggressive than that used by Russia today, but Chinese tactics are growing in number and sophistication.

Information warfare is an integral dimension of China's strategy of influence and intimidation. Since the beginning of the 2000s, Chinese strategists have been working on the implementation of the "three wars" (*sanzhan*) in the field of information. Combining the war for public opinion, psychological warfare and legal warfare, this approach is intended—in peacetime as in wartime—to control the dominant discourse and influence beliefs and perceptions so as to serve the interests of the PRC, while also reducing the ability of adversaries to respond.[101] This strategy, which explicitly targets public opinion in democracies, exploits the vulnerabilities of open societies.

The intelligence services (the Ministry of State Security, the Ministry of Public Safety, the second department of the People's Liberation Army [PLA] and the department of international liaisons of the PLA in particular) and certain departments of the Central Committee of the CCP (United Front Work Department—UFWD) have engaged in a similar reflection in recent years. Henceforth, the concerted efforts to reinforce the Chinese narrative (soft power) are now associated with clandestine operations aimed at boosting China's influence capabilities. This development, which is closely linked to China's rise to power in the international arena and subsequent sense of self-assurance, hinges on the combination of both the Russian example, from which Beijing draws its inspiration, and the

100. Beijing also organizes numerous conferences that seek to shape the content of media stories and influence a new generation of journalists. See Lu Anqi, "Chinese and African Media Discuss how to tell good stories," *Chinafrica*, 14 August 2016.

101. Elsa B. Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, XVI:13, August 2016, p. 10-14.

American retreat from the international sphere, initiated by the Trump administration.

Although there were some heated discussions brought about by Chinese interference in Australia (see box below) and New Zealand, Europe continues to show comparatively little concern for this threat even as Chinese operations continue to visibly increase.

These Chinese inference and influence operations come in various forms:

- Manipulation of leading former European statesmen working to promote Chinese interests;
- Penetration of regional organizations (Interpol, the Council of Europe) in order to orient their activities so that they align with Chinese interests;
- Manipulation of diasporas and Chinese communities living abroad, which can be mobilized by UFWD agents during diplomatic visits, for example;
- Pressure on researchers and the academic research apparatus using the issuance of visas and financial programs;
- Distribution, in exchange for remuneration, of a news supplement (*China Watch*) in major European daily papers, in order to create financial dependence and to stimulate self-censorship in the treatment of news pertaining to China;
- Taking control of the majority of Chinese-language European media;
- Retaliatory measures against governments that are critical or judged to be "unfriendly," just as Norway did in response to the decision to award a Nobel Peace Prize to Liu Xiaobo (downgrading diplomatic exchanges, indirect commercial sanctions, etc.).

The implementation of this multi-sectoral influence has already led to policy responses and the build-up of new security measures in several democracies, including Australia, from which Europe may draw inspiration. Today, Beijing enjoys systematic and multi-vector counter-influence and information-control capabilities. Chinese content that is broadcast in French-speaking Africa often conveys positions and principles that are contrary to French interests. This dimension goes well beyond the framework of the Franco-Chinese bilateral relationship and is part of a strategic global competition.

Chinese interference in Australia

Australia is a prime target of Chinese influence.[102] Officers from the UFWD department of the CCP and other agencies, including the Department of Liaison of the People's Liberation Army (PLA), are targeting and recruiting agents of influence from the Australian elite (entrepreneurs, politicians, academics, etc.). The CCP exploits vulnerabilities linked to the Australian model of financing universities, media and election campaigns in order to expand its influence and "buy" itself access to the country's political and scientific communities. There are certain corrupt political figures who, in exchange for funding from Chinese donors, advance the CCP's positions on international issues. Some Australian universities for example have equally become vehicles of Chinese propaganda. Self-censorship is rampant, including among researchers on China, an increasing number of which are avoiding discussing certain topics, for fear of losing their editor or access to the research field. Australia has become aware of these concerning developments, which are partly the result of the premium placed on counter-terrorism over counter-espionage in the Australian Security Intelligence Agency (ASIO) in the post-9/11 years. Canberra is currently in the process of rebalancing its priorities, and has significantly increased its legal arsenal in order to monitor foreign investment in its territory, including in the media.[103] In June 2018, the Parliament passed news laws against espionage and foreign interference.

102. John Garnaut, "How China interferes in Australia. And How Democracies Can Push Back," *Foreign Affairs*, 9 March 2018; Clive Hamilton, *Silent Invasion: China's Influence in Australia*, Hardie Grant, 2018.

103. Joshua Kurlantzick, "For Clues on How to Address China's Growing Political Influence Strategies, Look to Australia," *Council of Foreign Relations*, 18 December 2017 and Clive Hamilton, "Australia's Fight Against Chinese Political Interference: What Its New Law Will Do", *Foreign Affairs*, 26 July 2018.

Part Two

HOW?

From our analysis of attempted information manipulation in some twenty countries, certain common features have emerged, in terms of vulnerability factors and the means employed. This section of the report exposes those commonalities and then explores other incidents of information manipulation outside of the well-documented cases in Europe and North America.

I. Vulnerability factors

A. The presence of minorities

Manipulation attempts are facilitated by the presence of minorities, as they exploit the feeling of non-belonging that these communities might have with regard to their integration within the national community. This is indeed the case in the Baltic States. The large Russian-speaking minority, particularly in Latvia (37% of the population, just under 50% in Riga),[1] is not in itself a threat to national cohesion because these communities are diverse. In fact, there are several Russian-speaking communities of different nationalities (Lithuanian, Latvian or Estonian, with or without

1. The Russian-speaking minority in Latvia is the largest in the Baltic States as compared with 29% in Estonia and 6% in Lithuania.

the status of "non-citizen," Russian, Belarussian, and Ukrainian), and all have differing opinions on local and Russian authorities. Furthermore, Russian communities in the Baltic States enjoy a better quality of life and greater freedom of movement (in Russia and the Schengen Zone if they are permanent residents of Latvia) than they would otherwise enjoy in Russia. Moscow nevertheless tries to rally them and exploit them as part of its "compatriots" policy, at events such as the ceremony of May 9, without much success (only 100,000 people attended the ceremony in 2017, whereas 150,000 attended in 2016 and as many as 200,000 in 2015.) The Russian media is also developing narratives that specifically target this minority abroad (claiming, for example, that Russian-speaking Latvians would be discriminated against, oppressed, mentioning "apartheid" and even occasionally "genocide").

The Lisa Case

The "Lisa Case" swept Germany in January 2016. After disappearing for 30 hours, a 13-year-old girl belonging to the *Russlanddeutsche* community claimed to have been kidnapped, beaten and raped by three men who appeared to be of Arab descent. Russia immediately picked up the story, first on the major national channel, then in Russian media outlets abroad (RT, Sputnik, RT Deutsch) and on social networks, where the story was relayed notably by far-right groups. Through Facebook, demonstrations were organized, involving both the *Russlanddeutsche* and neo-Nazi groups. The events were covered by the Russian and German media. The Russian Foreign Minister Sergei Lavrov made two public statements in which he accused the German authorities of concealing the reality of the situation behind political correctness for interior political reasons and challenged the competence of the German police and judicial system. He argued that Lisa could not have "disappeared voluntarily for 30 hours." His German counterpart Frank-Walter Steinmeier accused Russia of political propaganda. In the end, the investigation showed that Lisa had lied: she had disappeared voluntarily and had been at a friend's house.

The Lisa Case showed the power of false information (how it could trigger demonstrations, feed anti-migrant sentiment and come close to provoking a diplomatic crisis). It also showed that the *Russlanddeutsche* community is one of Germany's vulnerabilities and that Berlin must put in place a mechanism with which to react to these challenges as soon as possible. The incident was allowed to develop as much as it did because the story was refuted too late. The main lesson is, therefore, the importance of responsiveness.

In Germany, alongside a small, but important local Russian-speaking community, there is a community of *Russlanddeutsche*. They are nationals of the German-speaking Soviet space, descendants of the Germans of the Volga transfered there by Catherine II in the 18th century, who were deported by Stalin to Central Asia and later repatriated to Germany after reunification. The existence of this community provides fertile ground for manipulation, the primary purpose of which is to accentuate the divisions between these *Russlanddeutsche* and other Germans in an environment of suspicion toward immigrant communities.

B. Internal divisions

Even where there is no significant diaspora or easily exploitable minority group, attempts at information manipulation can have an effect on social and political divisions within our democracies in an even more insidious manner.

Poland serves as an interesting case study in this respect. At first glance, it seems that the country would offer little opportunity for Russian manipulation attempts. The country has studied and learned Russian tactics (the Polish-Soviet War of 1919-1921 is retrospectively described as an undeclared "hybrid war"—use of propaganda, diversion, attempts to influence minorities, etc.). In addition, 70 years of communism has immunized the population to Russian propaganda. Furthermore, the country has neither a Russian-speaking minority nor a Russophile political party and anti-Russian sentiment is widespread. Yet, attempts at indirectly influencing Polish elections have been observed (i.e. the creation of fake accounts on social networks in preparation for the 2018 and 2019 elections). Moscow is taking advantage of the political divisions, which have lately been increasing.

An Oxford researcher studied Polish social networks and showed that only a few days after the Euromaidan movement in Kiev, a large number of fake accounts appeared on Facebook, along with different platforms which began spreading Russian propaganda. The researcher also pointed to the growing difficulty of detecting and attributing these actions to Russia, which has increasingly succeeded in normalizing them. He also showed that "right-wing" accounts are twice as numerous and active as those accounts belonging to parties on the "left-wing."[2]

2. Robert Gorwa, *Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere*, Working Paper No. 2017.4, University of Oxford, Project on Computational Propaganda, 2017.

C. External divisions

Tensions between neighboring countries are also exploited. Moscow is working to sow discord between Poland and its neighbors, Belarus, Lithuania, Germany and, above all, Ukraine. (The relationship between Ukraine and Poland has historically been fraught with sensitivity stemming from the massacres of Poles in Volhynia.) The objective is to make Poland the outcast of Europe, by weakening its relationship with both its immediate neighbors and the EU as an institution. In Lithuania in 2017, authorities observed a strong resurgence of messages directed at the local Polish community which were aimed at exacerbating inter-community tensions and degrading diplomatic relations between the two countries.[3] At the European level, Moscow tries to isolate the Baltic States (and Poland) by portraying them as paranoid, Russophobic hysterics compared to the more "moderate" States of Western Europe. One of the Kremlin's prime objectives is to maintain and caricaturize the existing divisions between European countries on Russian matters.

These dynamics do not only exist in Europe; in the Gulf, inter-state tensions are also used to catalyze the manipulation of information, as illustrated notably by the crisis between Qatar and its neighbors, which started in May 2017, after a cyberattack and the planting of a false news story (see below).

D. A vulnerable media ecosystem

One of the reasons why the Macron Leaks failed to have an effect on the 2017 French presidential elections (see below) is that the French media ecosystem is relatively healthy. By this we mean that the population relies mainly on traditional media sources with high journalistic standards. The French rely less on "tabloids," which are much more developed across the Channel, and less on the websites dedicated to conspiracy theories that proliferate in other countries. Information manipulation relies on a diversified arsenal: a populist press, social networks, disinformation sites, and the Russian media, which may rely on Russian-speaking minority groups in target countries or on translations of those articles in local languages. Their efforts are all the more likely to succeed if the media landscape is fragmented and conventional media outlets are weak, which can arouse distrust in part of the population and accelerate a variety of populist and conspiracy theories' vectors.

3. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 42.

The Russian-language media in the Baltic States

Russian-language media are abundant in the Baltic States (press, radio, television, internet). Since 2005, the Russian platform Baltic Media Alliance (BMA), officially registered in the United Kingdom, permits the broadcasting of Russian channels throughout the region with appropriate content (First Baltic Channel has three editorial committees for each Baltic State). A few years ago, Latvia (2014) and Lithuania (2015) temporarily blocked the Russian channel RTR-Planeta, accusing it of inciting hatred towards Ukrainians. But this temporary measure had no structural effect. Local channels have a hard time competing with Russian channels, which have considerable resources and very popular entertainment programs. In Latvia, authorities rejected the idea of creating a Russian-language channel, while Estonia launched ETV+ in 2015. However, Russian-language programs are still available on Latvian public TV channels (LT7) as is a particularly popular Russian-language radio station (Latvijas Radio 4).

In terms of influence, Russian television is considered to be "the greatest threat" to Baltic States because it allows Russian-speakers to live in an "information cocoon."[4] The Baltic States simply do not have the means to offer its Russian-speaking population media of the same quality. Furthermore, the idea of a single, common Russian-speaking channel is not feasible anymore because of rivalries and differences in perception.[5]

On the internet, the Latvian authorities refused to register Sputnik on the .lv domain. However, the protest was purely symbolic as the website was registered as .com (sputniknewslv.com). The most effective sites for spreading Kremlin propaganda are not those that are most obviously associated with Moscow, such as Sputnik; rather, they are sites which appear local, such as Vesti.lv, or regional, such as Baltnews or Rubaltic. Launched in 2014 in three distinct editions for each of the Baltic States, Baltnews belongs to Rossiya Segodnya through front companies. The content of its sites is partly determined by Russian diplomats in Riga, Vilnius and Tallinn. As for Rubaltic, it is registered in Kaliningrad. There is also the IMHO Club, a network of Russian-language blogs owned by Latvian pro-Russian activist Yuri Alexeyev, who, after successfully establishing himself in Latvia is trying to gain footholds in Belarus and Ukraine.

4. Todd C. Helmus *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, 2018, p. 66-67.

5. *Ibid.*, p. 69.

E. Contested institutions

The first part of this report demonstrated how distrust in institutions was one of the main reasons for the rise and effectiveness of attempts at information manipulation. It makes democratic institutions and public policies easy targets by constantly causing doubt, either of a government's so-called "hidden agenda" or of the effectiveness of government action.

Thus one of the narratives propagated by manipulation attempts in Baltic States is that these States are failed States, brimming with corruption that would collapse without the support of Western powers. This narrative is all the more dangerous because there is always a segment of the population, in every democracy, that is critical of and disappointed with its government.

Since 2014, the Kremlin has systematically challenged authorities in Ukraine by accusing them of inefficiency, corruption, etc. To this end, hundreds of thematic groups were created on social networks controlled by Moscow (Vkontakte was particularly active until it was banned in May 2017). These social networks use pro-Ukrainian symbols and nationalist rhetoric to call for the organization of a third Euromaidan.[6]

II. The means of information manipulation

A. Multiform levers and vectors

The RAND Corporation has thoroughly studied the means available to the Kremlin to launch an "information war." They have identified four categories corresponding to the degree of the Kremlin's control:[7]

1) Government bodies (the Kremlin itself, ministries, embassies, public agencies like Rossotrudnichestvo, whose mission is to further Russian influence abroad, especially in CIS countries);

2) Fake NGOs, financed by the State and/or working closely with it (Russkiy Mir, created in 2007 to promote Russian language and culture abroad and which serves in reality as a bridge between the government and relays of influence abroad, or the IDC, which is the Kremlin's think tank and has offices in Paris and New York);

3) Other organizations presented as having no connection to the State, but in reality act as proxies (the *Notchnye Volki* motorcycle club,

6. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 16.
7. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 56.

"the Night Wolves," which has about 5,000 members, is close to Putin). In this area, the Kremlin's strategy is to occupy a niche so that groups whose views do not align with those of the Kremlin cannot establish themselves;[8]

4) Religious, political or economic relays that are independent with respect to their decision-making but which, without being under the direct control of the Kremlin, support the Kremlin's interests or a close relationship with it (the Orthodox Church, certain economic circles, political parties who support a rapprochement with Russia, i.e. the Opposition Bloc in Ukraine, the Party of Socialists of the Republic of Moldova or the Alliance of Patriots in Georgia).

One could add a fifth category of individuals abroad who serve as pawns in the manipulation of public opinion or local relays of foreign policy. These "useful idiots," an expression (probably falsely) attributed to Lenin, may be intellectuals whom the Kremlin is trying to "capture" through forums such as the Valdai club. They may be political figures from far right or far left movements or activists from various movements.[9] The links with the outside can be formal (through diplomatic networks) or informal (through proxies, business, civil society, etc.)

In addition to so-called "white" (overt) propaganda, discussed above, there is "gray" propaganda, such as conspiracy theory websites and similar resources on the Darknet. There is also "black" propaganda, that is, propaganda that can be reasonably denied. These include trolls, bots and hackers.[10] This is how information campaign manipulations are organized: the aggressor State disperses its actions to hide its footprint and give the impression of spontaneous action, on various platforms and media, at different moments in time. The State uses propaganda elements from across the spectrum—from the covert (trolls) to the overt (diplomacy). In reality, this is a coordinated campaign.[11]

The Kremlin has a "media arsenal"[12] that consists primarily of two major overseas outlets, Rossiya Segodnya and RT, which are presented as separate entities but are actually run by the same editor, Margarita Simonyan. Rossiya Segodnya owns both Sputnik (founded in November

8. Mark Galeotti, "An Unusual Friendship: Bikers and the Kremlin (Op-Ed)," *The Moscow Times*, 19 May 2015.

9. See Orysia Lutsevych, *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood,* Chatham House, April 2016.

10. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 12.

11. See Ben Nimmo, "Russia's Full Spectrum Propaganda: A case study in how Russia's propaganda machine works," DFRLab Medium.com, 23 January 2018.

12. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 61.

2014 to replace the Voice of Russia) and RT, established under the name Russia Today in 2005 and renamed RT in 2009. The outlet claims to be "completely independent."[13] However, it also emphasizes that its purpose is to "secur[e] the national interests of the Russian Federation in the information sphere."[14] The initial objective of these news outlets was to improve the image of Russia abroad. However, the Kremlin quickly realized that Rossiya Segodnya and RT did not succeed in this endeavor. Consequently, the Kremlin then directed the outlets to adopt a negative approach: they are now primarily used to degrade the image of the adversary. These media receive little attention in the international arena, where CNN, BBC and Al-Jazeera dominate the media environment. They are, however, successful with audiences in the far left and far right political camps or those easily taken in by conspiracy theories.

The Kremlin can also count on Russian national TV channels (such as Russia 24, NTV, Channel One, RTR), which are still highly watched in the countries of the "near abroad." (This is because they are often better than the local channels.) In the Baltic States, most of the Russian "journalists" who publish Russia-oriented reports are working there illegally, having entered on tourist or business visas often issued in Europe.[15] These "journalists" interview small, local personalities who are opposed to the governing party. They also film protest movements, exaggerating their scale in order to give the impression of a divided country on the brink of civil war.

13. Tweet published by Ben Nimmo featuring the registration document of the RIA Global company in the United States, 21 June 2018 (https://twitter.com/benimmo/status/1009777111857553409).

14. Tweet published by Ben Nimmo featuring a statement of the Russian Federal Agency for Press and Mass Media, 21 June 2018 (https://twitter.com/benimmo/status/1009778691398946816).

15. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 41.

When Russian channels invent reality (Sweden, France)

In February 2017, a team from the Russian television channel NTV made their way to Rinkeby, a Stockholm suburb, to cover clashes with the police. Failing to find sufficient film to paint a portrait of a country on the brink of civil war, they offered to pay a group of teenagers 400 kroners each (40 euros) to play the role of troublemakers in front of the camera. The teenagers refused and reported the events to the Danish media. NTV aired its report a few days later: entitled "Migrants have transformed the suburbs of Stockholm into an extreme danger zone," it exaggerates the severity of the clashes and claims that the violence was unleashed by an investigation of a rape, while it was actually a crime related to drug trafficking.[16] Rape and sexual crimes in general are one of the most favorited pro-Kremlin disinformation stories because they arouse passions all the while illustrating a state of insecurity, of moral decadence and of the "barbarization" of Europe.

NTV is well-accustomed to putting on a show: in a news story from 2016 on the remilitarization of the island of Gotland, the channel showed an official from the territorial administration pointing to a number of areas on the map, while the commentator affirmed that Gotland was at the center of the 20th century wars. In reality, the film crew had asked the official to point to around a hundred different natural reserves, and at no moment were there any questions of military nature…[17]

These manipulations are not unique to Sweden. Several other similar incidents were detected in France: in a report from 2016 on Euroscepticism in France, the news channel Russia 24 interviewed French people and added a Russian translation that in no way resembles what they actually said. The year before, the television channel Russia 1 also aired a report in France on islamization that is riddled with lies—the journalist who went around Parisian streets notably insisted that "practically nobody speaks French. At the market, they only sell Halal meat […] One out of two women wears a burqa or a niqab. There are practically no non-Muslims in the neighborhood." She also invented statistics ("11 million Muslims" in France, nearly three times as many as the real figure, and stating that they make up 40% of the capital's population and 60% in Marseille, without citing sources).[18]

16. "Russian TV offers money for staged 'action' in Sweden?", EUvsDisinfo, 8 March 2017.

17. "Naturreservaten blev krigiska när den Gazpromägda ryska TV-kanalen rapporterade om Gotland," helahalsingland.se, 19 July 2016.

18. Allyson Jouin-Claude, "Le *Petit Journal* dénonce les manipulations d'une chaîne publique russe," *LeFigaro.fr*, 21 May 2016.

In April 2018, the Russian news agency RIA FAN announced the upcoming launch of a new "reinformation" website for the American public called "USA Really. Wake Up Americans." A press release describes the project as follows: "Due to the growing political censorship imposed by the United States, there remains less and less of information sources that are not under control of the US authorities. In this regard, US citizens cannot receive objective and independent information about events occurring on the territory of America and throughout the world."[19] RIA FAN, which is based in St. Petersburg, is in fact an offshoot of the well-known troll factory, the IRA (see below). RIA FAN and IRA were originally situated at the same address and owned by the same individual (Yevgeny Prigozhin). It is still too early to predict the effect that this new player will have on the Russian disinformation arsenal.

Even if information manipulation is spread into the virtual world (see below), it also has real-life effects. Depending on the countries, information manipulation relies on various mechanisms of influence, in the political, media, economic, and even cultural spheres. One of Moscow's biggest achievements is to have individuals or groups that are not Kremlin-related endorse its narratives. These individuals or groups all share a common suspicion or disdain for democratic institutions. They also defend ideas that are in line with Moscow's interests, even in those countries where no significant political force is explicitly supporting Moscow's policies.

The example of Poland is enlightening in this respect. Moscow can be expected to indirectly use conservative circles that are opposed to the liberal West (opposed to liberal standpoints on sexuality, abortion, family, religion, etc.). Alternatively, they may use: liberal circles opposed to the PiS (in order to cultivate internal division); Pan-Slavs, who believe that there is a regional culture of which Russia is the champion; nationalists who are often activists of extreme right movements and anti-Semitic; certain individuals, such as Eurosceptics or those who harbor anti-American and/or anti-Ukrainian sentiments; as well as conspiracy theorists or those who believe in alternative ideologies and who may be more inclined to challenge established facts.

In Sweden, parties as diverse as the Swedish Democrats and the far-right Nordic Resistance Movement or the Left Party and the Far Left Feminist Initiative are all potential relays of anti-NATO narratives or anti-migrant sentiment (in the case of the far right). In Finland, the

19. "USA Really. Wake Up Americans. The story of Russia's new private propaganda outlet," EUvsDisinfo, 16 April 2018.

populist and Eurosceptic "Finns of Finland" (or "True Finns") party has taken a pro-Russian turn as Russia has come to embody values that the party defends (nationalism as opposed to liberalism/cosmopolitanism, Christianity, white supremacy, etc.).

Russia can also take advantage of the networks of associations. In Sweden, associations with no outward connections to Russia hold positions that coincide with those of Moscow. Two examples are the Swedish Peace Council, on the far left, and Swedish Doctors for Human Rights, which denies that chemical attacks occurred in Syria. In addition, other alternative movements, such as the anti-vaccination movement, are progressively becoming pro-Russian. Finally, different research centers and institutes that have more or less overt links to Russia propagate Russian positions on foreign policy.

As far as the economy is concerned, in the Baltic States, strategic infrastructure projects that are likely to advance either European integration or energy independence are targeted. There are numerous examples: the Visaginas nuclear power plant project in Lithuania was targeted via the exploitation of opposition groups who denounced the project on ecological grounds. The rail project Rail Baltica was presented as economically unsustainable and evidence of aggression, as its purpose was allegedly to transport NATO troops. The Polish project to link the Vistula to the Baltic Sea by a canal was also criticized for being ecologically irresponsible, economically unsustainable and militarily aggressive.[20]

B. Calibrated narratives

The Kremlin's objective is not to persuade us to doubt in an alternative truth, but to believe that objective truth even exists, in order to sow confusion and paralyze any action. As such, it does not have to defend an ideological view point—this is, as already mentioned, a major change as compared to the Soviet era. The Kremlin can simultaneously support far right and far left movements, so long as they are in competition with one another. The Kremlin also endorses contradictory narratives: for example, it supports the most far-fetched—and mutually exclusive—explanations behind the MH17 crash, the Skripal affair and the chemical attacks on Douma.

20. Aleksander Król, "Information Warfare Against Strategic Investments in the Baltic States and Poland," *The Warsaw Institute Review*, 3/2017, p. 62-69.

Fifty Shades of Skripal

The Skripal affair (the poisoning of a former Russian spy in the United Kingdom in April 2018) initiated a heated Russia information campaign. The UK authorities have so far identified about 2,800 Twitter accounts which are likely to be bot-managed and have reached 7.5 million users.[21] The EUvsDisinfo website (belonging to the EU's East StratCom Task Force, see below) has produced a timeline of the narratives broadcast by Russian media. They spread stories of a Fentanyl overdose, Russophobia, a British experiment, a plot to justify Russian sanctions, an attempt to influence the Russian elections, an attempt to justify the boycott of the Football World Cup in Russia, an American plot, then a Ukrainian plot, then the fault of Yulia Skripal's future mother-in-law, then a British attempt to divert attention from rampant pedophilia in the country, that Skripal was trafficking in chemical weapons, a NATO toxin, etc. Ofcom has announced that it has opened seven investigations against RT, which it suspects of partiality in the handling of the case.

The narratives primarily target the most populous and influential States. For three and a half years the NGO Ukraine Crisis Media Centre (UCMC) analyzed the most popular televised news programs from three Russian channels (Channel One, NTV and Russia 1). Out of the more than 22,000 negative mentions of European countries, France was the most cited, with 17% of the attacks, followed by Germany and the United Kingdom.[22]

The messages are tailor-made, adapted to specific audiences, depending not only on the region but also on the socio-economic profile, age, etc. of the individual. The vectors are similarly adapted to the media ecosystem of each country. The socio-economic dimension is important: studies show that Russian influence depends on the concentration of Russian speakers as well as the concentration of underprivileged communities because it feeds on the frustrations of these actors.[23]

The topics are diverse, but certain recurring topics emerge (immigration, crime, American or NATO hegemony, moral decadence, etc.) which is no coincidence. The Kremlin first targets divisive, fear-inducing topics in our societies. One tactic is then to support both parties to these tensions and

21. "British officials probe 2,800 Russian bots that 'spread confusion' after Salisbury nerve agent attack on former spy," *Daily Mail*, 24 March 2018.

22. UCMC, *Image of the EU and Eastern Partnership countries on Russian TV*, 2 March 2018.

23. Aleksander Król, "Russian Information Warfare in the Baltic States—Resources and Aims," *op. cit.*, p. 61.

place them in opposition with one another, by tapping into tensions on race, LGBT rights, refugees, etc.

This pathocentered tactic rightly assumes that many people are less rational and more easily manipulated when it comes to emotional subjects. These subjects do not materialize out of thin air nor do Russian secret services invent them. They simply add fuel to a fire that is already underway. These tensions often have a firm and legitimate basis, which makes their manipulation all the more credible.

Pitting communities against each other: the case of race riots in the US

At least 29 Twitter accounts—with the hashtags #BlackLivesMatter, #BlueLivesMatter, #AllLivesMatter, on both the left and the right of the controversy—have been identified as having Russian origins. The best known is probably the Facebook account "Blacktivist," which had a photo of Freddie Gray (who died at the hands of a police officer a year earlier). This was liked by 360,000 people, which is more than the official account of the Black Lives Matter movement. The account helped mobilize, incite and accelerate the movement with messages encouraging action against the police. The account was revealed to be Russian and indeed part of the Russian effort to divide communities in the United States by tapping into racial tensions. The lesson for the online black American "community" to be extremely vigilant and double check the source of the information and the identity of the account holders before forwarding any messages.

While this technique has become well-known, this has not stopped it from being employed: at the end of July 2018, Facebook exposed an influence campaign involving fake profiles whose activities consisted in stirring hatred on both sides of a number of divisive subjects. In particular, one of the accounts created a counter-protest to a gathering of white nationalists which was planned to be held in Washington DC in August.[24]

The narratives supported by the Kremlin are numerous:

- conspiracy theories (Douma, Skripal) to sow doubt and distrust;
- *ad hominem* attacks to discredit a person or office (such as the rumor that British Prime Minister David Cameron put his penis into a pig's mouth—a story that Downing Street had to publicly counter as its ludicrousness did not prevent its spread);

24. Nicholas Fandos and Kevin Roose, "Facebook Has Identified Ongoing Political Influence Campaign," *The New York Times*, 31 July 2018.

• the "anti" narratives that attack our institutions (anti-EU, anti-NATO), our States (anti-Americanism) and our values (anti-migrants), that sometimes synergize with other issues (criticism of the EU is catalyzed by criticism of its migration policies and by the concept of "Eurabia," which refers to a European continent threatened by Islamization);

• provocateurs, on divisive issues, who set communities against each other: Russian-speaking minorities against local majorities, progressives against conservatives, the gay community against the homophobic community, etc.;

• historical tensions, those that lie in the darkest pockets of our respective national histories and that are vulnerable to exploitation, often with links, fictitious or proven, solid or tenuous, to Nazism;

• the moralizers, who try to demonstrate the moral decadence of the West (like the false story of the opening in Copenhagen of "the first zoophilic brothel in Europe" in October 2017).

Making use of history: the case of the Baltic States

First of all, there is a fundamental difference in interpretations of the Second World War. Russia claims to have liberated the Baltic States from the Nazis (which Russian-speakers celebrate on May 9th), whereas the Balts consider that they were occupied by the Soviets (1940-1941), the Germans (1941-1944) and then the Soviets again (1944-1991). History museums in the region place the Soviet and Nazi occupations on a similar footing, which is difficult for Russians to accept. This historical dispute is alive and well: in 2014, Latvia unilaterally suspended the bilateral commission of historians (although there was a recent announcement of the commission's reinstatement.) Russians tend to describe the Soviet (occupation) period as positive for Baltic States and try to minimize the crimes committed against Balts. For example, there is the idea circulating that the economic situation in the Baltic States has declined, that they were in fact much wealthier under the USSR—a "Soviet Silicon Valley"—and that their integration into the West allegedly crippled their high-tech industry.

Nazism persists as one of the most common narratives used by the Kremlin against the Baltic States (and Ukraine). In July 2017, NATO posted a video honoring the "Forest Brothers", who were Estonians, Latvians and Lithuanians who fought against Soviet occupation. The spokeswoman of the Russian Foreign Ministry reacted by saying that these "Forest Brothers" were "fascists" and "collaborators" with the Nazi regime. The Deputy Prime Minister of Russia tweeted that the "NATO clip about 'Forest Brothers' killing our soldiers confirms that in the face of NATO,

we are dealing with the heirs of Hitler's remnants." The Russian Mission to NATO also denounced the "shameful attempt to rewrite history [and] glorify inglorious former SS-fighters and nationalists to serve [the] political narrative of the day."[25]

Another historical narrative used in the region challenges the accession of independence for Baltic States, which is presented as both an error and a trap set by the West. According to the narrative, sooner or later, the Baltic States will return to Russia's sphere of influence. In light of this, the Continental Hockey League can also be seen as a way of reinvigorating old Soviet ties while demonstrating that, in this area at least, the Balts remain in the Russian zone of influence.

The strategic use of history can also be reflected in state monuments: the reconstruction and valorization of Soviet objects, including the graves of soldiers and monuments to the dead. This is the case in Lithuania, where both graves and monuments serve as "proof of Lithuania's inclusion in the Russian geopolitical space [and] serve as places to rally supporters of the Kremlin's policies."[26] The completion of rehabilitation work can also be a moment for celebration, with local dignitaries, diplomats and media coverage. Some sites are subject to serious contention and debate. For example, there is a memorial dedicated to the victims of communism in Tallinn that is currently under construction at the site of the Soviet memorial to the victims of the Great Patriotic War. This has generated controversy and debate in the Russian-speaking community and has been subject to complains from Moscow. Also noteworthy is the case of the "Bronze Soldier" , whose removal in 2007 from the center of Tallinn to a military cemetery at the outskirts of the city sparked riots and a wave of cyberattacks against Estonian websites.

C. Privileged places and mechanisms

Information manipulation derives its effectiveness from the viral character of its diffusion on the internet, by various relays, automated or otherwise. It is clear, however, that their viral character owes nothing to chance. It is the result of a thoughtful, coordinated and meticulously implemented strategy that relies on a chain of actors, culminating not only in the mass dissemination of manipulated information, but also on a sort of information "laundering" as it is taken up by actors from the media and various other institutions.

25. Donara Barojan and Ben Nimmo, "History Revisited: The Forest Brothers," DFRLab Medium.com, 18 July 2017. See also "The Nazi-obsession of pro-Kremlin propagandist," EUvsDisinfo, 21 July 2017.

26. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 44.

1. The places

The most advantageous place for manipulation is the digital platform. A platform is defined as "a service that acts as an intermediary by which to access information, content, services or assets that are edited or provided for by third parties."[27] The following characteristics are often added to this definition: "beyond its technical interface, [the platform] organizes and ranks content for the purposes of presentation and connection to end users."[28] This further highlights an essential function of these platforms, which do not simply edit the content diffused by its users in a neutral manner. Through the algorithms that these sites use, the platforms rank content and set the conditions for the diffusion of that content, which is then shared and published.

An attack against national defense and security

"Digital platforms, including social networks, can shape opinion more insidiously and are often vectors of values that are not those of the French Republic. In certain cases, they can be used for the purposes of disinformation and spreading propaganda to French citizens, particularly to the yougest ones. The opinions that are disseminated are therefore against France's fundamental interests and are an attack on defense and national security which is sanctioned by law."

(French National Digital Security Strategy, 2015, p. 20.)

This feature is very often underemphasized by the platforms themselves, who prefer to consider themselves as "technology companies" that host, more than edit, the information and content that is exchanged. The terminology is not neutral: the legal responsibility of those who edit content is much more constraining than that of the hosts. Therefore, even the way in which these platforms present their features, which is critical to defining their status, is a challenge for them. Such platforms have long been presented as technology companies that host, without editing, information and content.

27. French National Digital Council, *La Neutralité des plateformes*, June 2014.
28. *Ibid.*

Platforms today have, in large part because of outside pressure, modified their position and manner of approaching this subject. Mark Zuckerberg's statement to the US Congress in April 2018 perfectly illustrates this change of stance, especially when he acknowledged that Facebook is responsible for its content, even if it does not produce the content itself. This statement was surprising because it goes against the strategy employed by this particular actor in prior years. It signals an important paradigmatic shift: it is now time for platforms to rethink their status and, similarly, redefine the scope of their responsibilities.

This report focuses on "big digital platforms": Google, Facebook, YouTube and Twitter. These platforms benefit from networks effect, "these positive externalities of the information economy,"[29] which ensure them a large number of subscribers and a high rate of retention. They are therefore the most advantageous location for information manipulation campaigns, which by definition are massive and large-scale. In this respect, other digital platforms, which are restricted to smaller circle, are not the focus of this report. The term digital platform is in our view preferable to "social network". The term "social network" does not adequately cover the variety of actors involved in such activities and runs the risk of conflation with unrelated actors. For example, the "news" feature of Google is not a social network. It does, however, play a significant role in the dissemination of fake news as it has the power to increase or decrease the visibility of that information.

The Pro-Russian Twittosphere in France

Pétiniaud and Limonier use data analysis (Big Data) of social media networks—notably the "Pro-Russian Twittosphere"—to understand the Russian strategy in France. They show that the French "Russosphere" is "neither homogenous in terms of the individual profiles that compose it nor in terms of their political orientations. On the contrary, the French 'Russosphere' is a diverse galaxy of which a significant portion could exist even without Russia playing any role. However, we note that the 'central' accounts, whether they belong to political personalities or the Russian media, play an important role in terms of connecting and ensuring consistency."[30]

29. See *Plateforme et dynamiques concurrentielles*, Renaissance numérique, 2015.

30. Louis Pétiniaud and Kevin Limonier, "Cartographier le cyberespace : le cas des actions informationnelles russes en France", *Les Champs de Mars*, 30, Vol. 2 (supplement), 2018, p. 321.

Large digital platforms are not the only ones to relay and amplify information manipulation campaigns. These involve other digital actors:

• (Dis)information sites, such as those financed by Moscow (RT, Sputnik) or those with ideological affinities with the Kremlin, and "cloned sites" (ABCNews.com.co, nytimess.com, etc.).

• Discussion forums that have been at the forefront of many information manipulation campaigns. It was on 4Chan that the "Macron Leaks" were first published and attracted the attention of internet surfers. These users then quickly relayed the stolen information to major platforms (Twitter, Facebook). Indeed, discussion forums often serve as a launching pad for manipulation campaigns and for the propagation of rumors. Nevertheless, if discussion forums are susceptible to the spread of fake news, their users are often conscious of the controversial nature of the content exchanged and of the fact that the content is potentially untrue. The debate often takes place among a small group of users who exchange their opinions anonymously. Even if these forums eventually allow this fake news to achieve high visibility and affect public opinion, they are used, first and foremost, to launder false information, giving the impression that the information actually originated from actors who have no ties to the political aim pursued. It is important to note that during the "Macron Leaks," in particular, some of these forums (e.g. jeuxvideo.com) censored discussion boards that reported the stolen documents, observing that this was likely to fall under the purview of the law (specifically, criminal law).

• Messaging applications, such as WhatsApp and Telegram, are also used as vessels for information manipulation: on a number of occasions, false information was disseminated through discussion groups with a large number of subscribers. With the amount of mobile equipment in use being high and constantly growing, and the barriers to entry being minimal (i.e. to register for and acquire free applications), applications are a means of achieving a high threshold of exposure while enjoying a complete absence of moderation.

• The Darknet. Information manipulation campaigns can involve the use of stolen documents. Sometimes these documents are auctioned off and broadcast on the Darknet, a sphere that, because it does not abide by the rules governing the internet, is particularly conducive to the exchange of illegally acquired information.

The 7 stages of online propaganda

1. recognition of the target (research on the audience),
2. armament (preparation of the narratives and fake news, creation of background stories to make the disinformation credible and creation of alternative versions tailored to the different audiences),
3. massive dissemination (by all available means, social and traditional media),
4. activation of specific relays (military groups on social networks),
5. growth (purchase of advertisements, bots, trolls),
6. maintenance (by varying the stories, responding to objections),
7. laundering (traces of the original actor disappear once the goal is achieved, diversion of attention and suppression of online posts and even accounts).

2. Amplification mechanisms

Information manipulation is amplified by two particular mechanisms:

a. Bots

Firstly, automated or semi-automated actors, like bots or netbots. This tactic involves fake Twitter or Facebook accounts that allow for the rapid diffusion of fake news through biased retweets and likes. By "fake account," we refer either to an account that is managed by someone pretending to be someone else or to accounts that are not managed by people, but are automated (bots). The fake accounts on social media are "the foot soldiers in this form of warfare."[31] They work to amplify the message, introduce hashtags and intimidate or block other users.

These bots are very active and present on social networks: for example, Russian-speaking bots were responsible for 70% of the messages posted in Russian on the subject of NATO during the latter half of 2017.[32] In the case of the Irish referendum, it is also estimated that 14% of the 165,323 #Savethe8th tweets, an anti-abortion hashtag, originated from accounts with digital pseudonyms while 6% of tweets originated from accounts without locations.[33]

31. Ben Nimmo, In his hearing before the Singaporean committee, 22 February 2018.
32. NATO StratCom CeO, *Robotrolling* 2/2017.
33. Rachel Lavin and Roland Adorjani, "L'Irlande a déjà trouvé la parade aux fake news (mais on ne pourra pas la reproduire)," *Slate*, 13 June 2018.

While bots often play an important role in amplifying operations, this is not always the case: each campaign is different and, in some circumstances, the aggressor prefers to use human relays. For example, during the electoral campaign for the 2018 Colombian presidential election, the amplification process was essentially human, originating from politicians or notable supporters from both political camps.[34]

b. Trolls

Secondly, there are internet trolls: individuals who spread information, saturate certain websites with comments, and/or harass others. This activity is partly institutionalized (see box below), but is also carried out autonomously by individuals of all nationalities. Moscow began developing "troll factories" in reaction to the protests in the Winter of 2011-2012, which were organized through social networks (mainly VKontakte and LiveJournal). A large number of Kremlin supports suddenly appeared on these networks to create controversy, sow discord, and ultimately weaken the adversarial communities. Since 2012, the international media has drawn attention to the role of the *Nashi* movement: a group of young nationalists who support President Putin through activities such as trolling and hacking.[35] The first mention of a "troll factory" dates back to 2013 (see box below).

IRA, the troll factory in St. Petersburg

The Internet Research Agency (IRA) is a Russian company located in St. Petersburg. In reality, it is a "troll factory" financed by the Kremlin, whose existence was discovered in 2013 by Russian journalists pretending to be candidates applying for jobs there.[36] The regional press, including Finnish and Polish news outlets,[37] then got hold of the story, followed by

34. Jose Luis Peñarredonda, "#ElectionWatch: Everyday Misinformation in Colombia: Humans, not bots, were the main vectors of misinformation," @DFRLab, Medium.com, 20 July 2018.

35. Miriam Elder, "Polishing Putin: hacked emails suggest dirty tricks by Russian youth groups," *The Guardian*, 7 February 2012.

36. The first revelations are dated around August-September 2013. See Ben Nimmo and Aric Toler, "The Russians Who Exposed Russia's Trolls: A tribute to the Russian journalists who exposed the 'troll factory,'" DFRLab Medium.com, 7 March 2018.

37. Jessikka Aro, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View*, 10 May 2016.

the international press,[38] US intelligence,[39] and finally Special Prosecutor Robert Mueller. In the midst of his investigation into Russian interference, in February 2018, Mueller indicted the IRA, two companies owned by Yevgeny Prigozhin who created the IRA (Concord Catering and Concord Management and Consulting), as well as 13 individuals, one of whom was Prigozhin himself.

The IRA is accused of having led an operation to influence the American electoral campaign. Registered in July 2013, the IRA would have begun targeting the United States around April 2014 and was receiving funding ($1.25 million per month during the campaign) from 14 affiliated companies in Concord. In 2015, hundreds of young Russians were employed at the IRA, working 12 hours a day in a highly organized fashion: there were bloggers writing posts, news editors making reference to these posts, trolls commenting on them and communicators active on all social media.[40] They were briefed on the Kremlin's positions on all topics of debate and a "foreign bureau" briefed them on the state of the American debate on divisive issues (such as racism, firearms, immigration, LGBT, taxes, etc.). Through fake accounts and bots, a few dozen people have succeeded in reaching 150 million people through Facebook and Instagram. The IRA alone controlled 3,814 human accounts and 50,258 bots on Twitter, with which 1.4 million Americans interacted. They also had at least 470 Facebook accounts that reached at least 126 million Americans (with $100,000 USD spent on advertising). The indictment of the US Special Prosecutor has provided detailed information on the operations of the agency. It does not, however, accuse the Russian government of anything nor does it acknowledge that the IRA succeeded in influencing the vote.

The Kremlin does not appear concerned with the international attention that the IRA has garnered in over the past few years: in 2017, the agency moved in order to expand its activities, going from 4,000 to 12,000 Sqm^2 of office space.[41] While this agency showcases this phenomenon, it draws attention away from other troll factories present elsewhere on the Russian territory, as well as abroad. However, the IRA is not an isolated case, and must not become the tree that hides the forest.

38. Shaun Walker, "'Salutin' Putin: Inside a Russian Troll House," *The Guardian*, 2 April 2015; Adrian Chen, "The Agency," *The New York Times*, 2 June 2015.

39. Office of the Director of National Intelligence (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections*, Washington DC, January 2017.

40. Ben Popken & Kelly Cobiella, "Russian Troll Describes Work in the Infamous Misinformation Factory," *NBC News*, 16 November 2017.

41. "Figure of the Week: 12,000," EUvsDisinfo, 9 January 2018.

These mechanisms played out fully during the American presidential campaign of 2016. In 2015, Russian trolls and bots began exacerbating racial tensions (#BaltimoreVsRacism, #FergusonRemembers), fear of jihadism (#TexasJihad, #ISISinGarland), the debate on firearms (#NoGunsForCriminals, #GunViolenceOregon), homophobia (#IndianaFedUp), etc., and began attacking Hillary Clinton. It was during 2016 that the first coordinated operation took place, involving cyberattacks and information manipulation, against Hillary Clinton and in favor of Donald Trump.[42]

Trolls do not serve only as relays: they also have more active and aggressive functions. Trolling generally proceeds in three stages, inspired by fishing:[43] baiting, biting the hook and hooking the catch. First, the troll posts a controversial message to provoke a reaction. If no one challenges the message, the troll may do so himself by posing as a third person who challenges the post or, alternatively, supports the post but in so exaggerated a manner that he provokes a reaction and draws others into the exchange. When a user has "bitten" the hook by engaging in the discussion, the troll reels him in by systematically challenging his comments. To keep the "discussion" going, the troll varies the characters involved and the tone of the comments from insult to irony.

There are several types of trolls. A study by the NATO Center of Excellence for Strategic Communications has identified five types[44]: "blame the US conspiracy trolls" (that always see an American hand behind the scenes) that create distrust, "bikini trolls" (that pose as attractive young women) that draw attention, "aggressive trolls" that intimidate and dissuade people from participating in certain activities and discussions, "Wikipedia trolls" that edit the content of pages, and "attachment trolls" that post links to pro-Russian content.

Among them, the aggressive trolls that proceed through intimidation, brutality and even harassment are the most effective means of saturating the debate and silencing opposition voices. A number of investigative journalists and well-known personalities, who are opposed to Russian interests, have been the victims of such attacks. This was the case for Finnish journalist Jessikka Aro who dissected the intimidation techniques

42. For a study of Russian interference in the American campaign, see Boris Toucas "*L'Affaire russe" : la démocratie américaine ébranlée*, IFRI Research Paper, Potomac Papers, 32, December 2017.

43. Robert Szwed, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, NATO Strategic Communications Centre of Excellence, May 2016.

44. *Internet Trolling as a tool of hybrid warfare: the case of Latvia. Results of the study*, NATO Strategic Communications Centre of Excellence, 2016.

used by trolls.[45] Since journalists are particularly targeted, the NGO Reporters Without Borders (RSF) dedicated a report to this issue.[46]

In order to discredit someone, trolls often accuse the person of colluding with foreign intelligence services and/or of committing treason. To make them crack, they use insults, humiliation and threats (rape and death threats), repeatedly (sometimes sending dozens of messages an hour). They may also use illustrations (such as drawings or memes).[47]

The spiral of silence is well known to authoritarian regimes: internet surfers tend not to share their viewpoints if these viewpoints go against the dominant opinion of the forum. In this way, a few trolls can, by posting a number of comments, give the impression of a majority opinion even when it is not at all the case—it is enough to have a paralyzing effect on others. This technique consisting of giving an appearance of popularity is called "astroturfing," a reference to a brand of artificial turf (AstroTurf). The trolls thereby participate in a wider phenomenon, which is the brutalization of online public debate. Trolling "designates both the banalization of expressive violence and the radicalization of the opinions it engenders."[48]

Some researchers have become experts in the study of trolls. This is particularly true of Ben Nimmo, a researcher at the Atlantic Council, who regularly uncovers networks of trolls and provides detailed descriptions on their functioning.[49] These analyses are extremely useful for detecting and, *in fine*, countering them.

D. Leaks

The phenomenon is nothing new (Pentagon Papers in 1971, Watergate in 1972-74) and has actually been accelerating for several years. In fact, around forty cases were identified from 2006 to 2017[50] (the most known cases being the 2010 American diplomatic telegrams on Wikileaks, the

45. J. Aro, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View*, 10 May 2016.

46. RSF, *Online Harassment of Journalists: Attack of the trolls*, 2018.

47. Carly Nyst and Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, *op. cit.*, p. 13.

48. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 65.

49. See for example Ben Nimmo, "#TrollTracker: From Tags tTo Trolling: How tweets to a small group precede attacks on critics of the Syrian and Russian regimes," @DFRLab, Medium.com, 27 June 2018 and "#TrollTracker: Russia's Other Troll Team: Mueller points to existence of second Russian troll operation focused on activist groups and foreign policy," @DFRLab, Medium.com, 2 August 2018.

50. Pierre Gastineau and Philippe Vasset, *Armes de déstabilisation massive. Enquête sur le business des fuites de données*, Fayard, 2017.

2013 Offshore Leaks, the 2014 LuxLeaks, the 2015 SwissLeaks, the 2016 Panama Papers, the 2017 Paradise Papers, and the 2016 Football Leaks). Initially this was the sole work of "whistleblowers," ostensibly motivated by the virtue of transparency (all the while remaining anonymous themselves). However, this method is increasingly used to serve political or economic interests. In this way, leaks may form part of an information manipulation campaign, such as is evidenced by the American presidential election (2016 DNC Leaks) and French presidential election (2017 Macron Leaks), As such, they can be used to discredit a target, who may be either a victim of hacking, or a third party.

This has the advantage of lending the impression to a target population that they have access to the truth, to crude, unfiltered information, particularly since it was obtained through interception (conversations, emails, documents). While this may occasionally be the case, it is equally possible that these documents were manipulated between the time they were obtained and the time they were publically released, as was the case in the "Macron Leaks" (see below). These are referred to as "tainted leaks."[51] They are all the more difficult to detect since the modifications are subtle and credible, and the altered files are surrounded by authentic documents. Journalists would have a lot of trouble with verifying these documents because they do not in general have access to the original source. The most serious journalists cover these types of events with extreme prudence, looking at the leak itself as well as its content, but they are a small minority: the vast majority simply relay the information without any filter.

E. The falsification of documents

One of the most common methods—though crude and relatively easy to detect—is the falsification of documents:

- Images. (In November 2017 on social media, the Russian Defense Minister presented an image supposedly taken on the Iraqi-Syrian border as "irrefutable proof" of American support for ISIS. This image was actually a screenshot of a video game.[52] In Sweden, there are several famous cases, such as the image of a car on fire which supposedly illustrated the rising crime rate caused by migrants. The image in question was actually taken in Sofia. There was also the image of a young

51. Adam Hulcoop *et al.*, "Tainted Leaks: Disinformation and Phishing With a Russian Nexus," *The Citizen Lab*, 25 May 2017.

52. Eliot Higgins, "The Russian Ministry of Defence Publishes Screenshots of Computer Games as Evidence of US Collusion with ISIS," Bellingcat, 14 November 2017.

blond boy who was allegedly wounded by migrants "because his eyes are blue." In reality, the photo was of a young Welsh girl attacked by her dog in 2008.);

• articles in reputable newspapers. (In Sweden again,[53] in May 2016, a fake article by *Dagens Nyheter*, the country's leading newspaper, on former Foreign Minister Carl Bildt. In France, in March 2017, during the presidential campaign, a fake article appeared in a Belgian newspaper *Le Soir* alleging that Emmanuel Macron was the preferred candidate of Saudi Arabia. This article was circulated by a number of people, including Marion Maréchal-Le Pen, before being identified as a fake news story. This particular article imitated the web layout of *Le Soir* but used a different address, lesoir.info instead of lesoir.be);

• internet sites. (In Finland, Johan Bäckman distinguished himself by creating a fake site for the European Centre of Excellence for Countering Hybrid Threats that was so believable that even some of the ambassadors invited to the opening of the center had the wrong address.)

When the falsification involves text—or images, such as "memes" which have become very popular—the quality of the language can be a useful means of detecting distortion as manipulators usually rely on automatic translators like Google Translate. That said, as these tools improve, detection will become more difficult (see the section below on future challenges).

F. Electoral interference

Electoral interference can target systems (electronic voting, voting lists), which consequently affects the population's confidence in the results, or the voters themselves in order to influence their vote.

After studying dozens of cases of interference in cyber-democratic processes in nearly 40 countries on five continents in the past ten years, Canada's Communications Security Establishment (CSE) concluded that three-quarters of the activities involved sophisticated methods (i.e. were probably orchestrated by States) for strategic objectives. Only a quarter of these activities employed less sophisticated means for criminal

53. The falsification of documents, image and text is apparently a preferred method against Swedes: Martin Kragh and Sebastian Åsberg have identified 26 fake articles between 2015 and July 2016 ("Russia's strategy for influence through public diplomacy and active measures: the Swedish case," *Journal of Strategic Studies*, 2017).

purposes (i.e. stealing voter information, probably for resale). There is a worrying "upward trend in the amount of cyber threat activity against democratic processes."[54] This increase is attributable to a combination of factors: the democratization of cybercapacities, which are increasingly easy to access; weak capacity for attribution (only 20% of incidents are attributed), prevention and punishment (most incidents go unpunished); the exponential growth of social media; the fact that more electoral organizations are using online processes, which are by definition more vulnerable; and finally the fact that certain successes incite other attackers (by emulation or imitation).

There are multiple vulnerabilities in the democratic process. The first component concerns elections, beginning with voter registration. If registration is completed online, adversaries can modify the databases (by slipping in fake voters' files), render them inaccessible (by encrypting the data, for example), and erase or steal the data (to sell or use the personal information). At the very least, this interference slows down the election process and leads voters to question the integrity of the election's outcome. Online voting is undoubtedly the most vulnerable, since it is then possible to attack the site or fill out virtual ballot boxes. Even manual voting is also vulnerable if there are counting machines that could be modified before the vote to falsify or erase data. In addition, dissemination of the election results online makes those results vulnerable to interception and modification by a third party. If the news of the results is affected, the consequences could be serious (long delays, loss of public confidence in the electoral process, even challenging the election outcome). Finally, at any moment in the process, the aggressor may also target critical infrastructures that are needed for organizing elections, such as the power grid.

Second, parties and politicians are vulnerable to a number of threats. Party databases contain extensive personal information on millions of people. For this reason, they are choice targets for commercial purposes (i.e. the resale of personal information on the Darknet) as much as for strategic purposes. These attacks may damage the party (by deleting, modifying or encrypting data) or individuals (by using the information collected to discredit or blackmail). In addition, the presence of a candidate on the internet (his or her official site, his or her social media pages) can also be hacked (pages deleted, blocked, defaced). The risks to

54. CSE, *Cyber Threats to Canada's Democratic Processes*, June 2017, p. 32.

one's reputation—and in some instances, the risk of physical harm—can persuade certain candidates to pull out of the race. There is also the risk of collusion, that is to say, of foreign powers providing illegal financial or logistical support to certain candidates in order to try and influence the campaign and the outcome of the vote. This is illustrated by the American Special Prosecutor's investigation on what has come to be known as the "Russian Affair."

Third, the media may be a target. This is where information comes directly into play, especially on social media (see above).

Referenda are particularly suited to electoral manipulation for several reasons: firstly, they generally relate to controversial, divisive issues that are quick to incite emotions. Secondly, the consequences of their results are complex and sometimes difficult to assess even when the proposed choices, which are generally binary, appear simple (i.e. independence/non-independence, exiting the EU/remaining in the EU).

After the 2014 referendum on Scottish independence showed that a majority (55%) wanted to remain in the UK, the Russian media tried to discredit the results, as they did not suit their liking. They interviewed so-called "experts" who claimed that the vote did not respect international standards and supported a petition. Although ultimately in vain, it nonetheless acquired over 100,000 signatures.[55] Other significant instances of information manipulation include the 2016 referenda on the approval of the Association Agreement between Ukraine and the EU in the Netherlands and on the United Kingdom EU membership.

55. Ben Nimmo interviewed in Severin Carrell, "Russian cyber-activists 'tried to discredit Scottish independence vote'," *The Guardian*, 13 December 2017.

Five stages of election interference

By comparing interference in the American, French and German elections in 2016-2017, Finnish researcher Mika Aaltola produced a model of election meddling involving five stages:[56]

1 - "Using disinformation to amplify suspicions and divisions": accentuating political polarization, tensions, etc.

2 - "Stealing sensitive and leakable data."

3 - "Leaking the stolen data via supposed 'hacktivists'" or whistleblowers. It is the spread of data, more than the theft itself, that has an effect on the population, provided that one knows where—or rather, to whom—and when exactly to disseminate the data. These two criteria (targeting and timing) are crucial.

4 - "Whitewashing the leaked data through the mainstream media." Boris Toucas underlines the tertiary role played by whistleblowers, who use their "critical credibility" to pass the information on to the mainstream media where it is further developed.[57] **The first among them, WikiLeaks, has been relatively discredited since the American elections**[58] **but it remains popular among a certain demographic and retains a large number of followers.**

5 - "Secret collusion": links between a foreign State and a party, candidate, etc.

The interference in the American election, which served as a model for the author, passed through these five stages. The meddling in the French election did not exceed stage three because the traditional media did not succumb (see below), while the interference in the German election did not exceed stage two.

56. Mika Aaltola, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Aurocratic Meddling*, FIIA Briefing Paper 226, November 2017.

57. Boris Toucas, "Exploring the Information-Laundering Ecosystem: The Russian Case," CSIS Commentary, 31 August 2017.

58. Julian Assange did not hide his support for candidate Donald Trump and Wikileaks relayed a certain number of fake news stories that were hostile towards Hillary Clinton (including the famous Pizzagate). By edging in the direction of the American alt-right and becoming an ally of the Kremlin, Wikileaks disappointed many of its initial supporters. See in particular Kevin Poulsen, "Defector: WikiLeaks 'Will Lie to Your Face'," *The Daily Beast*, 8 May 2018.

The midterm elections of 2018

The American presidential election of 2016 was marked by the hacking of Democrat servers and the dissemination of thousands of documents on Wikileaks (DNC Leaks), among other measures relating to the information manipulation campaign that was underway. The investigation led by Special Prosecutor Robert Mueller since May 2017 has highlighted the role of Russia in what appears to be interference. Digital platforms equally updated and suspended thousands of accounts that appeared to be created and controlled by Moscow, particularly via the IRA (see above). In the current context, with daily revelations about the scope of the 2016 operations, American authorities are particularly concerned with avoiding repetition of the same incident during the midterm elections which will be held on 6 November 2018.

Echoing the concerns of the American intelligence community, Dan Coats, the Director of National Intelligence, had already said back in February 2018 that "the midterm elections of 2018 remains a potential target for Russian influence operations."[59] By the end of July, his fears were confirmed as Facebook announced that it discovered and neutralized a network of around 30 fake Facebook profiles and Instagram accounts involved in the preparation of a "coordinated" operation, quite similar in fact to what the IRA was doing.[60]

The reaction of the authorities is however stunted by a lack of political unity, between Democrats and Republicans and within each party; a lack of coordination between numerous administrative structures dedicated to the fight against information manipulation (the Department of State, the Department of Justice, the Department of Homeland Security), intelligence services, etc., see below); the reluctance to share information with the private sector. The first meeting between federal agencies and digital platforms in preparation for the elections took place only six months before the elections, at the end of May at Facebook's head office[61] and at the request of private companies, not the government. Several voices highlighted the importance of this public-private cooperation and the necessity for sharing information with digital platforms if we expect them to effectively engage in the fight against these threats.[62]

59. Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the record, 13 February 2018.

60. Nicholas Fandos and Kevin Roose, "Facebook Has Identified Ongoing Political Influence Campaign," *The New York Times*, 31 July 2018.

61. Sheera Frenkel and Matthew Rosenberg, "Top Tech Companies Met With Intelligence Officials to Discuss Midterms," *The New York Times*, 25 June 2018.

62. Joshua A. Geltzer and Dipayan Ghosh, "How Washington Can Prevent Midterm Election Interference," *Foreign Affairs*, 25 July 2018.

During the crisis in Spain in September-October 2017 resulting from the referendum on self-determination for Catalonia, the Kremlin seems to once again have blown on the embers. Catalonia is not and has never been a concern for Moscow. The vote was an opportunity for the Kremlin to divide—and thereby weaken—European States.

During the crisis, the Russian media, with RT and Sputnik at the head, produced indulgent, sensationalist coverage of the Catalan movement, spreading all kinds of fake news ("Catalonia will recognize Crimea as Russian," "In Catalonia, Spanish is studied as a foreign language," "European officials supported violence in Catalonia," etc.). A variety of stories suggested that the Balearic Islands were, in turn, demanding independence, publishing false maps indicating which European States supported independence (the United Kingdom, Scandinavian and the Baltic States were indicated as supporters of Catalan independence). They drew parallels with Ukraine (Catalonia would be the Donbass of Europe, Spain would make "the same mistakes" as Ukraine). They even compared it with Kosovo, in one soberly titled article, "Why is NATO not bombing Madrid for 78 days?"[63]

The Spanish-language versions of RT and Sputnik are relatively influential as they are widely read in Latin America, especially in Venezuela and among Chavist movements. During the Catalan crisis, these outlets effectively served as relays for Moscow. This has been confirmed by a study of more than 5 million messages posted on social networks, which shows that the majority of the most active accounts that reposted the content of RT and Sputnik were Chavist or Venezuelan accounts (32%), followed by anonymous accounts (30%) and fake or automated accounts (25%). Their geolocation confirms that Venezuela is the second most common origin of these messages after Spain.[64]

Personalities from the digital world such as Julian Assange and Edward Snowden suddenly became passionate about the Catalan issue. WikiLeaks went so far as to ask *El País* to fire David Alandete, who was investigating Russian interference.

63. There are numerous examples in the EUvsDisinfo database. See also the report: The Integrity Initiative, *Framing Russian meddling in the Catalan question*, October 2017.

64. David Alandete, "Russian network used Venezuelan accounts to deepen Catalan crisis," *El País*, 11 November 2017.

III. Other regions affected by information manipulation

While the post-Soviet space, Europe and North America are, for the moment, the areas where the main examples of information manipulation are taking place, other areas of concern are emerging, especially in the Middle East, Africa and Latin America. The vulnerability of these populations to information manipulation attacks is heightened by several factors: the presence of conflict and/or an authoritarian government; the absence of sufficient trustworthy and credible information; hightened fears and emotions, be it as a result of these structural causes or of a particular event such as a terrorist attack or a natural catastrophe. Democratic transitions and elections also provide fertile ground for information manipulation, as does the rapid growth in digital connectivity, particularly in rural zones where the population is less educated and has a stronger tendency to believe in online rumors.

A. The Middle East

1. Syria

Russian information operations are expanding in the Middle East. The case of Syria is the most well-known, but it is not the only one. In January 2016, the "South Front: Analysis & Intelligence" website (southfront.org) was launched. It claimed to be a product of a team of experts and volunteers from the four corners of the Earth but it "looks more like a professional info-war project run or backed by the Russian military."[65]

Since 2013, the White Helmets, a Syrian humanitarian organization operating in opposition-held areas to save civilians, has been the target of a massive, systematic and coordinated information manipulation campaign.[66] This campaign has continued to spread two main messages over the past five years: on the one hand, that the organization works closely with the Syrian branch of Al Qaeda and could, therefore, be described as a terrorist organization. On the other hand, the organization is alleged to be responsible for several "false flags," whose purpose was to incriminate Damascus and provoke Western strikes. These accusations have been made five times against the White Helmets since 2013.

65. Jessikka Aro, "The Cyberspace War," *op. cit.*, p. 126.

66. Olivia Solon, "How Syria's White Helmets Became Victims of an Online Propaganda Machine," *The Guardian*, 18 December 2017.

The media ecosystem behind this disinformation campaign involves Iranian, Russian and pro-Assad media. Other regions, notably Latin America through TeleSur and anti-imperialist networks, echo this disinformation.[67] The strategic alliance between these various actors in Syria doubles as a united and coordinated front on social media.[68]

This systematic defamation operation makes it possible to achieve several strategic objectives: 1) it lends credibility to the narrative propagated by the Assad regime and its allies, namely that in Syria the only two options were Bachar el Assad or the jihadists, without any other possible alternative emanating from civil society; 2) it discredits information from the ground regarding the humanitarian situation and the shelling and abuses carried out by the Syrian regime and its allies. Ultimately, any initiative to counter impunity in Syria can be invalidated if it is based on the testimony of the White Helmets; 3) it accuses the White Helmets of staging fake chemical attacks and generates uncertainty about the responsibility of the Syrian regime for such attacks.

The Douma chemical attack of 7 April 2018, which sparked outrage from the international community and caused American, French and British strikes a week later, led to the publication of a wide variety of fake news stories in the Russian media. These stories ranged from outright denial (claims that there was no chemical attacks, no patients in hospitals, and that photos and testimonies were completely fake) to conspiracy theories (that this was a scheme by the White Helmets, Westerners or the British to divert attention from the Skripal affair), to defending the regime (by arguing that "everyone knows" that Syria does not have chemical weapons) and finally Godwin's law (that the West uses the methods of Nazi propaganda in Syria).

This information manipulation campaign is, therefore, a central element of the combined strategy of Russian, Iranian and pro-Syrian regime networks in the propagation of a narrative which seeks to discredit all forms of opposition or action against impunity for the war crimes committed in Syria. It also demonstrates that NGOs can be targets, an issue that is witnessed elsewhere in the world (Muslim foundations in the United States, NGO assistance to refugees in Europe, etc.).[69]

67. "Los Cascos Blancos, artistas del montaje," TeleSur, 17 April 2018.

68. Donara Barojan, "#SyriaHoax, Part Two: Kremlin Targets White Helmets," DFRLab Medium.com, 20 February 2018.

69. Sarah Oh and Travis L. Adkins, *Disinformation Toolkit*, InterAction, June 2018.

2. The Gulf

Other States have been able to orchestrate foreign information manipulation operations, or in other words, information interferences. On May 23, 2017, the eve of President Trump's official visit to Saudi Arabia, the Qatar News Agency (QNA) published a statement online by Emir Tamim bin Hamad al-Thani which was directed at the Trump Administration. The Emir criticized the "negative ambitions" of its Gulf neighbors, calling Hamas "the legitimate representative of the Palestinian people" and announcing that Qatar had "excellent" relations with Israel.[70] A few minutes later, the QNA's Twitter account posted three messages revealing the existence of a plot against Qatar, attributed to Saudi Arabia, Kuwait, the United Arab Emirates, Bahrain and Egypt. It further announced the recall of Qatari diplomats from these five countries and the dismissal of these countries' ambassadors to Doha. Major media outlets in the region, including those in Saudi Arabia and the UAE, quickly spread these statements, which triggered a crisis.

The Qatari government then revealed that "the Qatar News Agency (QNA) website has been hacked by an unknown entity" and that a "false statement attributed to His Highness has been published." The QNA's Twitter account had also been hacked. Qatari technicians took more than nine hours to regain control of them.

Upon request from Doha, the FBI conducted an investigation and concluded that the QNA had indeed been hacked.[71] The Qataris blame Yousef al-Otaiba, the UAE's influential ambassador to Washington, for having orchestrated this virulent anti-Qatari media campaign.

The rest is well-known. As of June 5, Saudi Arabia, the UAE, Egypt and Bahrain have worked to isolate Qatar, by recalling ambassadors from Doha, imposing a trade embargo, refusing to allow Qatari planes to enter their airspace, and launching an offensive, international media campaign. These States quickly submitted an ultimatum to Qatar with a list of thirteen conditions for lifting the sanctions (such as limiting relations with Iran, shutting down Al-Jazeera and other media, closing the Turkish military base under construction, and severing ties with a list of "terrorist" organizations, including the Muslim Brotherhood and

70. Nabil Ennasri, "Reprise de la guerre froide du Golfe," *Orient XXI*, 31 May 2017.

71. Karen De Young and Ellen Nakashima, "UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence official," *The Washington Post*, 16 July 2017.

Hezbollah). These conditions were immediately deemed unacceptable by the Qatari government.

B. Africa

The practice of information manipulation in Africa is marked by several distinct features: just as mobile technology skipped a technological generation to reach the age of the smartphone (and its accompanying social networks), so too has disinformation been grafted, adapted and developed to fit this innovation which is now available to all. Influencers (actors on these social networks that can issue, validate and/or repost this information to various audiences) play a role in shaping and distorting popular information, in States where public information is largely questionable (because of the quality or limited independence of the media).

1. The next playground for Russian "information warfare"?

There are several indications that Africa could be the next playground for Russian "information warfare," especially since French and English are easy languages with which they penetrate the African continent. The work of a French research team revealed the growing spread of Russian content through the French-speaking African web.[72] This success is due to a combination of several factors. First, the widespread popularity of anti-Western rhetoric propagated by major Russian international media outlets (RT and Sputnik). The African public often views Russia through the lens of its anti-colonial Soviet past. In some countries, such as the Côte d'Ivoire, this rhetoric fuels local political debates. Thus pro-Gbagbo movements find the information and narratives produced by Russian media to be quite opportune. The choice made by RT and Sputnik editors to strongly publicize certain issues of direct interest to the African public, such as those affecting the future of the CFA franc, naturally aggravates matters.

Another problem is the tendency of many African online newspapers and media to republish Russian media content on their websites alongside news items from major Western agencies such as AFP and Reuters. This

72. The Observatory of the Russian-speaking cyberspace headed by Kevin Limonier, lecturer at Paris 8 University, researcher at the French Institute of Geopolitics and at the Castex Chair of Cyberstrategy. See his research paper to be published in the near future by IRSEM.

practice helps Russian content reach a large audience by simply being visible to a large number of people. In Senegal, for example, many of Sputnik's articles on Africa are picked up by seneweb.com, the fourth most visited site in Senegal. Seneweb is followed by more than 1.5 million people on Facebook.

In addition, digital marketing strategies used by Russian agencies on social networks (buzz, clickbait) are particularly well-suited to the African context, where many users rely on Facebook as a source of information. The conspiracy theories and other sensationalist news that the Russian media are fond of publishing allow them to increase their audience as tabloid-style media is very popular in Africa.

Part of the African youth is fascinated by the figure of Vladimir Putin—to whom many fan pages are devoted on Facebook—and the image of military might that is associated with him. Moscow's position on the Syrian conflict has also been the subject of many debates on social networks in the Maghreb (and more particularly in Algeria).

Until now, the activity of Russian platforms on the African continent was unstructured and their popularity could be understood as a collateral effect of the efforts directed towards French public opinion. But now, both RT and Sputnik plan to expand their network of correspondents in Africa. As an indication of this new strategy, the Facebook page of RT in French saw its audience increase significantly in January 2018 (around +60% in web traffic). The vast majority of these new viewers are young men from the Maghreb and Sub-Saharan Africa. It is unclear whether these are real profiles or bots.

2. The anti-French campaign in Goma

On 2 January 2018 in Goma, the Democratic Republic of Congo (DRC), a digital campaign called #BoycottFrance was launched. The Lucha, a citizen movement, spread its slogan on Twitter: "To condemn is not enough. Let us unite in the #BoycottFrance campaign in the Congo and wherever the African people are oppressed and France is complicit." More specific accusations targeted the French diplomatic presence in Goma: the *Institut français* was compared to a "French intelligence cell made to loot the resources of Kivu." Two caricatures published on Twitter and widely shared on social media accompanied this campaign. Under the headings "The sponsors of barbarity in the DRC" and "The heirs of Leopold II in the DRC," these images intended to denounce alleged French support for Joseph Kabila.

Their success has three dimensions: the popularity of the caricaturist Kash, the explicit slogans from Lucha and the references borrowed from the idea of *Françafrique* (the barrel of Total oil, a machine gun to signify military support and skulls on the ground to signify the Rwandan genocide). These references are mixed with real facts that cannot be linked to French diplomatic actions, such as the ongoing Total negotiations or the presence of the Themiis training institute. Key to this campaign was the reinterpretation or clustering of facts that have no causal link with one another. This had the effect of both inspiring new rumors and feeding existing ones, and it only took the circulation of some fake news to trigger the campaign. The paradox is that this attack was carried out by actors (La Lucha and Kash) with whom the French Embassy is in contact. The reflection on the ways to get rid of such fake news or to counter the viral nature of such caricatures and come up with alternative methods of communication, should take into account the unique character of online communication today on the African continent.

C. Latin America

The relative neglect toward Latin America by many Western States has presented several geopolitical entrepreneurs with the opportunity to build new partnerships at little expense, under the banner of post-Western multipolarity.

Since the mid-2000s, different economic, political and media strategies have been attempted in Latin America: by China (natural resources, infrastructure, education), by Iran (cultural centers, media), by Syria (mobilization of Syrian-Lebanese diasporas, social networks[73]) and by Russia (trade, military cooperation, energy, media).[74]

RT began broadcasting in Spanish in 2009. The channel now has offices in Argentina, Venezuela, Cuba, Nicaragua and Madrid as well as in North American urban centers where Latino communities are concentrated, like Miami and Los Angeles. According to the Atlantic Council,[75] RT's audience is significantly large in these communities, judging by the activity on the Spanish channel's Facebook page: 5.8 million subscribers as compared

73. Janaina Herrera, "La crise syrienne au prisme latino-américain (Venezuela, Brésil et Argentine)," *Les Carnets de l'Ifpo*, 14 September 2012.

74. Julia Gurganus, "Russia: Playing a Geopolitical Game in Latin America," Carnegie Endowment for International Peace, 3 May 2018.

75. Donara Barojan, "#ElectionWatch: RT y Sputnik Hablan Español," DFRLab Medium.com, 12 February 2018.

to 4.9 million for the English page. Sputnik has also been available in Spanish since 2014. It is namely through these South American networks that Russian media were able to play a role in the Catalan crisis (see above).

This investment in Spanish-language channels has been accompanied by a strategy of creating partnerships and amplifying information on social networks. The broadcasting of RT programs has been facilitated by hundreds of specific agreements with national media and some programs are being jointly produced with the Venezuelan channel TeleSur.

This method makes it possible to disseminate a common world view based on anti-imperialism, criticizing liberalism, and generating public awareness on matters to which the Kremlin holds dear (denunciation of Western Russophobia, highlighting the failures and crimes of the West, tying the color revolutions to conspiracy and terrorism). It should be emphasized that this worldview corresponds to important trends in Latin American public opinion and that this editorial orientation does not preclude the production of good quality programs.

Today, Latin America offers extremely fertile ground for information manipulation because of a convergence of economic and structural factors:

- massive use of social networks, especially Facebook[76] and WhatsApp, which allow communities to virally circulate unverified information between acquaintances and trusted persons;
- a generally unfavorable socioeconomic context, particularly in Venezuela, Mexico and Brazil, which is reflected in widespread discontent and insecurity;
- a normative framework that is less demanding than that of Europe or the United States in terms of the right to privacy and political marketing on social networks;
- strong polarization, resulting in the rise of populism and far-right candidates;
- a series of important elections in six countries in the region, including Brazil, Mexico, Colombia and Venezuela.

In both Brazil and Mexico, several detailed reports have documented widespread use, from all political parties, of bots and trolls on social

76. Brazil is the third country after India and the US in terms of Facebook users, followed by Mexico. There are also 120 million WhatsApp users in Brazil.

networks,[77] and of the extreme polarization of exchanges. Several months before the Mexican federal elections of July 1st, 2018, H. R. McMaster,[78] then President Trump's National Security Advisor, publicly denounced the implementation of a sophisticated strategy of Russian influence in favor of leftist candidate Andrés Manuel Lopez Obrador. The Kremlin would, in this scenario, be interested in seeing an ally rise to power in Mexico and destabilize its large northern neighbor. Mexico and the US already have tensions (on issues such as immigration, NAFTA and the fight against drugs). At this point, there was indeed an editorial line from RT and Sputnik that openly supported Obrador. Having said that, the other camp did not stand idly by. On the eve of the election—which saw the victory of Obrador—a detailed analysis by Ben Nimmo and his colleagues at the Atlantic Council's Digital Forensic Research Lab, uncovered the existence of a network of several million bots and dozens of disinformation websites that were being used against Obrador, likely by the entrepreneur Carlos Merlo, sometimes described by international media as the "fake news millionaire."[79]

77. Dan Arnaudo, "Computational Propaganda in Brazil: Social Bots during Elections," in Samuel Woolley and Philip N. Howard (eds.), Working Paper 2017.8., Oxford, UK: Project on Computational Propaganda.

78. David Alire Garcia and Noe Torres, "Russia meddling in Mexican election: White House aide McMasters," Reuters, 7 January 2018.

79. Ben Nimmo *et al.*, "#ElectionWatch: Trending Beyond Borders in Mexico," *op. cit.*

Part Three

THE RESPONSES

In recent years, several actors—States, international organizations, civil society and private actors—have put mechanisms in place to combat information manipulation. This section will limit itself to outlining the most common responses to information manipulation, by offering a synthesis of these endeavors, by both state and non-state actors, which are the "first signs of an autoimmune response."[1] The section begins with an examination of the so-called "Macron Leaks," a failed attempted interference in the 2017 French presidential election which, because of its failure, illustrates the virtues of a combined and coordinated response by the aforementioned actors. It then examines the responses employed by other States on the institutional, legislative, and educational levels. Finally, this section provides an overview of the responses prescribed by a variety of international organizations, civil society and private actors.

A common question is whether it is better to respond to an information manipulation attack or to simply ignore it and, if the choice is to respond, whether it is sufficient to correct it or if the opportunity should be used to promote an alternative message. This answer is a combination of ignorance and both defensive and offensive measures.

1. Jakub Janda, "Why the West is Failing to Counter Kremlin Disinformation Campaigns," *The Observer*, 30 December 2016.

Ignoring the attack is tempting, if it is believed that the information will die on its own. The rhythm of the media is such that few events outlive the daily flow of information, and public opinion tends to forget quickly. Refuting is repeating and may help to keep the story alive. "Strategic silence" may therefore, in some cases, be the preferred option. Yet, this also comes with the risk of allowing such false and potentially dangerous ideas to sink into the minds of the population. If they are not contradicted from the outset, these ideas may continue to grow with time. Ignorance as a strategy should therefore only be reserved for minor and inoffensive forms of information manipulation.

Reacting defensively by correcting false information has the advantage of not allowing the ideas to spread and be left unchallenged, by quickly cutting them short. But the task requires time and human resources—to monitor social networks, detect manipulation attempts, formulate a response, disseminate it, and analyze its reception. There is also a risk that it will have the opposite effect, as the response could spark a debate, and even involuntarily give new wind to the trolls. The most efficient solution would therefore combine a defensive strategy with an offensive one, by providing new information that will help to take back control over the discussion. Unfortunately, this requires even more time and resources.

I. Case study: the 15 French Lessons of the "Macron Leaks"

In the long list of foreign interferences in electoral processes in recent years, the 2017 French presidential election is the exception that confirms the rule. These targeted actions against presidential candidate Emmanuel Macron neither succeeded in interfering with the election nor in antagonizing French society and, as such, is of particular interest to our study. By "Macron Leaks," we refer not only to the release on Friday, May 5, 2017—just two days before the second and final round of the presidential elections—of 9 gigabytes of data that were hacked from Emmanuel Macron's campaign team. We refer more generally to the orchestrated campaign against him that started several months earlier, through numerous information manipulation operations. This section will provide an analysis of the "Macron Leaks," the actors who (presumably) orchestrated the attacks, how it was successfully countered and, finally, the lessons that can be learned.[2]

2. This section is the summary of an upcoming detailed report: Jean-Baptiste Jeangène Vilmer, *The Macron Leaks: A Post-Mortem Analysis*, CSIS Europe Program, Washington D.C., Fall 2018.

A. What happened?

The leak itself was only the culmination of a long-running campaign orchestrated against the presidential candidate. It began with the diffusion of rumors and insinuations that grew in January and February 2017. For example, on 4 February 2017, an article by Sputnik presented Macron as a "US agent" supported by a "very wealthy gay lobby."[3] However, the Kremlin was not the only player. Some attacks came from Marine Le Pen's "foreign legion" of American alt-right trolls.[4]

Last but not least came the "#MacronGate" rumor. Two hours before the final televised debate between Emmanuel Macron and Marine Le Pen, on Wednesday, 3 May at 7 pm,[5] a user with a Latvian IP address posted two fake documents on the US-based forum 4Chan, suggesting that Macron had a secret offshore account. It was quickly retweeted by some 7,000 Twitter accounts, mostly pro-Trump, often with the #MacronGate and #MacronCacheCash hashtags. During the debate, Le Pen herself mentioned the existence of a hidden account. The rumor was quickly debunked as several investigative journal pieces proved that these documents were fake.[6]

Curiously, the same people who posted the fake documents on 4Chan on Wednesday announced on Friday morning that more was coming. By this declaration, those responsible for the "MacronGate" inadvertently provided evidence that they were the same people responsible for the "Macron Leaks" that came out later that day.

The operation started with a series of phishing attacks several months earlier. Macron's team confirmed that their party had been targeted since January 2017.[7] Several attacks were carried out with email spoofing. In total, the professional and personal email accounts of at least five of Macron's close collaborators were hacked, including his speechwriter, his campaign treasurer and two MPs.[8]

---

3. "Ex-French Economy Minister Macron Could Be 'US Agent' Lobbying Banks' Interests," *Sputnik*, 4 February 2017.

4. Josh Harkinson, "Inside Marine Le Pen's 'Foreign Legion' of American Alt-Right Trolls," *Mother Jones*, 3 May 2017.

5. All timestamps in this article are presented in GMT+2 (Paris time).

6. "How we debunked rumours that Macron has an offshore account," *France 24–The Observers*, 5 May 2017.

7. Michel Rose, Éric Auchard, "Macron campaign confirms phishing attempts, says no data stolen," *Reuters*, 26 April 2017.

8. Frédéric Pierron, "MacronLeaks : 5 victimes et des failles de sécurité," fredericpierron.com blog, 11 May 2017.

The hackers waited until the very last moment to leak the documents: 5 May 2017, just a few hours before official campaigning stopped for the "purdah period," a 44-hour political media blackout ahead of the polls' closure. The files were initially posted on Archive.org, then on PasteBin and 4Chan. Pro-Trump accounts (William Craddick and Jack Posobiec) were the first to share the link on Twitter, using the hashtag #MacronLeaks, which was soon after picked up by WikiLeaks. Overall, the hashtag "#MacronLeaks reached 47,000 tweets in just three and a half hours after the initial tweet."[9]

Other fake documents were spread on Twitter, some of which were not part of the original leak, but came instead from or were addressed to people who did not even exist. One email, evidently fake, allegedly written by the Macron's director of general affairs, contained statements of the following nature: "sometimes I masturbate while listening to .wav of emptying sink noises," "my love for Yaoi [japanese gay manga] and progressive metal prevented me from seeing the truth" and "fuck the people."[10] These statements were retweeted more than 1,000 times.

In summary, the Macron Leaks reveal the following information manipulation pattern: first, the content is dumped onto a political discussion board like 4Chan. Second, it is brought to mainstream social networks like Twitter. Third, it is spread through political communities, notably the US alt-right and French far-right with catalyst accounts or "gurus" (Craddick, Posobiec) and finally the content is retweeted by both real people ("sect followers")[11] and bots. The use of bots was obvious as some accounts posted almost 150 tweets per hour.[12]

B. Who is responsible?

It is indeed easy to see the connection between the information component—that is, the spread of rumors and fake news during the presidential campaign—and Russian interests, particularly since the Russian media, with Sputnik and RT at the head, played a non-negligible role in the diffusion of this information. A study on social networks

9. Ben Nimmo, Naz Durakgolu, Maks Czuperski and Nicholas Yap, "Hashtag Campaign: #MacronLeaks. Alt-right attacks Macron in last ditch effort to sway French election," DFRLab Medium.com, 6 May 2017.

10. https://twitter.com/joshdcaplan/status/860868394534522880

11. The "gurus"/"sect followers" mechanism has been described by Lion Gu, Vladimir Kropotov and Fyodor Yarochkin, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*, A Trendlabs Research Paper, Trend Micro, 2017, p. 42.

12. Ben Nimmo *et al.,* "Hashtag Campaign," *op. cit.*

also revealed there was a strong congruence between communities who diffused the rumors, most of which were directed at Macron, and the Russian-speaking communities (75% for accounts that passed on at least three rumors, and 95% for ones that passed on five). Belgian researcher Nicolas Vanderbiest, who led the study, concluded that "given the level of agreement and the presence of key actors in the Russian ecosystem, (…) we can detect Russian influence."[13]

However, it is structurally more difficult, sometimes even impossible, to attribute a cyberattack, and therefore to know with certainty who pirated Macron's campaign emails and who organized the massive leak of files. At the time of writing, more than a year after the incident, France still has not publicly attributed the attacks to any particular perpetrator. Others, however, have done so.

Most experts point to the Kremlin. They give several reasons to justify this attribution:

• The email address (frankmacher1@gmx.de) initially used to upload the files on Archive.org is registered with the same German webmail provider that was implicated in the 2016 cyberattack against Angela Merkel's party.[14] This latest attack had been attributed to APT28, a cyberespionage group linked to the Russian military intelligence agency, GRU.[15] Of course, this alone does not prove anything as GMX Mail has over 11 million active users.

• The successive phishing attempts against Macron's campaign staff were equally attributed to APT28 by the Japanese cybersecurity company, TrendMicro.[16]

• All of the Excel bookkeeping spreadsheets that were leaked contained metadata in Cyrillic. They indicate that the last person to have edited the files is an employee of the Russian information technology company Evrika (Eureka). Among the company's clients are several government agencies, including the FSB.[17] However, it is difficult to infer anything

13. Nicolas Vanderbiest, "Les institutions démocratiques : l'influence des réseaux sociaux durant une élection présidentielle," in Stéphane Taillat, Amaël Cattaruzza and Didier Danet (eds.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 187.

14. Sean Gallagher, "Evidence suggests Russia behind hack of French president-elect," *Ars Technica,* 8 May 2017.

15. Feike Hacquebord, "Pawn Storm Targets German Christian Democratic Union," *TrendLabs Security Intelligence Blog*, 11 May 2016.

16. Feike Hacquebord, *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat*, A Trend Micro Research Paper, 25 April 2017, p. 13 (https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm).

17. Sean Gallagher, "Evidence suggests Russia behind hack of French president-elect," *op. cit.*

from this connection as it could very well be intended to misdirect; a false flag operation pointing to Moscow.

• The metadata files from the #MacronGate rumor on offshore accounts shows that these documents were produced by two Canon machines costing US$30,000 and over US$100,000 each[18], indicating that those who were responsible for the attacks had access to substantial financial resources, closer to that of a State than of "somebody sitting on their bed who weighs 400 pounds," so to speak.[19]

• Kremlin propagandist and former member of parliament Konstantin Rykov, sometimes nicknamed the "chief troll" and who boasted of his role in Trump's election, also acknowledged having failed in the case of France. "We succeeded, Trump is president. Unfortunately Marine did not become president. One thing worked, but not the other,"[20] he mused.

• Facebook identified two dozen accounts spying the entourage of then-candidate Macron, and spoke of "Russian agents who were passing themselves off as close friends of Macron."[21]

None of these facts prove anything by themselves, however the available evidence, taken together, points unmistakably in the direction of Moscow. There is, however, one notable exception: the user responsible for "#MacronGate," which occurred two days before the leak, may in fact be American neo-Nazi hacker, Andrew Auernheimer.[22] Given the well-known alliance that exists between Russia and the American far-right movements,[23] these two hypotheses are not incompatible.

France never officially attributed the cyberattack. On June 1, 2017, Guillaume Poupard, the head of the French National Cybersecurity Agency (ANSSI), declared that "the attack was so generic and simple that

18. Bivol, "'Canon' for Macron: The fake news on Emmanuel Macron offshore account looks too professional," 5 May 2017.

19. "It could be Russia, but it could also be China. It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds" Donald Trump declared during his first televised debate with Hillary Clinton, 27 September 2016. See Jeremy Ashkenas, "Was It a 400-Pound, 14-Year-Old Hacker, or Russia? Here's Some of the Evidence," *The New York Times*, 6 January 2017.

20. Konstantin Rykov in a mediametrics.ru interview, in the Paul Moreira's documentary, "*Guerre de l'info*," Arte thema, 2018.

21. Joseph Menn, "Exclusive: Russia used Facebook to try to spy on Macron campaign–sources," Reuters, 27 July 2017.

22. David Gauthier-Villard, "U.S. Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm," *The Wall Street Journal*, 16 May 2017.

23. Casey Michel, "America's neo-Nazis don't look to Germany for inspiration. They look to Russia," *The Washington Post*, 22 August 2017.

it could have been practically anyone."[24] What can be safely assumed is that, whoever the perpetrator was, they were at least linked to Russian interests and received help from the American alt-right and French far-right, two communities that share a very close vision to that which is articulated by the Kremlin.

C. Why did the operation fail and what lessons can be learned?

In fine, the leak did not significantly influence French voters, despite the efforts of the aforementioned actors. Why? French success resulted from a combination of structural factors, luck, as well as the effective anticipation and reaction of the Macron campaign staff, the government and civil society, especially the mainstream media.

1. Structural reasons

Compared with other countries, especially the US and the UK, France presents a less vulnerable political and media environment for a number of reasons. First, the election of the president is direct, making any attempt at interference in the election more obvious. Furthermore, the French election has two rounds, which creates an additional difficulty for meddlers, as they do not know in advance who will make it to the second round. This also permits the population to shift their support to another candidate and correct an unexpected result after the first round.

In addition, the French media environment is robust: there is a strong tradition of serious journalism, the population refers mostly to mainstream media sources, and tabloid-style outlets and "alternative" websites are much less popular than they are in the US and in the UK.

Finally, cartesianism plays a role: rationality, critical thinking, and a healthy skepticism are part of the French DNA and are encouraged as early as primary school and throughout one's professional life.

2. Good luck

Chance certainly also has a part to play: hackers were sloppy and made a number of mistakes. Firstly, the hackers were overconfident. They overestimated their ability to shock and mobilize online communities,

24. Andrew Rettman, "Macron Leaks could be 'isolated individual', France says," *EU Observer*, 2 June 2017.

underestimated the resistance and the intelligence of the mainstream media and, above all, they did not expect that the Macron campaign staff would react—let alone react so well. They also overestimated the interest of the population in a leak that ultimately revealed nothing. They assumed that the creation of confusion would be enough and that the content of the leaks would somehow be secondary. But, as it became obvious that the thousands of emails and other data were, at best, boring and, at worst, totally ludicrous, the public lost interest.

Then, the idea to launch the offensive just hours before the purdah period was a double-edged sword. The goal was certainly to render Macron unable to defend himself and to mute the mainstream media. Perhaps the hackers expected to attract attention with the announcement of the leaks rather than the content of those leaks because the content did not contain anything interesting. Regardless, the timing of the release did not leave provocateurs long enough to spread the information, and it made the leaks appear suspicious.

Finally, the attack suffered from cultural clumsiness. Most of the catalyst accounts (and bots) were in English because the leaks were first spread by the American alt-right community. This was not an effective means of penetrating the French population, which is known for not having the best foreign language skills.

3. Good anticipation

Lesson 1: Learn from others. Paris has benefited from the errors that were observed during the American presidential election: disdain and disinterest for information manipulation campaigns, reticence when it came to responding to and framing the DNC hacking, a delayed response, etc. In January 2017, the French Minister of Defense acknowledged that "our services have the necessary exchanges on this subject, if only to draw lessons for the future."[25] The American intelligence services also warned their French homologues of the Russian interference attempts during the French presidential campaign.[26]

Lesson 2: Use the right administrative actors. Two bodies played a particularly crucial role. First, there is the National Commission for the Control of the Electoral Campaign for the Presidential Election

25. Jean-Yves Le Drian (Minister of Defense), interviewed in *Le Journal du Dimanche*, 8 January 2017.

26. Martin Matishak, "NSA chief: U.S. warned France about Russian hacks before Macron leak," *Politico*, 9 May 2017.

(CNCCEP), a special body set up in the months preceding every French presidential election to serve as a campaign watchdog. Second, there is the National Cybersecurity Agency (ANSSI), whose mission is two-fold: to ensure the integrity of electoral results and to maintain public confidence in the electoral process.

Lesson 3: Raise awareness. ANSSI and CNCCEP alerted the media, political parties and the public to the risk of cyberattacks and disinformation during the presidential campaign. ANSSI was proactive, offering to meet with and educate all campaign staff at very early stages of the election. In October 2016, ANSSI organized an open workshop on cybersecurity. All but one party participated: the Front national rejected the offer.

Lesson 4: Show resolve and determination. From the start of the electoral campaign, the French government signaled both publicly and through more discrete, diplomatic channels, its determination to prevent, detect and, if necessary, respond to foreign interference. The Defense Minister declared that "by targeting the electoral process of a country, one undermines its democratic foundations, its sovereignty" and that "France reserves the right to retaliate by any means it deems appropriate."[27] The Minister of Foreign Affairs similarly declared that "France will not tolerate any interference in its electoral process."[28] A similar message was conveyed privately by the Minister to his Russian counterpart and by President Hollande to President Putin. This was evidently not enough to stop the attack, which is why it would be an exaggeration to call it deterrence, however it is possible that the remarks helped to contain the operations, which could have otherwise posed a bigger threat.

Lesson 5: Take technical precautions. ANSSI heightened security at every step of the electoral process in order to ensure the integrity of the vote. Following the recommendations set forth by ANSSI, the Foreign Minister announced, at the beginning of March 2017, the end of electronic voting for citizens abroad because of the extremely high risk of cyberattacks.

Lesson 6: Put pressure on digital platforms. Ten days before the vote, Facebook announced that it had deleted 30,000 suspicious accounts in France. It would later be revealed that this number was actually 70,000.[29] This was an unprecedented step that was the result of growing pressure,

27. Jean-Yves Le Drian (Minister of Defense), interviewed in *Le Journal du Dimanche*, 8 January 2017.

28. Martin Untersinger, "Cyberattaques : la France menace de 'mesures de rétorsion' tout État qui interférerait dans l'élection", *Le Monde*, 15 February 2017.

29. Joseph Menn, "Exclusive: Russia used Facebook to try to spy on Macron campaign–sources," *op. cit.*

by both States and the public, on digital platforms—the principal medium for the spread of disinformation.

4. Good reaction

Lesson 7: Make public all hacking attempts. Throughout the campaign, the En Marche! team communicated openly and extensively about its susceptibility to hacking and, soon after, about the hacking itself. At the peak of the crisis, when the documents were leaked, En Marche! reacted in a matter of hours. At 11:56 pm on Friday, 5 May, only hours after the documents were dumped online and 4 minutes before the purdah went into effect, the Macron campaign issued a press release.[30]

Lesson 8: Beat hackers at their own game. As the hacks could not be avoided, the En Marche! team placed several traps: fake email addresses, fake passwords, fake documents. This diversionary tactic, which involves the creation of fake documents to confuse attackers with irrelevant and even deliberately ludicrous information, is called cyber or digital blurring. Thanks to this tactic, the Macron campaign staff did not have to justify potentially compromising information contained in the Macron Leaks; rather, the hackers had to justify why they stole and leaked information which seemed, at best, useless and, at worst, false or misleading.

Lesson 9: Strike back on social media. The forceful presence of the Macron campaign staff on social media enabled them to respond quickly to the spread of information. They systematically responded to posts or comments that mentioned the "Macron Leaks."

Lesson 10: Use humor. The campaign's injection of humor and irony into their responses to the hackings increased the visibility, popularity, and rate of diffusion of those responses across different platforms.

Lesson 11: Alert law enforcement. On the Friday night, when the Leak was underway and within a few hours of the initial dump, the public prosecutor's office in Paris opened an investigation, entrusted to the Brigade for the Investigation of Information Technology Fraud (BEFTI).

Lesson 12: Undermine propaganda outlets. On 27 April, Macron's campaign confirmed that it had denied RT and Sputnik accreditations to cover the rest of the campaign. Even after the election, both outlets have been denied access to the Élysée Presidential Palace and Foreign Ministry press

30. "En Marche a été victime d'une action de piratage massive et coordonnée," press release, En Marche !, 5 May 2017.

conferences. This decision is justified on at least two grounds. First, these outlets are not press but propaganda organs. This has been Macron's position, expressed clearly during the campaign and most famously before President Putin at the Versailles press conference only weeks after the election.[31] It has also been the position of the European Parliament as of November 2016.[32] Second, attendance at these press conferences is by invitation only so there is no need for French institutions to justify their exclusion of these news outlets.

Lesson 13: Trivialize the leaked content. The En Marche! press release said that the leaked documents "reveal the normal operation of a presidential campaign." Nothing illegal, let alone interesting, was found among the documents.

Lesson 14: Compartmentalize the communication. If there is nothing scandalous to be found in the leaked emails, it is because Macron's campaign staff was aware that everything they wrote in their emails could one day be made public. Therefore, they had three levels of communication: "the trivial and logistical by email, the confidential on the [encrypted] apps, and the sensitive in face-to-face."[33]

Lesson 15: Call on the media to behave responsibly. On Friday night, Macron's team referred the case to the CNCCEP which issued a press release the following day, requesting "the media not to report on the content of this data, especially on their websites, [and] reminding the media that the dissemination of false information is a breach of law, above all criminal law."[34] The majority of traditional media sources responded to this call by choosing not to report on the content of the leaks. Some have even gone one step further by denouncing an electoral interference attempt and calling upon their readers to not let themselves be manipulated. The reaction of *Le Monde* is exemplary in this respect.[35]

31. Emmanuel Macron, joint press conference with Vladimir Poutine, Versailles, 29 May 2017. See Marc de Boni, "Devant Poutine, Macron dénonce la 'propagande' des médias pro-russes," *Le Figaro*, 29 May 2017.

32. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)).

33. Nathalie Raulin and Guillaume Gendron, "Piratage : l'équipe Macron sur le pont," *Libération*, 10 August 2017.

34. Press release, CNCCEP, 6 May 2017.

35. "Le Monde et les documents des 'MacronLeaks'," *Le Monde*, 6 May 2017.

Conclusion

According to the five stages of election meddling described by Mika Aaltola in the context of the 2016 American presidential election,[36] the "Macron Leaks" only reached the third stage. There was a disinformation campaign, data hacking, large scale leaking, but no laundering or mainstreaming. What was successfully prevented was "the 'laundering' of this counterfeit online currency of invented news, disseminated and then relayed by authorities, [that] legitimizes them in the public's eyes."[37] "Information laundering" is defined as the process by which the initial traces of meddling are washed from the information, stories and narratives. Finally, structural factors as well as an effective, responsive strategy allowed the French to successfully mitigate the damage of the Macron Leaks.

II. Other state-led responses

European States have in recent times developed a more acute awareness of the challenge posed by information manipulation as well as a greater determination to tackle it. More countries are coming to grips with the problem and have come to realize that the most dangerous activities are not the most visible ones—such as the "Lisa Case" in Germany or instances of electoral interference in the United States and France—but the day-to-day undermining of trust in institutions and liberal, democratic values. Indeed the peril of foreign interference lies less in targeted operations than in the long-term alteration of the political environment. Accordingly, States have taken a number of corrective actions, or are in the process of doing so.

A. Internal organization: networks and a few specialized centers

A consensus prevails: the nature of the problem requires a global approach, a de-compartmentalized, holistic response from services that are generally fragmented. Everywhere, States organize networks: this way of working is familiar to Nordic countries (Finland speaks of "intersectoral collaborative bodies") and less familiar to other countries. However, all

36. Mika Aaltola, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling*, *op. cit.*

37. J.-Y. Le Drian, Speech of 4 April 2018.

States do recognize the need for a coordinated approach. A number of them have already established formal networks:

• Sweden has a task force which deals with influence campaigns under the authority of the Office of the Prime Minister, while the Swedish Civil Contingencies (MSB) agency, which concentrates resources for the fight against information manipulation, also acts as a hub.

• Finland deals with the issue through a high-level generalist network (the Security Committee, which is made up of 19 members and 3 experts representing all of the concerned Ministries and services as well as the business community, and which meets nine times a year). Finland also has a dedicated network, the "Information Influencing Network." Created in December 2014, it is an informal network in that it was not officially appointed, however it was approved by the Security Committee. Its mission is to identify, analyze and respond to hostile foreign interference attempts. This network comprises about thirty government experts holding key positions within their respective Ministries as well as ICRC and other NGO representatives, who all meet once a month.

• Denmark has set up a task force, which is chaired by the Ministry of Justice and also includes the Defense and Foreign Affairs Ministries and the intelligence services. The Danish Ministry of Foreign Affairs also has its own internal task force that involves three departments—namely Public Diplomacy, Security Policy and European Neighborhood & Russia. This cross-disciplinary team of about a dozen members is placed under the direct authority of the political director, which speeds up the decision-making process.

• The United Kingdom has an inter-ministerial strategic communication unit hosted by the Foreign and Commonwealth Office (FCO), with substantial financial and inter-ministerial resources (about twenty staff) at its disposal. The purpose of this unit is to ward off information manipulation narratives through the identification of their source and the examination of their effects, as well as build up the resilience capacity of those third States that are particularly exposed to information manipulation. The unit also develops partnerships with the media, technological actors and civil society so as to establish a network of fact-checkers.

• The Netherlands has a network managed by the National Coordinator for Counter-terrorism and Security (NCTV) under the supervision of the Justice Ministry, and which involves Foreign Affairs Ministry, the

Defense Ministry and the intelligence services, alongside the NCTV and Social Affairs.

• Latvia has a working group on information threats chaired by the Media Policy Division within the Ministry of Culture and operating in partnership with other ministries, the intelligence services and representatives of Parliament.

• Singapore has a network coordinated by the Ministry of Communications and Information.

Alongside this overall trend of network creation, a number of States have also established dedicated centers:

• The United States (see below) created a Global Engagement Center (GEC) in 2016, based within the Department of State. Initially established to counter ISIS propaganda, the Center's mission was broadened the following year to include threats from foreign States, primarily those from Russia. Sometimes described as coordinating the work of a variety of agencies (in particular the Department of Defense, the intelligence community, USAID, the BBG and the Department of State), the GEC mostly comprises Pentagon staff, who are more numerous and better trained on these issues than Department of State personnel. There are also numerous task forces dedicated to the fight against disinformation and/or foreign influence in other departments, such as the Department of Justice and the Department of Homeland Security. In contrast to other countries, the United States does not lack resources in this domain so much as it lacks coordination: there are so many different institutions it is difficult to know who does what, and above all, who gives the directions (see below). It is for this reason that some Democratic Senators deem it necessary to go a step further and they have urged the President, in a recently published report, to set up a high-level inter-agency "fusion cell" modeled on the National Counter-Terrorism Center (NCTC) to coordinate all elements of US policy in response to Russian influence operations.[38]

• The Czech Republic created, in January 2017, a Center Against Terrorism and Hybrid Threats (CTHT) within the Ministry of the Interior. Comprising about 15 staff members, the Center combines a dual mission of policy making and strategic communications (a system of information monitoring and targeted responses). In order to offset

38. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 4.

information manipulation, it does not produce counter-narratives but merely issues refutations of false information. The Center also has a public interface (e.g. it organizes public events and is active on social networks).

• Sweden should create a new authority of "psychological defense," announced the Prime minister in January 2018. This new authority could absorb the counter-influence section of the MSB, which is one of the most well-organized and innovative structures that we have visited.

It is important to emphasize that these centers are no substitute for networks but are a complementary element: we are not faced with two models—one flexible (the network) and the other more static (the center)—but with widespread consensus as to the importance of networks, topped off, in some States, by the creation of a dedicated center.

The efficacy of these structures depends on the means devoted to them, that is, on human and financial resources, which are themselves dependent on political will. These structures must also overcome a number of difficulties, related first and foremost to issues of institutional affiliation, which can spark territorial struggles between different services, and of communication, both external (to demonstrate that the new entity is no Orwellian "Ministry of Truth"), and internal (to prove its utility).

B. The involvement of Parliaments

The United States and the United Kingdom have undertaken in-depth parliamentary inquiries to establish responsibility for the interference operations of which they were victims. The public nature of those inquiries, which are the focus of close media scrutiny, has the advantage of increasing public awareness, providing them with very precise information (the expertise gathered by each inquiry is considerable) as well as, arguably, having a deterrent effect. Certain committees have produced authoritative reports, which greatly contribute to our knowledge of the problem. An example worth noting from the United States, is the work of Democratic senators (*Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,* published in January 2018 for the Foreign Affairs commission). In the United Kingdom, there is also an upcoming report from the Digital, Culture, Media and Sport Committee (*Disinformation and 'fake news'*, a draft report was published in July 2018, and the final version is expected for this fall).

Yet another interesting case from a different region: Singapore. The Singaporean authorities are very aware of the vulnerability of their population: their diversity (multiethnic and multireligious) always has the potential to generate tensions, and the fact that they are Anglophone makes them easily penetrable. For these reasons, they are highly exposed to Chinese influence. The Singaporean parliament addressed the issue and, to introduce a new law against disinformation, they created in January 2018 a Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures, which has since conducted a great number of hearings, including with international experts. All of the resulting documentation is available on the Committee's website and constitutes a valuable source of information.[39]

C. Awareness and Education

In order to raise public awareness of the dangers posed by information manipulation, States have implemented a number of measures, such as:

- production of doctrine (e.g. the 2016 Central Government Communications Guidelines in Finland);
- support for research through partnerships with universities (the Swedish MSB published a Handbook on influence operations in collaboration with Lund University) and the funding of research projects (the MSB funds between 2 to 5 research projects, representing an overall budget of 2 million euros);
- massive awareness-raising campaigns, including through mail distribution (the Swedish MSB has printed out 4.7 million copies of a booklet explaining what to do in the event of a crisis, including terrorist attacks and information manipulation campaigns. This booklet is sent to every household in the country—these dedicated pages used to appear in the phone directory, however the shift away from print has reduced the dissemination of information, particularly in rural areas);
- training of civil servants, journalists and companies (the MSB has already trained 11,000 civil servants);
- media literacy (from 2018 onwards, all primary schools in Sweden will teach the basics of programming and develop pupils' capacity to distinguish between reliable and unreliable information; Latvia

39. Parliament of Singapore, Select Committee on Deliberate Online Falsehoods—Causes, Consequences and Countermeasures.

will introduce defense-related subjects in schools from 2020, including media literacy, cybersecurity and defense education; Singapore has adopted the Swedish concept of "total defense" and teaches it in schools; the Italian Ministry of Education has initiated an innovative program which provides fact-checking training and has already yielded encouraging results[40]);

• international presence by sending personnel to Brussels (EU East StratCom Task Force), Riga (NATO StratCom CoE), Helsinki (Hybrid CoE) and important annual summits (StratCom Summit in Prague, Riga StratCom Dialogue, StratCom of the Atlantic Council in Washington DC).

• creation of simple identification and diagnostic tools that are available to the public. Accordingly, the report by Swedish MSB and the University of Lund suggests the regular performance of a "DIDI" diagnostic test on informational activities. To qualify as disinformation, an informational activity must 1) contain deceptive elements; 2) have the intention to harm; 3) be disruptive; and 4) constitute an interference. Such a diagnostic offer the possibility for both its users as well as public opinion to differentiate information manipulation from more sincere operations of influence.[41]

D. Media Outreach

The four main state measures relating to the media consist of registration, prohibition, regulation and denunciation.

1. Registration

The United States uses the Foreign Agent Registration Act (FARA), a law originally adopted in the 1930s to counter Nazi propaganda, which requires that any entity engaging in political information and receiving foreign funds openly identify as such and disclose the nature of its foreign financial connection. Pursuant to this legislation, the Department of

40. Christopher Livesay, "Italy Takes Aim At Fake News With New Curriculum For High School Students," NPR, 31 October 2017; and interviews conducted in Rome on 30th November 2017.

41. James Pamment *et al.*, *Countering Information Influence Activities: The State of the Art,* Department of Strategic Communication, Lund University, research report, version 1.4, 1 July 2018, p. 14.

Justice requested that RT and Sputnik follow this registration procedure, which they did despite Moscow's objections.[42]

The FARA legislation is useful in that no ruling needs to be made on the content of the messages put forward by these "foreign agents" (it is not an instrument of censorship); it seeks, rather, to increase transparency regarding these actors' sponsors, leaving it to citizens to form their own conclusions as to the credibility of the published messages. However this system is less effective when faced with hybrid actors, who are neither companies nor registered lobbyists, and whose financial links with foreign powers are not easily demonstrable.

In addition, a registration race is underway with Russia. In November 2017, Moscow amended its 1992 press law so as to make it possible for a media actor to be construed as a foreign agent—the Russian response to the American decision to apply the FARA law to RT. Henceforth, "any legal person registered in a foreign country or any foreign entity without legal personality which distributes written, audio or audiovisual material to an unlimited audience can be defined as a foreign media, performing the role of a foreign agent." This actually connects the legislation on the media to the law adopted in 2012 on NGOs, which labelled any NGO receiving funding from abroad as a "foreign agent." Russian authorities invoked the principle of symmetry ("we do the same as the Americans"). The difference, however, is that the American legislation aims at transparency and does not undermine the freedom of the media to conduct their work. In Russia, by contrast, it is feared that the Russian law, under the guise of transparency, will exercise enough pressure on some media as to force them to shut down.

2. Prohibition

This is particularly true of Ukraine: the prohibition of Russian media in Ukraine started in 2014 with the main broadcasters. Eventually, 73 channels were banned in 2016. Ukrainian-language content quotas were also imposed for radio and television. Moreover, several Russian websites, such as VKontakte, Odnoklassniki, Yandex and Mail.ru were banned in May 2017, which caused their audiences to decrease dramatically. The Ukrainian government also created a Ministry of Information Policy, for which Kiev was widely criticized, not just by Moscow but also by the

42. Jack Stubbs and Ginger Gibson, "Russia's RT America registers as 'foreign agent' in U.S," Reuters, 13 November 2017.

West. Ukraine defended its position by claiming to be in a state of war. Numerous other countries, including Indonesia, equally chose to block websites or social networks in order to fight information manipulation.

3. Regulation

It is the middle-of-the-road option and the preference of most liberal democracies. The British Ofcom is regularly cited as an example in this domain, as it often does not hesitate to call out RT on its biases. In France, the media regulatory authority (*Conseil supérieur de l'audiovisuel*, or CSA) issued a formal notice to the RT France channel on 27 June 2018 for "lacking honesty with respect to the rigorousness of the information and the diversity of opinions presented."[43] This is namely because, in a report broadcast on 13 April, the news channel falsified the translation of a statement given by a witness from Ghouta, by making him say that the chemical attack was simulated, while in reality he was talking about famine plaguing the region. The channel later claimed it had been a "purely technical error."

More generally, regulation may entail passing so-called "fake news laws." Numerous States have or are currently trying to introduce such legislation. The Poynter Institute keeps an updated list.[44] The most well-known is undoubtedly the German law known as "NetzDG" (for *Netzwerkdurchsetzungsgesetz*), in effect since January 2018, which obliges digital platforms of more than two million members (Facebook, YouTube, Twitter) to delete "blatantly illegal" content within 24 hours or face fines up to 50 million euros.

Defining the object also poses certain challenges (especially if it is placed under a category as vague as "fake news," as is often the case), as does finding an equilibrium with the protection of civil liberties and the freedom of the press. In democratic countries, civil society, namely NGOs and associations of journalists, along with a certain number of parliamentarians, are often skeptical of the need and the effectiveness of introducing new legislation. Many point out the risks of it having the opposite effect.

43. CSA, "Manquements à l'honnêteté, à la rigueur de l'information et à la diversité des points de vue : la chaîne RT France mise en demeure," plenary Assembly held on 27 June 2018, 28 June 2018.

44. Daniel Funke, "A Guide to anti-misinformation actions around the world," The Poynter Institute, 2 July 2018.

4. Denunciation

Some States allow their citizens to denounce false information on a government website. In Italy, for example, there is a portal that allows anyone with an e-mail and a link to the incriminated information to get the attention of the Polizia Postale, the police unit in charge of cybercrime. The Thai government, through the Ministry of Public Health, launched a mobile application, "Media Watch," developed by the Fund for Development of Safe and Creative Media for Mental Health, that allows anyone to report fake news. The Chinese army also created a website allowing the population to report fake news (with all the ambiguities that this measure would entail in a non-democratic context).

E. The case of the United States

Throughout the Cold War, the American institutional system developed a very sophisticated architecture with which to respond to Soviet information manipulation.[45] Countering disinformation and the Kremlin's "active measures" became a priority for American national security at the beginning of the 1980s.[46] This architecture was dismantled after the fall of the Berlin Wall before being militarized after 9/11, in the context of the long War on Terror. Since the attacks of September 2001, and in the absence of any public diplomacy arsenal comparable to that of the Cold War years with which to approach the ideological war waged against the United States by Jihadist groups like Al Qaeda and ISIS, American counter-propaganda capabilities have largely centered around IOs (Information Operations) and military counter-propaganda. These actions are deemed all the more necessary in light of shrinking resources and the "bunkerization" or disappearance, in some operational theatres, of public affairs officers (PAOs) who are the main agents in the field of public diplomacy. Yet the sum of those actions, conceived and implemented at

45. For this entire section, see Maud Quessard, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information ?*, IRSEM Research Paper 54, 30 April 2018.

46. On 15 January 1983, President Reagan signed Directive 77 (National Security Decision Directive 77), which reinforced the role attributed to public diplomacy by defining it as "those actions of the U.S. government designed to generate support [abroad] for our national security objectives." Directive 77 gave public diplomacy a key place in the foreign policy decision making process, and it affirmed a multidirectional strategy aimed at weakening Soviet influence by supporting the actions of dissidents across Eastern Europe. The sole goal of this significant reorganization of foreign affairs was to successfully complete Project Truth, designed in 1981 by President Reagan and his advisors, to counter the effects of Soviet propaganda.

both national and regional commandment levels (Centcom, Africom, Pacom, etc.), can appear redundant or even counter-productive, which generates inter-agency controversies as to the distribution of responsibility, efficiency and the cost of both military and civilian "public diplomacy" activities.[47]

Following Russian interference in the American electoral process of 2016 (characterized by the targeted use of internet platforms and social networks) and the establishment of the Russian state media Sputnik and RT in the United States, the American media have voiced deep concerns regarding what the political world perceives to be new strategies of Russian influence. Such concerns reflect a deeper anxiety, widely shared across political, diplomatic and military circles in the U.S., of a deficiency in preparedness and coordination to respond adequately and proportionally to this new threat.

The atmosphere in Washington is redolent of McCarthyism and the official responses of the new "warriors of disinformation" seem to draw on the Cold War experience. Already in January 2017, the former National Intelligence Director James Clapper, with the support of, among others, Second Commander of U.S. Cyber Command Admiral Mike Rogers, advocated for a restoration of the Cold War "information machine"—the USIA (United States Information Agency)—in order to tackle the range of Russia's influence strategies (both through the media and internet). Clapper's call for a USIA "on steroids" only reinforced the confusion between influence diplomacy and counter-propaganda.[48] Indeed, the contemporary public debate in the U.S.—in the media, in Congress and in military circles—brims with nostalgia for the "Cold War information machine," which essentially relied on the USIA. The Cold War conflict is construed as the archetype of "Total War," which mobilizes all elements of national power, also referred to as DIME (Diplomatic, Information, Military, Economic).

The failure of the various congressional endeavors initiated as of 2017[49] to articulate a coherent doctrine for American counter-propaganda results from the sheer diversity of actors engaged in the counter-offensive,

47. Wallin Matthew, "Military Public Diplomacy. How the Military Influence Foreign Audiences," White Paper, *American Security Project*, February 2015.

48. Carlo Muñoz, "Clapper calls for U.S. Information Agency 'on steroids' to counter Russian propaganda," *The Washington Times*, 5 January 2017.

49. Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives, "Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment," *115th Congress, 1st session, Washington, USGPO*, 15 March 2017.

who act on behalf of independent agencies, institutions, and departments without efficient coordination. This feature is a recurring weakness in American bureaucracy.

Coordination is rendered all the more difficult, for both internal organization and external policy, by the competing—and even sometimes conflicting—endeavors of agencies. The Department of Homeland Security (DHS) therefore created an anti-disinformation task force which became operational in January 2018 and thus far comprises a dozen staff (and is expected to expand.) Its mission is to better coordinate the various actions undertaken by different agencies, as well as to build capacity and involve private actors. The following month, in February 2018, the attorney general also created a Cyber Digital Task Force within the Department of Justice, whose mission is to combat hostile foreign influence operations—a role that has long been assigned to the Department, in particular to the FBI which, in November 2017, created a Foreign Influence Task Force (FITF). One of its roles is to coordinate actions with other agencies, including the DHS, the Department of State, the NSA and the CIA, while establishing relationships with the federal and local authorities, the private sector and digital platforms.[50] In July 2018, the NSA and the Cyber Command announced they would begin working together to fight against the threat of Russian interference, in light of the November midterm elections. Acknowledging the lack of coordination, general Paul Nakasone, commander of Cyber Command and director of the NSA, declared he was doing everything he could in the absence of an "overall approach directed by the president" or the White House.[51]

Most recently, studies conducted by several American think tanks (Atlantic Council, Brookings, American Security Project) and by the London School of Economics have endeavored to draw lessons from the Cold War legacy and apply those lessons to contemporary challenges. As a matter of fact, the need to re-establish a para-governmental agency modeled on the USIA or an inter-agency coordination committee (Active Measure Working Group, AMGW) had become obvious long before suspicions arose of Russian interference in the 2016 American elections. In particular, the need for greater efficiency was already sensed in the struggle against jihadist propaganda. However, the suggestions

50. U.S. Department of Justice, *Report of the Attorney General's Cyber-Digital Task Force*, 2018, p. 8.

51. Ellen Nakashima, "NSA and Cyber Command to coordinate actions to counter Russian election interference in 2018 amid absence of White House guidance," *The Washington Post*, 17 July 2018.

currently being floated in Washington, supported by the new "warriors of disinformation," tend to rely too heavily on the Cold War experience of the 1980s in their interpretation of contemporary challenges. They also seem to disregard some of the more worrying aspects that underpinned the Cold War era, notably in times of high tension, when it was deemed acceptable to use the weapons of the enemy and thus to overtly wage a war of information.

In 2016, Congress authorized the replacement of the Center for Strategic Counter-Terrorism Communications (CSCC) with the Global Engagement Center (GEC) within the Department of State. The purpose was mainly to counter ISIS propaganda and to endorse a strategy commensurate with the new information environment. The driving idea was to foster cooperation between a greater number of public and private actors (para-governmental agencies, NGOs, businesses) at both the national and international level. The new Center's most enthusiastic supporters wanted to quickly turn it into the main organ responsible for combatting the Kremlin's subversive activities.[52] However, they quickly came up against the complexity of the American bureaucratic system. The 2017 National Defense Authorization Act (NDAA) was designed to extend the prerogatives and mission of the GEC so as to include activities aimed at offsetting state propaganda, be it from Russia, China, Iran or North Korea.

Yet this inter-agency entity represents but one layer of the inherently multi-dimensional response to those challenges. For some, the various strategies being deployed today still bear the name of "talk-back," in the language of the Cold War, while for others they are referred to as "stratcom." Contemporary debates on American influence and counter-propaganda capacities sometimes present an overly compartmentalized vision of public diplomacy programs, on the one hand, and military information operations (IO), on the other. However, public diplomacy and IOs are only two distinct facets of the overall U.S. strategic communication apparatus.

The Active Measure Working Group is the latest instance of an effective coordination on the part of the United States. Based on this model, civil and military public diplomacy professionals have made the

52. The National Defense Authorization Act was intended to expand the GEC's mission by making it an organization fighting against "state propaganda," whether Russian, Chinese, Iranian or North Korean.

following recommendations during the 2017 post-electoral congressional inquiry:

— the creation or reinforcement of an entity involving all of governmental and para-governmental actors, both public and private (Pentagon, Department of State, CIA, NSA, GAFAM corporations, major actors in the ongoing shift of information warfare);

— the need to modernize public diplomacy. The digital turn announced by the Department of State at the end of Georges W. Bush's second term was not successfully completed and the public-private partnerships initiated in those years and then substantially developed through the many initiatives undertaken under Hillary Clinton (with the GAFAM), while she headed to the State Department, must be carried on.

On this basis, diplomatic and military operational actors recommend turning the GEC into an equivalent of the Office of the Director of National Intelligence, so as to coordinate inter-agency work and synchronize operations. In order to organize countermeasures in information warfare 3.0, they also deem it necessary to foster a global approach bringing together the whole range of institutional actors around a common strategy.[53]

The recommendations drawn up during congressional hearings as well as those found in think tank reports (Atlantic Council, Brookings) emphasize the crucial role assumed by the chairperson of this inter-agency entity in the National Security Council's decision-making process. This chairperson could be granted a role at the highest federal level as Deputy-Secretary General or Special Advisor. Indeed, without such close cooperation between the President and the chief of this entity responsible for the elaboration of public diplomacy strategies, responses to the Kremlin's ongoing "active measures" risk remaining incoherent and ineffective. For the record, the Kennedy and Reagan Administrations had both chosen to work with influential media figures (such as the CBS journalist Edward Murrow or the Hollywood producer Charles Wick). Back then, the directors of both the Information Agency and the CIA were—as the President's close collaborators—also linked into to the activities of the National Security Council (NSC), notably during major security crises, when the management of strategic communications proved particularly crucial (e.g. during the Cuba or the Euromissile crises).

53. Michael Lumpkin, coordinator appointed by Barack Obama in 2016, ex-Deputy Secretary of State for Special Operations.

Finally, the appointment of former CIA Director Mike Pompeo as Secretary of State could provide a good opportunity to reinforce inter-agency cooperation and the sharing of information in the fight against information manipulation. The Trump Administration has shown interest in reinforcing the role of the GEC by ring-fencing its budget (via the transfer of 40 million from the Department of Defence to the GEC). This has allowed the creation of the Information Access Fund (since February), a support fund for citizen, entrepreneurial (GAFA) or para-governmental (NGO) initiatives.

III. International organizations

A. The European Union

At the European level, the rise of information manipulation has triggered a progressive response, which was dispersed at first between various institutions. The issue was initially apprehended through the prism of external relations and the need to protect the EU's image in the Eastern neighborhood. The conclusions of the 19-20 March 2015 European Council stressed "the need to challenge Russia's ongoing disinformation campaigns" and invited the High Representative to prepare an action plan on strategic communication.[54]

The Strategic Communications Division of the European External Action Service (EEAS) is made up of three pillars, represented by three teams that each reflect different geographical priorities: the oldest and best-funded one is the East StratCom Task Force whose creation resulted from a decision of the March 2015 European Council meeting. This task force began its activities in September 2015 and set itself three distinct goals: 1) monitoring activities in cooperation with civil society and other European institutions, such as the intelligence center (INTCEN); 2) counter-disinformation activities with a focus on raising awareness on those who read the news; 3) support to independent media which pursue information objectivity in the Eastern neighborhood.

The proponents of the East StratCom Task Force insist that their goal is "not to do counter-propaganda."[55] The activities of the task force are publicized on its website "EU vs Disinformation" (euvsdisinfo.eu), via a

54. European Council, Cover note from the General Secretariat of the Council Delegations on the subject of European Council meeting (19 and 20 March 2015), EUCO 11/15, 20 March 2015.

55. "L'UE crée une équipe pour contrer la propagande russe," *Le JDD*, 31 August 2015.

weekly *Disinformation Review*, and on social networks, under the title "EU Mythbusters." The institution's motto is "Don't be deceived: question even more," in reference to RT's own motto, "Question more." Its Russian language page appears to have a large audience, attracting a quarter of the traffic on the EEAS website.[56] By 2017, they had already identified over 2,500 instances of disinformation in 18 languages. These instances are "stories that contradict publicly available facts."[57] However the task force has first had to convince the public of the importance of the issue, as one of its representatives explains:

> [W]here we started in September 2015, it was depressing because it looked like 95 percent of Brussels didn't believe in Russian propaganda and [the] other 5 percent said it was not a big threat. Now it is a different situation, and most [of] Brussels [sees it as a threat.] We see [that] the interest in this issue is on the rise and more media are writing about it; more Member States taking action… We are working for these objectives. We try to raise awareness, make it a theme of public debate. We are still not there but moving in this direction.[58]

Despite its good results, this task force is under-resourced in terms of both staff and funding. Comprising only eleven personnel, it exists and survives thanks to the good will of a handful of Member States that fund it and lend it members of their own staff. Until recently, European institutions did not appear to be very involved and the EEAS has sometimes been criticized for not taking the Russian disinformation threat seriously. Above all, these difficulties betray an absence of European unity on the issue.

Indeed, national approaches to disinformation remain quite varied across Europe, due to diverging perceptions of the threat. The Prague-based think tank European Values ranks States in an annual classification that encompasses five groups:[59] at the head are the Baltic States, Sweden and the United Kingdom, who take the most offensive approach. They are followed by Czech Republic, Denmark, Finland, France, the Netherlands, Poland, Romania, and Spain. For reasons that are both diverse and sometimes recent, these countries are most aware of this

56. Philippe Régnier, "Tacler la désinfo russe," *Le Soir*, 24 November 2016, p. 12.

57. "Cybermenaces et désinformation : les pays occidentaux se mobilisent," AFP, 16 February 2017.

58. Cited by Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 76.

59. *2018 Ranking of countermeasures by the EU28 to the Kremlin's subversion operations*, European Values, 13 June 2018.

issue and take the threat seriously. They are followed by a group of States characterized as "hesitant" (Belgium, Bulgaria, Croatia, Ireland, Slovakia), and then those countries considered to be "in denial" (Austria, Hungary, Italy, Luxembourg, Malta, Portugal, Slovenia). Lastly there are Cyprus and Greece, who not only take no action to fight against the threat, but who even systematically block any effort to deal with the issue at the EU level. The European Parliament has expressed its concern at "the limited awareness amongst some of its Member States that they are audiences and arenas of propaganda and disinformation," and it has emphasized the "need to raise awareness and demonstrate assertiveness."[60]

The other two teams of the EEAS's Strategic Communications Division are a "South" task force, created in 2015 with a staff of four people who work to counter jihadist propaganda, and a "Western Balkans" task force, established in July 2017 and comprising three officers who focus on defending the EU's image in the region.

In a June 2017 Resolution, the European Parliament asked the Commission to conduct a detailed analysis of "the current situation and legal framework with regard to fake news, and to verify the possibility of legislative intervention to limit the dissemination and spreading of fake content."[61] At the end of 2017, the Commission seized upon the issue of disinformation within the context of its activities towards a digital European society, under the authority of the Commissioner for Digital Economy and Society, Mariya Gabriel. The Commissioner established a high-level expert group which released its report on 12 March 2018, calling for increased transparency for online content, enhanced media literacy, the development of research and a closer partnership with civil society.[62]

Drawing on this report as well as on a broad public consultation process, the European Commission published, on 26 April 2018, a Communication entitled: "Tackling online disinformation: a European approach."[63] This Communication provides for the convening of a multi-stakeholder forum, bringing together online platforms, the advertising industry as well as media and civil society representatives

60. European Parliament, Resolution of 23rd November 2016, *op. cit.*

61. European Parliament, Resolution of 15 June 2017, on online platforms and the digital single market, P8_TA(2017)0272, para. 36.

62. *A multi-dimensional approach to disinformation, Report of the independent High-Level Group on fake news and online disinformation,* March 2018.

63. Communication of the European Commission to the European Parliament, the Economic and Social Committee and the Committee of Regions, *Tackling online disinformation: a European Approach*, 26 April 2018, COM(2018) 236 final.

with a view to drafting, by July 2018, an "EU-wide Code of Practice on Disinformation" intended to foster fact-checking and self-regulation measures.

This code, published on 17 July 2018, is structured around the following five lines of action: 1) improving surveillance of advertising placements in order to reduce the financial appeal of disinformation; 2) guaranteeing transparency in political or themed advertising in order for users to rapidly identify targeted content; 3) guaranteeing the integrity of services delivered by digital platforms by identifying and eliminating fake accounts by using appropriate mechanisms to flag and report these automated interactions (bots); 4) helping users to discover and access different sources of information with alternative points of view; 5) reinforcing the capacities of research communities by providing them access to digital platform data that is needed to continually analyze disinformation online. The Forum's advisory committee will hand in a first draft at the beginning of September 2018 and will adopt a final version at the end of the same month. The Commission intends to assess the Code's implementation at the end of 2018 and it makes provisions for possible additional measures. The Commission also states its commitment to safeguarding electoral processes, notably in anticipation of the 2019 European parliamentary elections, in cooperation with Member States, with whom primary responsibility for these matters lies. However, up to the present day, no regulatory action has been announced, and the Commission is unlikely to put forward any legislative proposal before the end of the current term of office.

The 2018 EU budget provides increased funding for strategic communications, including 1.1 million euros dedicated to countering disinformation (disbursed in July 2018 for the StratCom task forces). Furthermore, part of the funding allocated to the Horizon Europe program (formerly Horizon 2020) will be channeled into research on artificial intelligence and algorithms with the potential to contribute to the fight against disinformation.

Transparency, diversity, credibility and an inclusive approach

"In the Commission's view, the following overarching principles and objectives should guide action to tackle disinformation:

• First, to improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated and targeted in order to enable citizens to assess the content they access online and to reveal possible attempts to manipulate opinion.

• Second, to promote diversity of information, in order to enable citizens to make informed decisions based on critical thinking, through support to high quality journalism, media literacy, and the rebalancing of the relation between information creators and distributors.

• Third, to foster credibility of information by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers.

• Fourth, to fashion inclusive solutions. Effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement and the cooperation of public authorities, online platforms, advertisers, trusted flaggers, journalists and media groups."

(European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 24 April 2018, COM(2018) 236 final, p. 8-9.)

Finally, the EU Intelligence and Situation Centre (INTCEN) handles disinformation, perceived primarily as a threat coming from Russia. Broader issues of influence within European agencies arise as well, for the positions of number 2 and 3 in these agencies, although quite crucial (power over appointments and budget), are often sought and held by British officials. In this respect, Brexit will entail an interesting reconfiguration.

In the eyes of INTCEN agents, the efficacy of malicious foreign influence actions—of which information manipulation is but one dimension—lies in a strategy of "trial balloons/wide targeting" which, by definition, can never lose as it is essentially cost-free.

INTCEN's strategy consists first and foremost of exchanges of information, awareness-raising and the removal of barriers between relevant agents. INTCEN established an information exchange network which enables it to raise awareness and refine the interpretative framework used by implicated actors so that they can better detect influence attempts.

To this end, it implemented a number of organizational changes: regular meetings with pertinent actors (East StratCom Task Force, national contact points, NATO), the creation of the Hybrid Threat Fusion Cell dedicated to a transversal tackling of threats of a more specifically hybrid nature, alarm-raising in targeted States (aimed at providing support rather than pointing out weaknesses), etc. The Hybrid Threat Fusion Cell emphasizes the need to anticipate with as few preconceptions as possible. Its priority is to protect the vital infrastructures of Member States, hence the importance of having national correspondents.

As for the means at its disposal, INTCEN's Hybrid Threat Fusion Cell comprises seven members and its approach is chiefly political. It relies on three sources of information: open sources (in collaboration with civil society, think tanks, and NGOs); Member States (e.g. Germany for the Lisa Case); and dedicated institutions, such as the East Stratcom Task Force or the Helsinki European Centre of Excellence for Countering Hybrid Threats.

The European Parliament against hostile propaganda

The European Parliament "1. Underlines that hostile propaganda against the EU comes in many different forms and uses various tools, often tailored to match EU Member States' profiles, with the goal of distorting truths, provoking doubt, dividing Member States, engineering a strategic split between the European Union and its North American partners and paralysing the decision-making process, discrediting the EU institutions and transatlantic partnerships, which play a recognised role in the European security and economic architecture, in the eyes and minds of EU citizens and of citizens of neighbouring countries, and undermining and eroding the European narrative based on democratic values, human rights and the rule of law; recalls that one of the most important tools used is incitement of fear and uncertainty in EU citizens, as well as presenting hostile state and non-state actors as much stronger than they are in reality;

2. Calls on the EU institutions to recognise that strategic communication and information warfare is not only an external EU issue but also an internal one, and voices its concern at the number of hostile propaganda multipliers existing within the Union; is concerned about the limited awareness amongst some of its Member States that they are audiences and arenas of propaganda and disinformation; in this regard, calls on the EU actors to address the current lack of clarity and agreement on what is to be considered propaganda and disinformation, to develop in cooperation with media representatives and experts from the EU Member States a shared set of definitions and to compile data and facts about the consumption of propaganda."

(Excerpt from the European Parliament Resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties.)

B. NATO

The Atlantic Alliance has much experience with these issues, having been confronted throughout the Cold War with Soviet tactics of "psychological warfare" and the use of "active measures." Even today, the Alliance continues to view this phenomenon through the lens of the Russian threat. The Alliance's vulnerability to this threat is heightened by its extended deterrence presence in Eastern Europe, a key target for information manipulation attempts which tend to exaggerate the volume and nature of NATO's military presence in the Baltic countries and in Poland (see above). Other attempts to spread rumors about the alleged crimes perpetrated by German soldiers in Lithuania under NATO command have been detected.

NATO's strategy when responding to such tactics has three dimensions: detection, stemming either from NATO countries themselves or from the Alliance's internal structure (e.g., cells in charge of strategic communications in the context of NATO's Enhanced Forward Presence in the East); analysis of the content and origin of malicious information operations; and response, by confronting the disinformation campaigns with objective facts and ensuring the broad dissemination of those facts.

Within the NATO structure, there is the NATO Strategic Communication Excellence Centre (NATO StratCom COE), created in 2014 in Riga. Their work centers on doctrines, operations and training, and they publish a large number of analyses. The Public Diplomacy Division (PDD) of the International Secretariat primarily plays a coordinating role, by liaising with States, civil society actors, and relevant organizations, notwithstanding their affiliation with NATO (Riga Excellence Centre) or independence from it (EU East StratCom Task Force). The Hybrid CoE in Helsinki acts as a bridge as it is an independent actor cooperating with both the EU and NATO. PDD also engages with the civil society actors concerned. A team of around a dozen people monitors disinformation operations with specialized tools.

The Alliance's website thus has a page dedicated to debunking myths and refuting Russian accusations made against it. For each of the long list of "allegations" made against it, NATO provides a response starting with the word "Fact." PDD has published an abridged version of this list in the form of a factsheet entitled "Russia's top five myths about NATO." The Alliance is also anxious to bring more objectivity to the debate, by publishing hard evidence (such as satellite photographs showing Russia's involvement in Ukraine).

The French position, which holds that NATO's role in this field should remain confined to the detection and analysis of and response to hostile operations targeting its activities (rather than all disinformation and malicious interference operations) is widely shared within the Alliance. Fault lines nevertheless arise between allies on the question of what sort of response is most appropriate. They also disagree over whether or not to try to "beat Russia at its own game," including within Russian-speaking communities, by spreading doubt about Moscow's activities and goals or by offering a revised version of some chapters of history. Such an approach is highly contentious within NATO, where there are diverging views on the severity of the threat that partly reflect different perspectives on Russia's role and the adequate NATO response to Moscow.

C. The OSCE

The OSCE must take into account the positions of all participating States, including Russia, along with the very different situations of countries within the OSCE zone in terms of respect for the rule of law, fundamental rights and freedom of expression.

At the OSCE level, there have been no specific actions taken against propaganda within the framework of the commitment to freedom of expression. The sole exception is the Helsinki Final Act, which deals specifically with the issue of "war or hatred propaganda." The OSCE Representative for Media Freedom, Harlem Désir, approaches these questions from the angle of freedom of speech, by emphasizing the transparency of sources, media pluralism and media literacy. This position has led him, for example, to reject the penalization of disinformation, which can be used as a means of repressing the freedom of expression in authoritarian regimes.

In March 2017, the OSCE representative for media freedom, the UN Special Rapporteur on freedom of opinion and expression, the OAS Special Rapporteur on the freedom of expression and the Special Rapporteur on freedom of expression and access to information for the African Commission for Human and People's Rights published a joint declaration on freedom of expression and "fake news," disinformation and propaganda.[64] The objective of this text was to remind States that the fight against disinformation must not be used as a pretext to limit

64. *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda*, 3 March 2017.

civil liberties, in particular freedom of expression, above the level of that which is permitted by international law.

IV. Civil society

Civil society is at the front line with information manipulation. Whatever measures States may implement, the resilience capacity of any society depends primarily on the mobilization of its citizens. Responses by civil society were initially sporadic and reactive, mostly through fact-checking. Given the intrinsic shortcomings of this approach, civil society has developed complementary initiatives, involving either a longer time frame, a normative dimension or research.

A. Fact-checking

Checking the veracity of facts is the most natural response to fake news and hence the most common one. There were at least 149 active fact-checking websites in 2018,[65] and not all of them are recent. Among the oldest ones is the American site Snopes, which was launched in 1994 and has since become a reference. There is also another American website worth referencing, PolitiFact, which was created in 2007 and won the Pulitzer Prize in 2009 for its analysis of the 2008 Presidential campaign. The proliferation of fact-checking mechanisms is on the rise all over world. Even certain States have taken initiative: in Malaysia, for example, the Communications and Multimedia Commission launched a fact-checking portal (sebenarnya.my) in March 2017. The efficacy of government-led verification is, however, debatable as people who are prone to believing or disseminating fake news are often the very same ones who distrust public institutions. These sorts of websites can even inadvertently vindicate conspiracy theories and boost narratives claiming the existence of a "Ministry of Truth." There is a rather widely held belief that the State should, to as great an extent possible, refrain from directly engaging in fact-checking activities. The one obvious exception is when crises that threaten public order occur.

It is, therefore, within civil society that a proliferation of initiatives can be found. The mainstream media have developed their own fact-checking

65. According to Reporters'Lab, a research centre on journalism of the Sanford School of Public Policy of Duke University, in the United States, which maintains an updated inventory of fact-checking sites in the world. (reporterslab.org/fact-checking/).

websites—an important development in journalism in the past ten years (the AFP Fact Check, the BBC's "Reality Check," *Le Monde*'s "Decodex," the "Hoax or not" section of the Indonesian *Detik*, etc.); Google launched "CrossCheck," an initiative associating over thirty French media companies. Some projects have evolved and are no longer confined to fact-checking, such as the Ukrainian website StopFake, which was created in 2014 by teachers, students and graduates from the Mohyla School of Journalism and has become a reference for its analysis of propaganda from the Kremlin. The Poynter Insistute's international network for fact-checking also adopted a "code" of common principles for guaranteeing transparent and unbiased verification.[66]

Civil society also demonstrated its resilience in Ireland, during the referendum on the 8th amendment and for the purposes of responding to the activities of automated anti-abortion accounts. In this case, a group of pro-abolition volunteers created the Repeal Shield, an instrument which blocked a list of more than 16,000 accounts deemed to be "trolls, bots, and false accounts spreading lies and hateful messages." The tool was used by more than 4,500 users during the referendum campaign.[67]

The power of fact-checking lies principally in its potential to embarrass those who disseminate false information, that is, in reputation-related reasons, rather than in ideological reasons. These people like to be the first to disclose new information, and would be embarrassed in their communities if the disclosed piece of news turns out to be false.

However, fact-checking also has significant structural limitations. First of all, the human brain is relatively impervious to correction. Studies have shown that the correction of a preexisting belief is usually ineffective: most people continue to use the all or part of the information which they know is untrue. This phenomenon is known in psychology as the "continued influence effect."[68] This effect is even stronger when the refuted beliefs were deeply-held. Fact-checking works better on novel topics, to which we attach no preconceptions. The problem is, of course, that "fake news nowadays relates essentially to political themes which reflect deep ideological convictions."[69]

---

66. *Code of principles*, International Fact-Checking Network (IFCN), Poynter.

67. Rachel Lavin and Roland Adorjani, "L'Irlande a déjà trouvé la parade aux *fake news* (mais on ne pourra pas la reproduire)," *op. cit.*

68. Stephan Lewandowsky *et al.*, "Misinformation and its correction: Continued influence and successful debiasing," *Psychological Science in the Public Interest*, 13:3, 2012, p. 106-131.

69. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 50.

Further, fact-checking is by definition a retrospective tool: its corrective nature means that it occurs only once the harm is done—after the incriminated news has been circulated. The act of fact-checking may challenge the falsity, partiality or forgery of a piece of information, while also serving a pedagogical role—but it does not erase the significant psychological impact associated with the consumption of fake news.

Moreover, the results of the fact-check do not always, or even often, hit the target audience, in that the correction is seldom read by those who need to be convinced that a given story was untrue. "The audiences most at risk of being influenced by Russian disinformation might be the least likely to routinely consume or access disinformation sites."[70] "As fake news is the manifestation of popular distrust of the political and intellectual elite, how could verification by those same elites possibly convince those propagating it [the fake news]?"[71]

Finally, there is a risk that fact-checking itself becomes a market, appropriated by an increasing number of actors (NGOs, media and online platforms, such as Facebook). In particular, commercial objectives and/or the desire to appear virtuous can sometimes take precedence over the search for truth. For some, this can discredit the fact-checking tool. Besides, this tool is sometimes appropriated by those very actors who are most committed to circulating disinformation: RT, for example, has launched a "FakeCheck" program in four languages.

All these limitations do not invalidate the importance of fact-checking. It is absolutely necessary, but is insufficient by itself. It is a palliative measure, which must be complemented by other measures.

B. Normative initiatives

We consume information the same way we consume food. Both have the potential to be beneficial or harmful. It is, therefore, necessary to distinguish the former from the latter. In this regard, the fight against information manipulation can draw inspiration from nutrition labelling. This is what some have called the "Michelin model:"[72] labels, indexes and rankings can help to distinguish reliable media from untrustworthy sources. In 2014, Pomerantsev and Weiss recommended the creation

70. Todd C. Helmus *et al., Russian Social Media Influence*, *op. cit.*, p. 76-77.

71. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 48.

72. Clint Watts and Andrew Weisburd, "Can the Michelin Model Fix Fake News?" *The Daily Beast*, 22 January 2017.

of an international disinformation ranking, drawing upon the ranking methodology used by Freedom House or Transparency International.[73]

Several initiatives are underway, including a global index project (disinformationindex.com). The most promising initiative is arguably the "Journalism Trust Initiative" introduced by Reporters Without Borders (RSF). President Macron referenced and supported it during his New Year's Address to the press on 4 January 2018 ("some form of certification of media outlets that respects the profession's ethical code seems to me, in this regard, to be not only interesting but advisable"). RSF officially launched their initiative three months later, on 3 April, alongside their partners: the Agence France Presse, the European Broadcasting Union and the Global Editors Network. Rather than relying on the identification and condemnation of the agents of disinformation, the initiative aims at "reversing the logic by giving an actual advantage to all those who produce reliable information, notwithstanding their status," explains RSF Secretary General, Christophe Deloire. Accordingly, the idea is to grant a quality label to those media who deserve it, that is, who respect a certain number of criteria, such as editorial independence, transparency, and professional ethics.[74] The media would thus be encouraged to meet these criteria so as to reassure advertisers who seek stable and non-contentious environments. Digital platforms could, in the longer-run, decide to highlight quality content by putting forward certified media in their algorithms. RSF's approach is, therefore, of an incentivizing nature.

C. Research

Think tanks and universities have also seized upon the topic. To cite a few examples, the Czech think tank European Values has been convening an annual StratCom Summit in Prague since 2016, which has become one of the sector's most important gatherings. The most recent one, held in April 2018, brought together 200 governmental and civil society experts, from about thirty countries. In the United States, the Atlantic Council has set up a dedicated structure, the "Digital Forensic Research Lab" (DFRLab) which has quickly become a benchmark in the field. Working in partnership with the Bellingcat team, an online investigation platform, this lab performs an important role in detecting and investigating major

73. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 40.

74. François Bougon, "Un label pour redonner confiance dans le journalisme," *Le Monde*, 3 April 2018.

disinformation campaigns. In Brussels, the EU Disinfo Lab also produces noteworthy analyses. We can also add to the list the Alliance for Securing Democracy (ASD), a bi-partisan transatlantic organization whose goal is to respond to Russian interference attempts in democratic processes in the United States and Europe. Created in July 2017 by former senior officials in the American intelligence services and the State Department, the ASD is part of the German Marshall Fund. ASD is known in particular for its "Hamilton 68" Dashboard, which tracks 600 Twitter accounts linked to the network of Russian influence, so as to highlight in real time the themes and hashtags promoted by the Kremlin.[75] This dashboard provides a useful tool for research. A German equivalent was launched in September 2017.

Universities, in particular in the UK, are also tackling the issue: the University of Oxford has a research project on Computational Propaganda; King's College London equipped itself with a Centre for Strategic Communications; and the London School of Economics created a program called "Arena," based at the Institute of Global Affairs, that is dedicated to "overcoming the challenge of disinformation". Elsewhere in the world, Hong Kong University's Cyber News Verification Lab and the partnership between Lund University and the Swedish MSB also deserve mention.

The open-source method as a means to debunk disinformation

The profusion and speed of information on the internet at once magnifies the gravity of the disinformation issue and provides new means of countering it. It is indeed possible to collect a great volume of verifiable information in open source and to then use this information in order to deconstruct distorted news. This was demonstrated in a report by the CSIS, using the example of Syria.[76]

Accused of bombing civilians in Syria, the Kremlin responded "by employing three strategies: 1. *Denying the deed* […] 2. *Militarizing the victims* […] Russia and Syria were able to create an impression that all groups targeted by them were extremists. 3. *Attacking the witnesses* […] one of the most important witnesses to the suffering was the aid organization initially called Syria Civil Defense, later dubbed the 'White Helmets.'" The White Helmets published photos of incendiary cluster bomb fragments which Moscow denies using. On other occasions, it is the Kremlin's own communications

75. GMF - Alliance for Security Democracy, Hamilton 68, Tracking Russian Influence Operations on Twitter.

76. CSIS (Canada), *Who said what? The Security Challenges of Modern Disinformation*, *op. cit.*, chap. 6. The following quotations are taken from this report.

which unwittingly reveal compromising information: on 18 June 2016, for instance, in an RT report on a visit by the Russian Minister of Defense to the Khmeimim Air Base, RBK 500 ZAB-2,5SM incendiary cluster bombs could be discerned under an Su-34 strike fighter. This section of the video was cut out and is, therefore, missing from the version now available on YouTube. Thus hyper-connectivity is both the problem and part of the solution, enabling access to an abundance of information and allowing citizen journalists to conduct in-depth inquiries (such as those conducted by sites like Bellingcat.com, for example). Such an approach, which "empowers individuals not only to discover information about Putin's war in Syria, but also to verify the information themselves" is "the polar opposite of Russia's opaque disinformation campaign, which relies on ideological narratives over verifiable facts." One example of the power of collaborative journalism is the brilliant study conducted by *The New York Times*—undertaken in partnership with the Bellingcat investigation group—which proves that Al-Assad's regime was responsible for the chemical attacks in Douma.[77]

D. Grassroots initiatives

There are individual initiatives, such as the hashtag campaign #Кремльнашуисториюнеперепишешь (*#Kremlin you will not falsify our history*) launched by the Lithuanian writer and TV presenter Andrius Tapinas, as well as collective initiatives, such as the group acting as "elves," in contrast to trolls—an online community of Lithuanian origin of around 4,000 activists.

E. Journalists

Journalists are of course on the frontline of the struggle against information manipulation and they often participate, or even initiate, some of the aforementioned actions. A number of them have distinguished themselves individually. Two such journalists are Jessikka Aro, a Finn who studied troll factories, and the German Julian Röpcke, who investigates Russian influence in Germany. Journalists also act collectively, through the creation of groups such as the Baltic Center for Media Excellence, whose objective is to raise journalistic standards and improve the overall media environment in the Eastern partnership countries; or the Re:Baltica portal and the Toneboard start-up, which received a grant from Google to create a platform for verifying fake news.

77. Malachy Browne *et al.*, "One building, One Bomb: How Assad Gassed His Own People," *The New York Times*, 2018.

The challenge, even for the mainstream media, of implementing the necessary verification mechanisms for quality journalism is well-illustrated by the recent event known as the Babtchenko affair in Ukraine: virtually all of the higher-quality mainstream media had headlined the death of Arkadi Babtchenko on May 20, 2018, on the basis of information deemed credible, originating from the Ukrainian government, before having to announce the following day that they had been wrong.

V. Private actors

Large digital platforms have long shown a lack of interest in the struggle against information manipulation, which they presented as irrelevant in light of their "non-editorial status" and obligation to guarantee freedom of expression and trade freedom. But they have since revised their communication and response policy on two occasions: firstly, in the wake of the debate on the prohibition of terrorist and illegal content and, secondly, following the debate on interference in electoral campaigns.

A. From a non-subject to a matter of serious concern

The issue of the platforms' responsibility for the nature of the content disseminated through them first became a matter of serious consideration in the context of the fight against terrorism. In particular, digital platforms were publicly accused of permitting communication among terrorists as well as the circulation of shocking content aimed at unsettling users and/or mobilizing their support.

It is of course necessary to distinguish terrorist content from information manipulation. While in the case of the fight against terrorism, the principle of freedom of expression does not take precedence over the security imperatives, the terms of the debate are not as clear cut when it comes to information manipulation. However, in both cases it is important to recognize that digital platforms are in a position to monitor the information circulated and exchanged through them. They are equally capable of taking action to ensure that certain content is less visible or even eliminated completely.

Despite an enduring reluctance to publicly address the issue of information manipulation, large platforms have, under pressure from governments and civil society, been increasingly compelled to justify

themselves and then take appropriate action. In this regard, the 2016 American presidential campaign can be viewed as a double catalyst.

Firstly, the significant amount—in rubles—spent on political advertisement aimed at damaging Hillary Clinton's campaign sparked a wave of increased awareness in large segments of the American political elite. Accustomed to the vigilance of traditional media toward the sale and broadcasting of advertisements, especially when purchased from a foreign seller, U.S. political representatives were disconcerted by the small interest in the matter displayed by digital actors. Their unwillingness to enforce any control or verification mechanisms for advertisements, despite being in a position to implement precise targeted advertising, was seen by many to be unacceptable and a blatant lack of responsibility.

A few months later, the Cambridge Analytica scandal strengthened this perception. The issue at stake was no longer the sale of advertisements but the handling of personal data collected through Facebook, without the users' prior consent. Through this illegal harvesting, the company was able to implement particularly sophisticated micro-targeted advertising, aimed at shifting election results in favor of Republican candidate Donald Trump either by promoting his ideas and campaign promises or through denigrating those endorsed by the Democratic candidate Hillary Clinton.

Facebook is now criticized for failing to protect its users' personal data. Interestingly, the European model—usually derided in the U.S. Congress—has been explicitly commended for its attention toward this issue.

The roots of that realization do not just stem from the American Presidential election. Other factors have likely also played a role: the end of Obama's term in office (he was the "first digital President" and was particularly sympathetic towards large digital corporations), the desire by some on the Democratic side to deny responsibility for losing an election deemed impossible to lose, power relations in need of rebalancing between state administrations and private actors, etc.

Each of these factors helped to reverse the burden of proof. European States—who have often been criticized for being defensive actors with a preference for regulating innovation—saw a majority of Senators and the public agree with their cautious position. On the other hand, digital platforms were cast in a less flattering light. They were seen as indifferent towards privacy concerns and the operation of democratic institutions, as well as reliant on a questionable economic model. These actors are now the ones being called upon to explain themselves.

What the Cambridge Analytica Affair reveals about tomorrow's persuasion tactics

"The recent so-called Cambridge Analytica case reveals […] that tomorrow's persuasion tactics could be nothing like the old strategies of spreading rumors, and more like the targeting of each individual voter. Indeed, this new method consists of 'using data to change behavior,' or in other words acquiring such a deep understanding of each citizen by combining a multitude of information on his behavior, personal ties, habits, desires, fears, etc., that the computer will be able to incite them to vote or to buy that which perfectly matches their needs. The goal is no longer to convince the individual who has been profiled in this way and is anticipated to adhere to a certain set of ideas, but to make his political choice appear to be spontaneous: I believe A, therefore I receive a message telling me that candidate Y thinks so as well.
According to this model, we have gone from a strategy of mass political persuasion dumped by the media, to targeted soliciting tailored to our deepest wishes."

(François-Bernard Huyghes, "Que changent les *fake news*?" *La Revue internationale et stratégique*, 110, 2018/2, p. 83-84.)

Mark Zuckerberg's hearing in April 2018 is without a doubt the acme of this collective realization, because it was the first time that the CEO of a major digital corporation found himself obliged to publicly answer for the functioning and responsibility of his firm. Although many commentators continue to debate the long-term consequences of this recent wave of protest, for the moment Zuckerberg's hearing has not resulted in the withdrawal of a significant number of users or a decline in the market value of these digital platforms. It must be noted that platforms have hyped up publicity around their efforts to counter information manipulation.

B. The response of large online platforms to information manipulation

Online platforms have developed a significant array of mechanisms against information manipulation, in response to—and hence in accordance with—the criticisms they face. The intensification of these critiques has compelled platforms to put forward a great number of measures within a very short time span, without always having previously articulated a genuine response strategy. In this respect, the various proposed measures do not always have the same goal (provide targeted or more structural

responses), or the same temporality (preventive or *ad hoc* action), the same scale (measures applying to just one country or to all users). They can nevertheless be categorized along the six following criteria:

1. Raise users' awareness of the risks and challenges of information manipulation

A significant proportion of those measures aim at fostering Internet users' awareness of the processes by which information is exchanged, disseminated and hierarchized on online platforms: for example, Facebook has published user guides outlining good practices to deal with information circulating on social networks; Google has intensified its didactic efforts to explain the criteria underpinning the sequencing of information by search engines. These awareness-raising strategies are not confined to prevention: online platforms have also decided to alert their users who were exposed to false information. This was notably the case with Facebook, which announced they had sent a warning message to those users whose data had been collected by Cambridge Analytica during the U.S. presidential election (so far amounting to 87 million users). For each of these examples, the stated goal is to give internet users "the tools" that will enable them to identify and respond to information manipulation themselves.

Moreover, a number of platforms—including Facebook—have reached out directly to various candidates in the presidential election so as to make them aware of the risks and encourage them to develop good internet practices. More broadly, online platforms have also strengthened the protection of data privacy, for it appears that information manipulation campaigns are often based on the exploitation of personal data—either by stealing it or by tailoring it to their narratives. Thus Facebook has significantly improved the interface that allows its users to control the visibility of their personal data (in particular through a centralization of all settings). The platforms are also more active in protecting their users against the risk of data piracy: in early May 2018, faced with a leak which risked exposing its users' passwords, Twitter demonstrated its responsiveness by immediately asking users to change their passwords.

Finally, through public hearings, large online platforms contribute to raising public awareness of the need for increased vigilance against information manipulation.

2. Improve the detection of information manipulation

Information manipulation campaigns often rely on automated accounts (bots), networks of automated accounts (netbots) and anonymous accounts. Whereas platforms used to be reluctant to identify and deactivate the latter—for a number of reasons (economic model, editorial neutrality)—they have recently shifted their approach. They started by taking a closer look at their users' accounts so as to suspend accounts that were fake, automated, and/or suspected of participation in an information manipulation campaign. Twitter announced that it had suspended over 50,000 accounts "connected to Russian interference," to quote the company's spokesperson. However it is difficult to assess the effectiveness of these account suspension campaigns. They very often do not confine themselves to targeting accounts that are likely to participate in information manipulation campaigns: they mostly suspend fake accounts sold by reputation management companies whose aim is to boost their clients' visibility. In late 2014, Instagram thus launched an operation to purge 300 million accounts (#PurgeInstagram), which had significant repercussions for the visibility of American stars' accounts (Kim Kardashian, Katy Perry, Oprah Winfrey, Justin Bieber and Rihanna). Facebook had adopted a similar approach in 2012, by launching a large hunt against fake "likes," though with only limited success. Since 2016, the fight against "the fake" has become the object of a war of figures, the effectiveness of which is difficult to assess. At the end of the first quarter of 2018, Facebook claimed to have suspended 583 million fake accounts and about 1.3 billion over six months.

In cooperation with the US government, Facebook, Twitter and Google have also set up an initiative aimed at creating a common database listing fake accounts and the strategies developed by trolls to escape identification. The goal is to optimize information manipulation detection by exchanging information on the models and actors behind it. Other measures, relying on artificial intelligence, have been implemented to detect and suspend these accounts, sometimes even before they are activated. Twitter thus prohibited the use of multiple accounts simultaneously (a method very often adopted by trolls). Along the same lines, Facebook also announced that they had developed a tool enabling them to detect the serial publication of similar messages and comments. All of these techniques are routinely used by manipulation campaigns.

3. Contain the dissemination and impact of information manipulation campaigns

Online platforms have developed several measures to speed up the removal of malicious content. While techniques based on artificial intelligence are used as preventive measures (before the content is published online), platforms continue to rely on human involvement to monitor—and sometimes erase—exchanged content and dubious advertising. In December 2017, Facebook announced that they had recruited an additional 1,000 staff members to check advertising and remove it whenever it did not meet acceptable standards (i.e. when they target people according to their political, religious, ethnic or social affiliation). Facebook has also increased the teams dedicated to verifying dubious content by over 60%, with a total staff of 8,000 people globally. While this reinforcement of human involvement is significant, it must be noted that it primarily concerns the monitoring of content deemed illegal and/or related to terrorism. In July 2018, however, Facebook announced the implementation of a "new policy" of deleting content susceptible of causing violence, starting first with countries where disinformation has triggered violence,[78] such as Sri Lanka, for example, where messages claiming that Muslims were poisoning Buddhist food were erased from social networks.

Twitter also sped up the cleaning process, through the introduction in May-June 2018 of new mesures to combat trolling and hateful and extremist comments,[79] and the suspension of at least 70 million accounts in only two months—twice as high as the suspension rate in October 2017.[80]

Platforms have also enhanced reporting mechanisms: procedures allowing internet users to report dubious posts have been simplified. Google has recently introduced tools enabling its users to report "misleading and false" content. Facebook now grants greater attention to the feedback and comments of web users who have identified fake information. More broadly, Facebook seeks to standardize its response to information manipulation through the development of an analytical framework that they call "Problems, Surfaces and Actions." The goal of

78. Sheera Frenkel, "Facebook to Remove Misinformation That Leads to Violence," *The New York Times*, 18 July 2018.

79. Yoel Roth and Del Harvey, "How Twitter is fighting spam and malicious automation," blog.twitter.com, 26 June 2018.

80. "Twitter is sweeping out fake accounts like never before," *The Washington Post*, 6 July 2018.

this framework is to objectify response thresholds (when and how to respond), coordinate the work of various teams and enforce a standard response procedure. The latter includes, in particular, recommending fact-checking articles (which deal with the same facts as the dubious content posted online and enable users to take a step back from the fake information); notifying the number of other users who deemed the information to be false or misleading; and an alert that the user is likely to relay false information. In the same vein, YouTube chose to display, next to some conspiracy videos, a link to a Wikipedia article directly challenging the conspiracy narrative.

Finally, online platforms also developed tools to detect the "deep fake," i.e. fake news that can very convincingly reproduce the effects of reality. Google has announced that it has created a tool capable of detecting such videos (in particular those that can make public figures talk) and of removing such content before it is posted online.

4. Regulate and cooperate

For a number of reasons (cultural, economic, technical), online platforms are wary of regulation. They tend to favor informal cooperation with public authorities and the media.

Facebook thus collaborates on a regular basis with traditional media outlets so as to exchange records listing those articles circulating on its website which were flagged as fake news. Google reported having done the same during the American and French presidential campaigns. The two platforms also ran several initiatives in close cooperation with civil society and the media to counter information manipulation (see above).

Facebook also declared that it had collaborated directly with the German government during the most recent general elections. The terms of that partnership were directly dictated by German legislation regulating social networks, which—among other things—makes it compulsory for these online networks to remove any blatantly illegal content, and in particular hate speech and discrimination, within a very short time span (between 24 hours and 7 days in contentious cases). Other countries are also considering implementing legislative mechanisms that would oblige platforms to act more decisively against contentious content.

5. Promote good practices and institutional actors

Platforms very often choose to promote constructive approaches to counter information manipulation. A policy favored by many of them consists in reinforcing the visibility of reliable content and/or those produced by trustworthy media sources in their search engines and news feeds. This entails, in particular, updating ranking algorithms as well as blocking websites that do not display their country of origin. It also implies proactive action to detect the most common sources of disinformation (conspiracy sites, sites masquerading as institution websites and relaying false information) so as to reduce their visibility (without necessarily removing them).

YouTube, Google and Facebook also put in place the "Trust Project Initiative," in partnership with Santa Clara University, whose objective is to promote reliable content by enabling those who produce it to share information on the fact-checking procedures they implement, the history of the media outlets for which they work, as well as the structure and identity of its management and shareholders. These various elements of information, which appear as tabs, seek to highlight the ethical standards and the trustworthiness of these various media sources.

Finally, digital platforms also promote the creation of spaces for "constructive" debate: Twitter has undertaken to develop, for example, indicators that make it possible to monitor the diversity of exchanged opinion(s), the receptivity of users and media awareness of the issue. As for the Snapchat application, which is very popular with younger demographics, it has opted to divide its content into two categories: "Discover" and "Social." This division enables Snapchat to indirectly promote institutional media, which are the only media sources that appear in the "Discover" section (other types of content that present themselves as information—blog posts, comments, shared posts and articles—are confined to the "Social" interface).

6. Analyze the mechanisms of information manipulation campaigns

In the face of stark criticism for their naivety and lack of discernment towards the impact and the scale of information manipulation campaigns, the platforms have emphasized their need to better understand the phenomenon. To achieve this, they have put in place various partnerships and exchange policies with the world of research. Facebook has, for

example, recently agreed to share some of its data with Stanford University, enabling the latter to study information manipulation campaigns, notably through its "Project on Democracy and the Internet."

Likewise, the platforms contribute to the funding of initiatives aimed at developing a better awareness of ethical issues linked to platform usage, including in the field of information. This is, for example, what Google sought to do by creating "DeepMind Ethics & Society".

While the social platforms have come to grips with the fight against information manipulation, there remains a lot of work to be done. As *The Wall Street Journal* recalls, Twitter CEO himself, Jack Dorsey, shared at least 17 tweets from a Russian troll between late 2016 and mid-2017.[81]

C. The contribution of the field of advertising and marketing research

The field of advertising is often presented as a stronghold of disinformation, in that it seeks to manipulate the mind for profit and commercial purposes.[82] How does one boost sales? How should one make a product attractive to a particular public? How can one promote one product over another? Such questions are at the very root of not only information manipulation techniques, but also effective responses to this manipulation. How can we ensure that messages published by reliable conventional media are heard over the din of propagandist media?

The tools developed by advertising and marketing research arguably present at least two advantages as regards the study of information manipulation. First, by analyzing the response of target groups to particular campaigns, these tools enable us to better grasp the impact—visual, emotional, rational, and intellectual—of any given message on a particular audience. Furthermore, by highlighting the weaknesses and "voids" of published messages, as well as the reasons why a particular user is attracted to one particular message over another, these tools inform us on the manner in which conventional media, that are perceived as reliable, can better their appeal and capture the attention of those audiences who bypass them.

81. Georgia Wells, Rob Barry and Shelby Holliday, "Russian Trolls Weigh In on Roseanne Barr and Donald Trump Jr.", *The Wall Street Journal*, 19 June 2018.

82. François Géré, *Dictionnaire de la désinformation,* Armand Colin, 2011.

In the field of advertising, research seeks to analyze the influence of a campaign on *ex-ante* sample groups.[83] Studies aim to predict the effectiveness that an advert is likely to have on the market by analyzing the audience's attention levels, their connection to the brand, the entertainment generated by the ad for the user, drops in attention levels as well as the emotions produced. These tools also make it possible to identify the weak points of a given campaign. Studies are also conducted *ex-post* so as to monitor the evolution of preferences among various populations—in particular, among younger generations—untapped consumers to be ensnared. Such tools include interviews with sample groups as well as the monitoring of the user's perceptions of an advertising campaign.

Were they to be applied to information manipulation, these various techniques would arguably provide a strong explanatory dimension. One could imagine conducting a similar study to compare the respective trajectories of a conventional article and a "distorted" one. An analysis of the attractive power of the false information might thus allow us to strengthen the influence of reliable media on a variety of audiences. Devices such as "eye tracking," which measures the user's eye movements, also enable us to better grasp users' responses to fake news in order to better implement counter-measures.

Marketing studies, for their part, focus on analyzing market availability to particular products.[84] These studies can, for example, analyze the response of consumers to a particular brand (how is that brand perceived? What are its main features? How does it position itself in relation to other brands?) or to a given product (dissemination of the product within a sample group, assessment of new trends, assessment of the product name and price). These tools also aim at understanding consumers themselves (segmentation: who are they? Buyer's decisions: why do they buy? Internet monitoring: follow online forums and online after-sale services so as to evaluate consumer satisfaction, etc.).

Those who manipulate information already use a marketing technique called the "A/B test," which consists in comparing the impact of two variables, in this case two messages. For example, manipulating actors would start by circulating two messages stating that "black people are terrorists" and "black people are criminals" and, realizing that the latter works better than the former, they would then bank on this second message and continue to refine it so as to improve its potential to go

83. Joel J. Davis, *Advertising Research: Theory and Practice* (2nd Ed.), Pearson, 2011.
84. Paurav Shukla, *Essentials of Marketing Research,* Ventus Publishing ApS, 2008.

viral. Such techniques would surely have an explanatory function (why do particular fake news stories work?) as well as an operational utility (how to improve the attractiveness of reliable conventional media in comparison to RT and Sputnik?).

Despite the bad press often associated with it, advertising and marketing research can offer interesting perspectives in the fight against information manipulation. To counter manipulation, it is necessary to understand the reasons for its success among a variety of audiences: why is this message attractive? What sort of demand is there in the information market? The fight against manipulation also requires us to strengthen reliable conventional media sources, through a better understanding of their shortcomings and the efforts that are required to make them attractive to publics who are turning away from them.

Part Four

FUTURE CHALLENGES

I. How to anticipate the future?

It is difficult to anticipate future challenges. Our adversaries are creative and quick to adapt; technology and the media evolve rapidly; and it is easy for new actors to arrive on the stage (entry costs are nonexistent, the risks are very low due to the difficulty of attribution, and potential gains are very high). For all of these reasons, we should expect information manipulation to expand and involve an ever-increasing number of actors.

Had someone said ten years ago that the recently created social networks (Facebook in 2004, Twitter in 2008, Instagram did not exist yet) would play such a tremendous role in the lives of billions of people and be implicated in a massive information problem threatening our democratic life, hardly anyone would have believed them. It is, therefore, difficult to imagine what it is that will—ten years from now—shape our social interactions and pose the most serious challenges. For instance, it is possible to imagine that the use of currently open networks will decrease and the use of closed networks (WhatsApp, Telegram, etc.) will increase. This scenario would pose different types of challenges to public authorities, particularly in terms of encryption.

A. Technological challenges

In any event, technological innovation will play a decisive role. Not only innovation but also its democratization: costs will decrease at the same time as efficiency, accessibility, performance and the speed of propagation will increase. Artificial intelligence will make bots more human and, therefore, harder to detect. It will also progressively erode linguistic and cultural barriers (which remain a shield against foreign influence attempts for some countries), thanks to the enhancement of translation software. Photo, audio and video editing software, for example, will render it possible in the near future (some of them already do so today) to make anyone say anything. This makes the detection of false information even more difficult. "Deepfake videos," in which people's faces are digitally modified in order to make them do or say anything that one wants, are already very believable. The US Department of Defense also identified these altered videos as an issue in the midterm elections of 2018. As such, the US Defense Advanced Research Projects Agency (DARPA) even provided funding for the Media Forensics Project, whose goal is the development of technologies capable of automatically identifying and targeting these Deepfake videos.[1] An even greater danger, far more subtle than the creation of a fake video, arises from the slight alteration of only a part of an audio or video clip, such as a recording of a speech. Another peril lies in the possible creation of a great number of variations of that speech—e.g. the circulation of twenty different versions of a single speech, so as to hide the authentic version in the confusion.

Fictional personalities are another risk. Over a three-year period, from 2014 to 2017, Jenna Abrams was a famous pro-Trump activist, an icon of the American "alt-right," quoted by the mainstream media (including *The Washington Post*, *The New York Times*, *The Independent* and France 24) and followed by 70,000 accounts on Twitter. However, Jenna Abrams did not exist: her account was a creation of the IRA, the Saint-Petersburg-based troll factory.[2] Artificial intelligence will enhance the sophistication of fictional personalities and make them less readily detectable. These personalities will be able to give interviews and write columns in the press before they are uncovered.

1. Jeremy Hsu, "Experts Bet on First Deepfakes Political Scandal," *IEEE Spectrum*, 22 June 2018.

2. Ben Collins, Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World," *The Daily Beast*, 11 February 2017.

These trends will be part of an extreme atomization of information in light of the disappearance or weakening of those actors who serve as "trustworthy third parties" (such as traditional media, in a context in which the official word will continue to be largely discredited). In such an environment, the crucial issue will be to know how to recreate a "trustworthy third party." Aside from reinforcing the economic model and the credibility of traditional media, other approaches have already been put forward and deserve further exploration (such as the use of blockchain technology which allows for better information traceability).

Even progress in social psychology research, in particular in terms of the way in which we make decisions, can be "arsenalized," allowing us to carry out micro-targeting in a more precise and efficient manner. The strength of these three combined ingredients—knowledge in social psychology, big data and artificial intelligence—can be used to create a weapon of mass division.

B. Future trends in Russia's "information warfare"

It is, by definition, difficult to anticipate the next move by actors with a distinctive capacity to tailor-make their actions and learn from their mistakes. However, we believe that the Kremlin is going in the following directions:

1. Kinetization

We already observe a growing interest by Russian actors on the physical level, that is, the communications infrastructure. While this interest did not appear during the annexation of Crimea, it was undoubtedly reinforced by this operation, during which Moscow intervened directly in the information flow received by the population of the peninsula by literally cutting some internet and phone cables. The Crimean case nevertheless remains a unique case study, due to the peculiar geography of the region and Russian intelligence services' prior knowledge of the territory. In the long-run, the two physical layers that are of greatest interest to Moscow are the submarine—for the cables which, as we have known for years, can be pirated—and the spatial—for the satellites around which some maneuvers have on occasion been observed. We can, therefore, expect a greater overlap between the kinetic and non-kinetic dimensions of Russian operations.

2. Personalization

There is a trend towards the personalization of attacks. This technique is not new, as is evidenced by the Soviet and Russian services' use of the "*kompromat*" method, i.e. compromising a target who can thus be controlled and manipulated. In the field of information, the focus of this report, this trend could take the following guises in the years to come. Customized attacks could target active military personnel, which is already the case in Ukraine: the modern version of airdropping fliers is now sending text messages by phone. Ukrainian soldiers are already accustomed to receiving messages designed to lower their moral and cohesiveness, for example by claiming that they are "surrounded and abandoned." Then, several minutes later, their families receive a message announcing the death of their son, brother or father, at the hands of the enemy—which then brings families to call the soldiers, and allows through the concentration of signals to detect their location and bomb them,[3] in a tragic self-fulfilling prophecy.

A resurgence of Russian activity aimed at Western soldiers in external operations has also been observed. For example, military forces deployed in Baltic States in the context of NATO's Enhanced Forward Presence have been targeted. This activity involves traditional methods (using a physical approach) but also some more innovative approaches. The latter rely, for example, on the exploitation of soldiers' personal data via social networks.

Such personalized attacks could also target civilians, be they politicians, senior officials or prominent public figures. Particular vigilance must be maintained in the case of targeted attacks which would be embedded in legitimate campaigns carried out by a variety of actors, such as the Paradise Papers or the #metoo movement. Massive leaks, all too obvious in the wake of the "DNC Leaks" and the "Macron Leaks" are, therefore, less of a risk.

3. Mainstreamization

The range of media which spread the Kremlin's doctrine, sometimes inadvertenly, continues to expand. Those media sources which appear closely tied to the Russian government (RT and Sputnik) and/or who too obviously defend its positions are now clearly identified as propaganda organs. Even though their circulation is increasing and their target

3. Col. Liam Collins, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, 26 July 2018.

audiences are widening, they could face greater competition by other forms of information dissemination. The Kremlin is likely to invest more intensely in "converting" personalities who are not known to be pro-Russian. The Kremlin may also try to work some of its messages into the larger, more traditional media outlets. This would result in a Russia's information warfare going mainstream, which will be more difficult to counter. Crude disinformation, absurd fake news and "infotainment" websites are weapons of mass distraction: they offer a diversion that benefits subtler and hence more dangerous manipulation attempts.

4. Proxyzation

With Europe and North America becoming both obvious targets as well as spaces saturated with counter-measures, with highly educated populations with high levels of awareness regarding this phenomenon, we expect that the battlefield will expand to include new fronts as previously identified (see above), particularly in Africa and Latin America. From the aggressor's point of view, these regions have several added benefits: of being easily penetrable given that they speak common languages (English, French, Spanish), in which these informational apparatuses already exist; they have less educated populations who are consequently easier to influence, despite being highly connected thanks to the democratization of information and communication technologies. Their communities are also ripe with passions that are easily exploited, such as ethnic and religious tensions as well as resentment towards old colonial powers. As such, in its effort to weaken Europe, Russia may use these populations as proxies.

This phenomenon is already at play in the Maghreb, where there are massive Russian investments, not only in the energy sector. Populations in the Maghreb are largely exposed to propaganda from the Russia media in Arabic, which conveys anti-European messages. These populations serve only as an indirect target, or a vector; the real objective is for these populations, who interact on a daily basis with family and friends living in Europe, to relay these messages back to Europe and convince others that the European media is lying and that the Europeans are hostile towards them. The anti-immigration propaganda in Europe today, which works to agitate nationalist communities, is therefore only one facet of the operation. To create division and pit communities against each other, it is also necessary to convince immigrant populations that they are mistreated.

In this respect, the practice of using relays in North Africa is particularly effective.

These tendencies, which are only likely to increase in coming years, are of serious concern. What is even more worrisome is the knowledge that these actions will be less and less an isolated case: we must worry about the activities becoming pervasive and the actors becoming more diverse—the fact that many more will do tomorrow what the Russians have long been the only ones to do, or to do so well.[4]

II. A few prospective scenarios

The following scenarios are fictitious. They aim at drawing attention to a number of weaknesses.

• Scenario 1. In the context of the "citizen consultations" on Europe, which began last April and will end in October 2018, coordinated actions are deployed, combining online manipulation—a massive dissemination of false information and posts via bots—and the sponsoring of physical "Trojan horses"—identified in advance as proponents of opinions favorable to the manipulating interests—so as to foster a radicalization of the debate and/or jeopardize the credibility of the consultations. In a second phase, the content of the reports to the European Economic and Social Committee could also become the target of an information manipulation and/or a denigration campaign, through the automated propagation of the most subversive posts.

• Scenario 2. As the post-Brexit negotiations promise to be long and difficult, there are attempts at email hacking which would reveal the contact details of the political representatives and officials in charge of the negotiations, including their confidential correspondences. If successful, these attacks could result in the selective dissemination of—potentially falsified—content so as to discredit the negotiation process and/or spread the seeds of discord between European partners, and between the EU and the United Kingdom. One-off information manipulation campaigns are also likely to target specific points of the negotiations, so as to spark emotional responses from the British

4. Usha Sahay and Clint Watts, "WOTR Podcast: a conversation with Clint Watts on influence and information in the social media era," *War on the Rocks*, 19 June 2018.

and European public, and thus reinforce mistrust between the people and the European institutions.

• Scenario 3. Several information manipulation campaigns are launched in order to exacerbate tensions between EU Member States. One of these is targeted at the content of the Visegrád group meetings, crediting the Central European States with intentions they do not actually have—in particular, on issues of "illiberal" democratic governance or on differences in foreign policy matters—and thus reinforcing mistrust between Eastern and Western European States ahead of the 2019 European elections. Another campaign could target the EU leadership and the reform ambitions borne by the Franco-German partnership, and reinvigorate the intra-European divisions generated by the Eurozone crisis by spreading news of purported projects aimed at bringing to heel the Southern Member States (Italy, Spain, Portugal and Greece), notably on issues of monetary governance and renationalization of public spending.

• Scenario 4. Attacks specifically targeted at France take place in order to undermine the government by creating one or several major political scandals. A malicious campaign is organized against a particular member of government, drawing on a preexisting or entirely fabricated case with high media impact (fiscal evasion, corruption, harassment or sexual scandal). A short campaign is also launched against the government's institutional reforms, which calls into question the government as a whole and play on the emotional charge of certain mechanisms (use of the 49.3, "*ordonnances*" or government rulings, fake roadmaps, etc.).

50 RECOMMENDATIONS

I. General recommendations

1. Define and clearly distinguish the terms, as we sought to do in the introduction. This should help counter widespread relativism, in other words, the claim that "everything is propaganda" and that all the media spreads disinformation. We must not condemn the defense of national interests—Russian media have a legitimate right to defend Russian viewpoints, including those of the Russian government—but the information manipulation. Running a "DIDI" diagnostic (Deception, Intention, Disruption, Interference), as recommended by the Swedish MSB and Lund University, could help with differentiating real information manipulation from more benign influence activities.[1]

2. Do not underestimate the threat, even though it may not be perceptible on an everyday basis. The Finnish Security Strategy for Society insists that a good preparation against information manipulation depends on an accurate evaluation of the threat. To understand the threat, it recommends regularly envisioning possible

1. James Pamment *et al., Countering Information Influence Activities*, *op. cit.,* p. 7.

threatening scenarios and planning for the potential risks and conflicts that they would involve.[2]

3. See beyond the short term. Influence operations serve both long-term and short-term goals. The short-term goals relate to specific events, often an election, an armed conflict, a social protest, a natural disaster, an assassination (Nemtsov) or an attempted assassination (Skripal), a plane crash (MH17), etc. Fake internet accounts and hoaxes are thus more conspicuous, more aggressive, and less subtle because they have an inherently limited lifespan and are bound to be exposed or suppressed once the goal has been achieved. Long-term operations, on the other hand, are aimed at undermining certain ideas and opinions, or at exacerbating tensions and divisions within targeted communities. They have insidious, incremental subversive effects, steered by more subtle and discreet actors, and with consequences that are more difficult to assess. Those long-term operations are the most dangerous ones. They follow a pattern of erosion: it is through repetition and persistence over a long period of time that water eventually wears down rock. Hence it is important to go beyond short-term approaches, often through the prism of electoral cycles (i.e. that tackle only those informational threats that arise during elections), in order to understand the daily nature of the challenge.

4. Strengthen the resilience of our societies. Information manipulation feeds off of divisions and tensions that run through the fabric of our societies. Hence, we cannot fight back effectively, or durably, against these forms of manipulation without the political will to increase resilience within our societies. From this point of view, we have much to learn from certain States, in particular Finland, who has made resilience against so-called "hybrid" threats into a national concept.[3]

5. Do not surrender the internet to extremists. Conspiracy theories prosper all the more easily if they are not contradicted.[4] "Internet users who exercise a form of scientific rationality consider the exchange of views with 'believers' to be a waste of time and they prefer to mock or ignore them. In a similar fashion, 'liberal' internet users do not necessarily

2. Finnish Government, *Security Strategy for Society. Government Resolution,* The Security Committee, November 2, 2017.

3. René Nyberg, "Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History," Carnegie Endowment for International Peace, 8 February 2018.

4. Gérald Bronner, *La Démocratie des crédules*, *op. cit.*

deem it worthy to engage in debates with racist, sexist or homophobic users in order to deconstruct their arguments. As a result, online debate is saturated with lies and aggressive content."[5]

It is necessary, however, to also give due consideration to the risk of the "boomerang effect," for to refute is also to reiterate. Every correction indirectly increases the circulation of the false information. This propagation effect cannot be avoided and it is therefore important to pick one's battles, that is, to focus on counteracting those instances of information manipulation that are most dangerous.

6. Do not yield to the temptation of counter-propaganda. As Fred Iklé wrote in 1989, "truth is democracy's best POLWAR [political war] and PSYOP [psychological war] weapon," for "the goals of democracy can only be accomplished with methods that are compatible with democracy."[6] For democracies, then, the best possible response to information manipulation is always "a persuasive factual proof released at the right time."[7]

7. Do not rely on "technological solutionism," as Evgeny Morozov warns us his evocatively titled book, *To Save Everything, Click Here*.[8] There is no one solution to contemporary information issues; the response must be multi-dimensional (just as the problem is multi-dimensional).

II. Recommendations for Governments

8. Avoid heavy handedness. Civil society (journalists, the media, online platforms, NGOs, etc.) must remain the first shield against information manipulation in liberal, democratic societies. The most important recommendation for governments is that they should make sure they retain as light a footprint as possible—not just in keeping with our values, but also out of a concern for effectiveness. As one of the roots of the problem is distrust of elites, any "top down" approach is inherently limited. It is preferable to champion horizontal, collaborative approaches, relying on the participation of civil society. This also relates to attacks

5. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 174.

6. Fred Iklé, "The Modern Context," in Carned Lord and Frank R. Barnett (eds.), *Political Warfare and Psychological Operations*, Washington DC, National Defense University Press, 1989, p. 7.

7. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 232.

8. Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, PublicAffairs, 2014.

against the population: the largest investigation on the subject (with 74,000 respondents in 37 countries in 2018) shows that respondents feel that in the fight against information manipulation, the main responsibility falls unto the media (75%) and digital platforms (71%) and then governments, especially in Europe (60%) and Asia (63%), followed by the United States (40%).[9]

It is important to acknowledge the intrinsic limitations of any purely governmental response, which is bound to be regarded as biased and propagandist. The response therefore needs to be holistic. This is nothing new: in 1952, the Director of the Information Research Department (a then-secret section within the British Foreign Office, which employed up to 300 people tasked with offsetting Soviet influence in the United Kingdom) declared at a conference on counter-propaganda that "we have to dispel any idea that the fundamental issues, and the action that flows from them, are simply the business of governments and government-controlled agencies. Government-sponsored information, tendentious hand-outs, statements of opinion and all obvious attempts to influence free opinion are worse than useless, or should be."[10]

In this way, it is preferable that States design a choice architecture without enforcing a particular choice, in accordance with the "nudge approach" in behavioral economics.[11]

9. Create a dedicated structure. Most of the States concerned have already done so. Those that have not should establish a national entity responsible for the detection and countering of information manipulation. This entity can take various forms—from the network of competent people presently scattered across distinct services to the creation of a dedicated center endowed with its own staff. As it may involve bureaucratic rivalries, one crucial aspect relates to the issue of institutional affiliation. In the present international landscape, some entities are supervised by an inter or supra-ministerial body, while others are hosted within a particular ministry. The nature of the link (executive powers or merely a secretariat role) also varies. It is possible, however, to discern a number of features which are key to the success of a good network:

9. *Reuters Institute Digital News Report 2018*, p. 9.

10. *Counter-Propaganda: A Basic Analysis. Extracts from a lecture on counter-propaganda given by the Head of Information Research Department in a secret series of lectures on Communism*, SECRET (18674), no. PR 89/45 G, TNA FCO 141/7460, September 1952, on psywar.org, 30 April 2012.

11. Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008.

a) durability: structures that are permanent and that have clearly defined competencies and goals work better than *ad hoc* initiatives that often tend to dilute responsibility;[12]

b) variable geometry: the existing networks are usually made up of a security-leaning "core" (Foreign Affairs, Defense, Interior, Intelligence) who meet up on a regular basis and, depending on the agenda, involve other relevant ministries (Education, Culture, Justice), or even members of parliament and civil society actors;

c) a wide focus: networks usually make public that they are fighting information manipulation *in general*, even though they are often, in reality, focused on Russia. In theory, they are also capable of dealing with other state actors (China, Iran, etc.) as well as non-state ones (jihadist groups). Indeed a number of networks are working on establishing bridges between the fight against information manipulation and the fight against radicalization;

d) set-up: successful networks bring together a small number of people who are well-versed in digital matters and who know and trust one another. When the group is too large or too hierarchically heterogeneous, discussions tend to diminish in quality and efficiency. The interdisciplinary team should also include information system experts who tend to be confined to crisis resolution while they should in fact take part in the strategic thinking. Finally, the groups that work well are those that comprise at least a handful of permanent members who work full time on the subject;

e) production: in addition to meeting and the sharing of information, the best networks are productive. Three types of internal publications could be devised: warning notes, periodic reviews and thematic reports. The entity in question could also manage the publication of an annual report on information manipulation (some intelligence services—such as the Estonian KAPO—and even some armed forces—in Lithuania—already do this);

f) communication: given the crucial role played by transparency in dispelling conspiracy theories, these networks are public and sometimes engage in external communication. In those countries that are most exposed to foreign pressure, in Eastern and Central Europe and, more particularly, in the Baltic States, the role of the security and military forces is emphasized. In contrast, other countries prefer to highlight the work

12. Veronika Vichova and Jakub Janda (eds.), *The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, European Values, Kremlin Watch Report, 30 April 2018, p. 3 and 28.

of institutions closer to civil society so as to reassure their populations. In Canada, the brunt of responsibility in the fight against disinformation falls unto the Ministry of Democratic Institutions—insofar as information manipulation threatens elections, and thus the integrity of democratic processes.

Notwithstanding the institutional affiliation of the dedicated entity, the Ministry of Foreign Affairs has an important role to play in monitoring and providing early warning, especially in instances of malign campaigns targeting national interests abroad. Diplomatic networks can be effectively mobilized to warn about coalescing campaigns (antennas) as well as to propagate the Ministry's strategic communication (loudspeaker).

10. Scan the web to identify the communities that propagate the stories. It is difficult to anticipate threats. Nevertheless, they can be detected and the goal is to do so as early as possible. To achieve this, probing antennas must be extended into "risk communities" (extremist, conspiratorial and religious groups). These probes can be passive accounts, which only listen, or active ones, which take part in discussions. There are a number of technical solutions to monitor social networks (DigiMind, AmiSoftware, Linkfluence, etc.).

Official responses (websites, pages, accounts) have only limited efficacy. Clandestine operations, aiming for instance at manipulating the manipulators, are risky because, if exposed (and it is becoming increasingly difficult to prevent this in the long-run), they can jeopardize the very credibility of the source and invigorate conspiratorial actors—which would end up strengthening the very actors one aimed at undermining. What should therefore be done?

The first step is to survey the web in order to better grasp the communities that propagate false information on the social networks: identify the main actors (which can mean different things: those with the largest following, the most active ones, the most quoted, etc.), ascertain the type of community in question—its structure (is it centralized, hierarchical, horizontal, tribal, etc.?) and its spirit (is it cooperative or competitive? This distinction is important because in a competitive community, within which members compete for the recognition of others, the withdrawal of a key member will have little effect as he or she will simply be replaced by somebody else). Such painstaking work is essential in order to understand the channels of propagation, but also to enable anticipation and adequate action.

It is then possible to a) identify accounts that are the source of manipulations and, conversely, like-minded or at least more neutral and rational accounts that enjoy a significant audience; b) neutralize the former (cyberattacks, suspension) and support the latter (e.g. by offering them training); c) disclose the manipulation attempt, name its source (naming and shaming) and discredit the content of the fake news story—either directly, in an official manner, or indirectly, via like-minded accounts.

11. Communicate better. We will lose the information war if we only respond and react. In order to win this war, it is not only necessary to ensure a continuous presence on the web, to have a communication strategy, disseminate targeted messages, and be able to refute false information. It is equally important to be proactive by drawing the adversary out of their comfort zone. For example, whenever government services detect trolls or dormant bots, they should be exposed publicly before they are even used.

When under attack, communication is key. Defense personnel can tend to classify—rather than use—information. It is possible to condemn an attack without revealing its source and then leave it to the media to do their work. This was one of the reasons for the En Marche! campaign's successful response to the interference attempt during the French presidential election. This was also the approach the Germans adopted during their pre-electoral period. Proactive communication is now widely recognized as the strategy to follow.

For States who do not have English as their official language, it is also important to communicate information in English about their doctrine, national strategy and experience.

12. Legislate when required. States must be able to implement the following measures when necessary:

a) adopt a law against "fake news" if there is none, or adapt the existing legislation to meet the challenges of the digital era;

b) penalize more strictly the wrongdoings of the media, by following the example of the British Ofcom (which sanctioned RT on several occasions with some success, i.e. a dissuasive effect) and reinforce legislation which punishes online harassment, in particular towards journalists;

c) consider making registration compulsory for foreign media, by following the American example, which would not affect the circulation of these media (and would thereby not constitute censorship) but would

simply provide a transparency tool. The public has a right to know who speaks, similar to the logic that prevails in matters of food safety—the traceability of information must be a measure of its quality.

Develop our legal system

"I have decided that we would make changes to our legal system so as to protect democratic life from fake news. A law will soon be proposed on this issue. During the electoral period, […] platforms will be required to meet obligations of increased transparency regarding all sponsored content so as to make public the identity of advertisers and those who control them. Platforms will also have to limit the sums devoted to such content. […] In the event of the propagation of fake news, it will be possible to take legal action which, if necessary, will include deleting the content in question, dereferencing the website, closing the user account in question and even blocking access to the website. The regulating powers, which will be thoroughly reshaped in 2018, will be increased to manage attempts at destabilization by television services controlled or influenced by foreign States. This will allow the reworked CSA [*French media regulatory authority*], in particular, to refuse to conclude agreements with such services by assessing the content published by said services, including on the internet. It will also enable the regulator, in the event of an act likely to affect the outcome of the ballot—whether in the pre-election or election period—to suspend or cancel an agreement. […] This new mechanism will involve a duty of intervention on the part of intermediaries to quickly remove any illicit content brought to their attention."

(Emmanuel Macron, President of France, New Year's Address to the Press, 4 January 2018.)

We must nevertheless be careful to not overregulate. In other words, we must preserve the equilibrium between protecting the population and respecting civil liberties, which are the foundations of our liberal democracies. Overregulation is a real danger, and even a trap set by our adversaries: far from being bothered with overzealous regulations, they will actually benefit from the controversy and divisions that it will create. We must be mindful of the risk of our actions having such unintended effects.

13. Conduct parliamentary inquiries. The American and British examples show that public inquiries offer many benefits in terms of raising citizens' awareness, accumulating knowledge, and providing deterrence.

14. Hold digital platforms accountable. The role of social networks in information manipulation is now widely recognized. They have become the principal source of information, and hence of disinformation, for a majority of the population. Although information manipulation is costly for their reputation and despite the self-regulation pledges these platforms have made in recent times, it is unclear whether digital platforms actually want to curb these practices. It is our responsibility to find the right levers with which to compel them, at the European level, to:

a) make the sources of their advertising public—by demanding the same level of transparency as is required of traditional media;

b) implement adequate measures with which to fight information manipulation on their websites and contribute to the improvement of media literacy and the awareness of the general public of these issues.

It is up to legislators to strike the right balance between freedom of expression and the need for a greater accountability when it comes to digital platforms in the fight against information manipulation.

15. Share information with digital platforms. We cannot, on the one hand, wait for digital platforms to do more in the fight against information manipulation while, on the other hand, not providing them with information that is sometimes necessary for them to move forward. Public-private cooperation is of capital importance and demands knowledge-sharing in both directions. This is one of the recommendations made to the Trump administration by two former senior officials of the Obama administration, in the context of the midterm elections of 2018.[13]

16. Go international. In recent years, the issue of information manipulation has been raised primarily by the same group of States on the international stage: Central, Eastern, and Northern European States alongside the U.K. and the United States. France and Spain are in the process of stepping up their international presence because they too have been the target of attacks. Other States should not wait to be attacked; they should become more active now. This implies:

a) increasing their participation in existing initiatives: send an expert to EU institutions, as a priority the East StratCom Task Force; contribute to the work of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE); take part in important annual meetings (StratCom

13. Joshua A. Geltzer and Dipayan Ghosh, "How Washington Can Prevent Midterm Election Interference," *Foreign Affairs*, 25 July 2018.

Summit in Prague, Riga StratCom Dialogue, the Atlantic Council's StratCom in Washington DC);

b) increase meetings between regional communities. The Euro-Atlantic scene dominates but it is not the only one: there are many interesting developments in Asia, with Singapore being increasingly seen as a point of reference. Not only are authorities proactive and outward-looking, as is demonstrated by the parliamentary hearings and the fact that the Ministry of Defense will soon be sending a resident expert to the NATO Excellence Center in Riga, but so too has civil society been actively involved. The Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS) organizes an annual seminar on disinformation which is one of the very rare meeting points between research and practitioner communities from Europe, North America, Asia and Africa. This diversity is quite refreshing for those accustomed to the Euro-Atlantic scene, which tends to only view the subject through the Russian lens. Each situation is, of course, unique (information manipulation in India, Burma or Indonesia are concerning but endogenous, and thus far removed from the Russian interferences in Europe and North America), but as China presents itself as an ever-increasing threat in the region, such as the Australian case illustrates, there are interesting parallels with Russia to be explored, including to find out what these two countries are learning from each other.

c) innovate through the creation of new mechanisms. Information manipulation often has an inherently international scope. For this reason, coordination is critical. An international early warning mechanism could be established, connecting all of the networks, centers and agencies of the EU and NATO Member States. It might not be necessary to create a new network: from the EU's East StratCom Task Force to the Helsinki and Riga Excellence Centers, there are already various valuable hubs and interfaces for national teams.

Some groups, mostly in the United States, have suggested the creation of an international coalition. In their January 2018 report, Democratic U.S. Senators recommended the creation of "an international coalition against hybrid threats," which would be spearheaded by the United States. They urged the American President to convene an annual world summit on hybrid threats, modelled on the summits of the Global Coalition against Daesh or against violent extremism, which have been

held annually since 2015. Representatives from civil society and private actors would be invited to take part.[14]

Two months later, Fried and Polyakova made a similar suggestion: the creation of a "counter-disinformation coalition" by "the United States and Europe," "a public-private group bringing together on a regular basis like-minded national government and nongovernmental stakeholders, including social media companies, traditional media, ISP firms, and civil society."[15] The idea of creating a network involving nongovernmental actors is excellent. However, articulated in these terms, it appears problematic, not just because it excludes Canada, but because such a transatlantic alliance already exists (NATO) and also because it would require an explanation to Moscow. Moscow will certainly ask to join or why it cannot be part of this "coalition of the willing." The coalition would run the risk of looking like an anti-Russian—rather than an anti-disinformation—alliance. Existing structures, within the EU or NATO, are less susceptible to such criticism.

In May 2018, former U.S. Vice President Joe Biden, former Secretary of Homeland Security Michael Chertoff and former NATO Secretary General Anders Fogh Rasmussen created a transatlantic "Commission on Election Integrity." This Commission is a new actor worth watching, even though it is too soon to assess the role it will play.

Finally, the G7 offers an obvious platform from which to share best practices and formulate common approaches to countering information manipulation. Canada made the issue one of the priorities of its Presidency of the G7 in 2018, by proposing various mechanisms for exchanges and joint action. France, which will take over the G7 Presidency in 2019, should build on these initial results in order to carry out the joint efforts begun within this forum, which are predicated on the preservation and defense of democracy.

17. Train adults as well as children (media literacy and critical thinking). The promotion of media literacy in schools stands as one of the most widely agreed-upon recommendations, despite its unequal application by governments, as can be demonstrated by the Open Society

14. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 5.

15. Daniel Fried and Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council, 2018, p. 13-14.

Institute country ranking.[16] However, if we strictly limit ourselves to media-literacy obtained through schooling, as is often the case, it is a long term measure whose effects will only be visible once the children reach adulthood. It is important to consider media literacy and, more broadly, the development of critical thinking, for the whole population, at all stages of life. The education of teenagers and students is particularly important because they tend to be the most vulnerable to information manipulation for a variety of reasons (lack of experience, the need to assert independence, socio-cultural environment) and they have not necessarily benefited from media literacy training in their early years. Offering a core curriculum first-year course in university (text and image analysis, identification of sources) would be useful and easy to implement, at least in social sciences programs.

The idea is to ensure that any person faced with a piece of information can assess its validity (arguments, evidence) and its source (reliability, motivations). This is a public hygiene measure—just as people in the 19th century learned to wash their hands. One possibility would be to follow the Swedish model and publish a "digital hygiene guide" for use by politicians and political parties.

In other words, it is crucial to educate the general public from a very early age but also at different stages of life, about image, audiovisual media, critical thinking and rational argumentation. The assessment of information is a skill that can be learned. Courses in critical thinking and rational argumentation are widely available in some countries and even considered an indispensable prerequisite in university. These courses teach students how to recognize a paralogism or a sophism and to detect fallacious reasoning. Such measures of "intellectual self-defense" must be developed.[17]

a) Generally speaking, the actions implemented have been hampered by at least two factors: teachers are inadequately trained, and they do not have enough time at their disposal to include this activity in the program. Governments must be mindful of this situation and seek to resolve it.

b) Part of this education must include making people mindful of the mechanisms that exist (trolls, bots, deep fake, etc.). In school, children should be taught how to construct as well as deconstruct false information and conspiracy theories. This would enable them to break down and

16. Open Society Institute (Sofia), *Media Literacy Index 2018*. See Marin Lessenki, *Common Sense Wanted: Resilience to 'Post-Truth' and its Predictors in the New Media Literacy Index 2018*, March 2018.

17. Normand Baillargeon, *Petit Cours d'autodéfense intellectuelle*, Montréal, Lux, 2005.

relativize them. (If they can construct a false information themselves, they will then understand that adults can arguably do it even better.) Children should also learn to use Google image so as to verify the source of any given image. They should also learn not only how to decode/interpret but also how to engage in debate and particularly online debate, through workshops, simulations, etc.

c) Media literacy must include a technological dimension so that young people can understand the operation of social network algorithms (personalization, filter bubbles). It is undoubtedly a challenge to explain such workings to children when even adults struggle to understand them.

d) Go beyond the classroom: to improve its effectiveness, education on information verification should be communicated through a range of media, including television, which after all continues to reach the youngest members of the public. There could be awareness-raising messages played before YouTube videos or sent by digital platforms as private messages, e.g. on Snapchat or Instagram.

e) It is possible to reach out to adults through public campaigns around particular events or through training programs. In that regard, the activities of the NGO Baltic Centre for Media Excellence, which trains journalists and teachers across the region, provide an interesting example. In public service and, in particular, in the Ministries and services most concerned, it is crucial to train staff members so as to reinforce overall "digital hygiene" and develop an internal expertise enabling them to act in an autonomous manner. This involves new recruitment criteria as well as a new range of training programs, public-private partnerships and mobility programs enabling civil servants to acquire new skills from innovative companies. Institutions similar to the French Institute for Higher National Defence Studies (IHEDN) could offer training sessions dedicated to informational threats.

f) The recreational aspect is important, because information manipulation is often entertaining and responses to it are likely to miss their target if they appear too boring (see recommendation n°20). In this way, games, such as the ones developed for Facebook by the NATO Strategic Communications Centre of Excellence, can be quite effective at garnering the interest of young and old alike.[18] Yet another example of this is the Buzzfeed media and news compagny, which produces a highly successful weekly "Fake News Quiz."

18. "The News Hero" (https://apps.facebook.com/thenewshero).

18. Develop research. Our immune system against information infection is not only grounded in a capacity to monitor and analyze the information space—which requires us to allocate more intelligence resources to these activities—but also in an ability to comprehend those who manipulate information and, above all, Russia. Therefore, it is necessary to support research on Russia and the post-Soviet sphere at large. This does not mean reviving "sovietology," but acknowledging that it is possible to respond adequately only to that which we understand well.

In concrete terms, this means that States must increase research funding and introduce calls for tenders aimed at studies on predetermined topics or even fund PhDs and/or postdoctoral research projects as well as events (symposiums) and publications on the subject. The connection to information manipulation can either be direct (when it is the topic of research), or indirect, as it can be useful to support sub-projects in the information field, in social psychology or in political science—adding yet another piece to the puzzle.

19. Marginalize foreign propaganda organizations. Firstly, it is necessary to call out these organs for what they are. This is what the French President did in front of Vladimir Putin at Versailles, in the wake of his election, in a public statement which attracted international attention:

> Russia Today and Sputnik have been organs of influence during this campaign that have, on several occasions, produced untruthfull statements about myself and my campaign […] It is a matter of serious concern that we have foreign news organizations—under whatever influence, I do not know—interfering in a democratic campaign by spreading serious lies. And on this issue, I will yield no ground, no ground whatsoever […] Russia Today and Sputnik did not act as news organizations and journalists, they acted as organs of influence and propaganda, and of lying propaganda, no more, no less.[19]

Consequences ought to be drawn, by not accrediting or inviting organs of influence to press conferences reserved to journalists.

19. Emmanuel Macron during a joint press conference with President Vladimir Putin at Versailles, 29 May 2017.

20. Use humor. Counter-measures are often criticized for not being entertaining and, for this reason, missing their target audience. On the other hand, stories involving false information are usually amusing. Many people consume fake news like they would junk food: knowing full-well that it is bad for them, but giving in to the pleasure. RT and Sputnik practice "infotainment," a combination of information and entertainment, compared to which corrective measures can appear very stern. Yet experience in Europe and North America tells us that humor, satire, jokes and mockery work remarkably well against information manipulation. This is something civil society understands: there are a range of satirical programs ("Derzites tam!" in Lithuania), satirical prizes (the "Putin's Champion Award" of the European Values think tank), as well as numerous satirical accounts on social networks (Darth Putin on Twitter, who provides such advice as "Do not believe *anything* until the Kremlin denies it"), etc. The EU's task force also uses humor on its website EUvsDisinfo and on social networks. Therefore, even though this veers from their usual pitch, States should consider communicating through humor in some circumstances (Sweden does an excellent job of myth-busting certain clichés on its website Sweden.ru, for example).

21. Be aware of your own vulnerabilities. Information manipulation exploits the vulnerabilities of our democratic societies. For this reason, it is necessary to map out, locate and understand these vulnerabilities in order to anticipate and try to prevent hostile actions. The ability to put ourselves in the shoes of the adversary is, therefore, essential in order to better predict their next moves. To this end, we must not only study then by research and intelligence but also test our procedures through "red teams," i.e. teams that play the part of the opponent by trying to identify and manipulate our weaknesses.

22. Remember what we are fighting for. Information manipulation tries to systematically instill doubt in the values and principles of the communities it targets. The best way to combat these manipulation attempts are, firstly, to have a clear idea of what we wish to protect.

23. Acknowledge the unavoidable reversal and diversion of our counter-measures. It is important to recognize that our counter-measures will, in turn, be manipulated by the enemy. Sometimes there will be a mirror effect (RT has its own FakeCheck in four languages, the

Russian Ministry of Foreign Affairs' website launched a section entitled "Published materials that contain false information about Russia" in February 2017, etc.). Sometimes the counter-measures will be distorted by the enemy or third States (illiberal forces taking advantage of the situation to push restrictive laws). Therefore, it is necessary to encourage positive approaches that promote the free circulation of high quality information, in contrast to the fragmentation that currently dominates the internet.

24. Pay attention to weak signals beyond the Russian prism (other States, non-state actors) as well as those working against our interests outside of Europe (notably in Africa and in the Middle East).

25. Listen to civil society, especially journalists. Establishing a regular and open dialogue between journalists and policymakers can help to fight against information manipulation. In Sweden, a Media Council meets on a regular basis, bringing together media leaders and politicians to identify the challenges they face and, crucially, to coordinate their fact-checking efforts.[20] The Belgian group of experts recommends creating a "discussion forum" joining all the actors involved ("universities, the media, journalists and journalism schools, NGOs, digital platforms").[21] This excellent idea—which would nevertheless be easier to implement in smaller countries, where the actors are less numerous—would also provide the State with a point of contact, allowing them to regularly consult this discussion platform.

26. Keep other forms of influence in check. Information manipulation is but one element in a complex system; it feeds off of other forms of influence. In the case of Russia, targeted States should reduce their energy dependence on Russia as well as target corruption and the Russian financial circuits that contribute to the funding of influence operations.

27. In external operations, nurture relationships with the local population. It is important to never forget that "every action projects an image, generates a perception for the adversary, for local populations

20. Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Carnegie Endowment for International Peace, May 23 2018.

21. Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, *op. cit.*, p. 12.

but also today with domestic and international audiences. Troops deployed in an external military operation are therefore the first actors of influence, and their actions are not strictly non-lethal."[22] In the context of NATO's Enhanced Forward Presence in Baltic countries, American soldiers in Latvia have performed practical services for the Russian-speaking communities (such as chopping wood), which has enhanced their popularity and contributed to undermining anti-American propaganda circulated by Russian media among those communities.[23]

28. Punish those responsible for serious interference, during, for example, an electoral process and if responsibility can be clearly assigned, through economic sanctions or legal proceedings (American Special Prosecutor Robert Mueller indicted 13 Russians and three Russian entities in February 2018, along with 12 officers of the GRU in July 2018).

III. Recommendations for civil society

29. Understand and reinforce digital confidence-building measures. Information manipulation is both a cause and a symptom of the crisis of confidence in the digital arena. Effectively fighting against these manipulations will have the end result of increasing confidence. At the same time, this first requires having an understanding of the psychological mechanisms that underpin trust, by placing oneself in the users' position, and promoting good practices that will build trust. In this way, it would be useful to seek enhanced cooperation which would allow the establishment of reliability indices for online content.

30. Enhance fact-checking while remaining aware of its limitations. As most people tend not to accept the correction (and this tendency is even more pronounced if the correct information challenges deeply-held beliefs), fact-checking can be effective on a given individual provided that two conditions are met: firstly, the correction must not directly undercut one's vision of the world (otherwise it can even have the perverse effect of reinforcing the person's primary beliefs—this was observed in the case of Iraq's weapons of mass destruction, and discussions on climate change

22. Bertrand Boyer, "Les opérations sur l'environnement : la nouvelle guerre de l'information," in Stéphane Taillat, Amaël Cattaruzza and Didier Danet (eds.), *La Cyberdéfense. Politique de l'espace numérique*, *op. cit.*, p. 212.

23. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 89.

and vaccination). Secondly, the correction must entail an explanation of why and how disinformation was spread.[24]

31. Develop simple tools allowing citizens to expose information manipulation attempts themselves, such as knowing who is responsible for a particular advertisement (whotargets.me) or detecting trafficked videos (such as the AFP's project InVID).

32. Develop normative initiatives (rankings, indexes, labels, etc.) while recognizing that a proliferation of competing norms and standards will only weaken the overall effort. Therefore, the objective should be to put forward a small number of tools of reference, possibly in connection with reputable NGOs. The Reporters Without Borders (RSF) initiative is, in this respect, very promising.

33. Adopt an international charter of journalistic ethics, in a collaborative manner (by involving both major traditional and online media). The majority of major media platforms have charters of good editorial practices and ethics.[25] The 1971 Munich Charter can provide a useful foundation, but it needs to be adapted to the contemporary media landscape and, notably, the rise of digital media.

34. Train journalists to better understand the risks of information manipulation, in journalism schools and throughout their careers. How should one cover a massive leak, detect a fake profile or react to extremist content? There are concrete answers to these questions,[26] which may serve as a basis for teaching material.

35. Build confidence in journalism by enhancing transparency. The Trust Project,[27] a consortium that brings together news companies such as *The Economist*, *The Globe and Mail, La Repubblica* or *The Washington Post*, recommends revealing sources of funding (similarly, *The Conversation* also requires researchers who publish on their website to disclose any potential conflicts of interest, a common practice in scientific journals),

24. Stephan Lewandowsky, Ullrich Ecker and John Cook, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," *op. cit.*, p. 355.

25. See, for example, the AFP's Charter from 22 June 2016.

26. See for example Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," Alliance for Securing Democracy (GMF) Brief 2018 No. 009, March 2018, p. 4.

27. Thetrustproject.org

the profiles of the journalists, proof of their expertise on the subject matter, providing clear a distinction between an opinion, an analysis, or sponsored content, how the sources were accessed, why the journalist chose a particular hypothesis over another, etc. The idea is that the readers want to know how journalists work, and how they know what they know. This transparency in terms of practices, methods, and journalistic procedures can help to build trust.

36. Develop tools with which to counter "trolling," such as Perspective by Jigsaw, which uses machine-learning and self-learning as tools to identify toxic messages that can then be isolated, stopped before publication and then submitted to moderators. *The New York Times* and other major papers use such tools on their websites. Another method consists of the publication of lists of accounts identified as trolls.

37. Use artificial intelligence and automatic language processing tools in the detection of manipulation attempts and fact-checking. The profusion of fake or biased news is such that journalists, analysts and researchers together will never be numerous enough to spot and deal with all of the threats. Detection software, such as Storyzy, are continuously multiplying and being perfected. With respect to fact-checking, certain software can automatically compare the suspicious news story with all others that were already "debunked" so as to avoid repeating the same work for nothing. This assumes that there is shared access to databases—hence the need for verification networks. Automated verification saves time, but nevertheless still requires, for the time being, a human at the end of the process to validate its results.

38. Develop surveys and polls aimed at assessing public sensitivity to information manipulation. Collecting precise data on a regular basis would improve the effectiveness of counter-measures.

39. Enhance pluralism through tools promoting information diversity, in order to combat the phenomenon of "filter bubbles:" several projects, including Ghent University's "NewsDNA," allow citizens to adjust the degree of diversity in the news that they consume.[28]

28. Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, *op. cit.*, p. 9.

40. Rethink the economic model behind journalism, so as to reconcile the preservation of freedom of expression, free market competition and the fight against information manipulation.

41. Incite researchers to intervene in public debates. Pseudo-science proliferates because it occupies a space that is too often left vacant by actual scientists: in particular the dissemination of scientific knowledge (popular science). There are far too many researchers who neglect this activity, by considering the media exposure to be unethical and a hindrance to their career. However, in the context of this ambiguity and confusion, the social responsibility of academics was never greater: they are obliged to provide non-specialists access to the results of their research and to insert themselves in the public debate. In line with this exercise of disseminating research, higher education institutions must also organize media training courses, to teach the specific skills needed to best interact with the media. Moreover, the dissemination of research must be increasingly valorized in the career, as well as constitute a major criterion for evaluation, in order to incite academics to practice this exercise.

IV. Recommendations for private actors

42. Rethink the status of digital platforms: take platforms at their word and exercise decisive political pressure to compel them to ensure, through strict codes of conduct, that their asserted missions are indeed reflected at the operational level (algorithms, the role of moderators, policing of networks, etc.). In addition, it is necessary to come up with a hybrid status—something between media and host—that enables us to take into account the public service mission that digital platforms have *de facto* come to assume (digital agora). The possibility of an anti-trust regulation proposed by the European Commission expert group (see above) also deserves consideration.

43. Demand the establishment of a new contract with users that is founded on new digital rights. The terms of reference must be reassessed so as to make them intelligible to all and more explicit as regards issues of access to and management of personal data. It is critical that internet users reclaim control over the future use of their data (an opt-in system could be devised, a fee-paying service performing one or

several of the following functions: data confidentiality, advertisement blocking, traceability of personal data).

44. Impose a high level of transparency. In the aftermath of the Cambridge Analytica scandal, wishful appeals for more transparency are no longer good enough. Internet users must be informed of the campaigns that can affect them and the reasons for such targeting. Given the challenge this poses for democratic life, political advertising connected to the exploitation of big data must be subjected to specific regulation. In this context, the possibility has been raised of establishing a public mediator who would be granted access to algorithms under the condition of strict confidentiality.

45. Increase the cost of information manipulation while ensuring the protection of vulnerable individuals and movements. More systematic action must be undertaken against the agents of manipulation, drawing on the concept of "threat actor," a term that comes from the field of cybersecurity. (This concept allows for the identification of chains of command and infrastructures that are shared between various operations. Rather than censoring contentious content one by one [a "whack-a-mole approach"], platforms could conduct inquiries that lead to the identification of a hostile actor and then suppress all of those actor's online outlets. We might follow the model set by the deletion of all Facebook pages linked to the IRA.) Whistle-blowers and organizations that are targeted by an information manipulation campaign must, on the other hand, be warned in advance through a special detection system. They must also benefit from protective procedures (hotline) that will enable them to defend themselves.

46. Enhance and better remunerate quality journalism: the current system is unsustainable. Digital platforms have appropriated the bulk of the advertising revenue, which used to be allocated to the funding of traditional media. These platforms have also capitalized on these media's primary content without remunerating them. It is important to think about new methods of redistribution of information from digital platforms to quality media.

47. Require platforms to contribute to the funding of quality journalism, by requiring them to provide funding for fact-checking, for example.

48. Require platforms to contribute to the funding of independent research: experts agree on the need to access platforms' data in order to measure the impact of information manipulation campaigns, understand how the information goes viral and assess the effectiveness of measures aimed at countering false information. Platforms must contribute to the funding of this research effort without trying to impose any hidden conditionality as regards the orientation of this research or the political positions of researchers.

49. Consider the creation of "safe zones": given the present situation of information asymmetry, the challenge online disinformation poses to democracies cannot be met without the cooperation of digital platforms. This requires us creating the conditions for a constructive dialogue. It is, therefore, necessary to devise new forums in which platforms' intellectual property rights would be guaranteed, in exchange for easier access to their data, software and algorithms. These new spaces should foster cooperation between researchers, civil society and digital platforms. This entails, particularly in the wake of the Cambridge Analytica scandal, the establishment of a preliminary framework for ethical research based on the model by which doctors access their patients' medical files.

50. Explore redirection methods so as to ensure that those who seek fake news also come across debunking. Google Redirect, for example, is thought to have efficiently curbed the attraction of ISIS by identifying potential recruits (thanks to their search history) and by exposing them to YouTube videos that demystify ISIS. The idea is to apply such methods to other cases of information manipulation.[29]

V. Responding to objections

In many countries, responses to information manipulation raise concerns—sometimes sincere and other times feigned and calculated. In all cases, however, these responses are legitimate objects of democratic debate. In the following pages, we list the principal criticisms and provide some answers to these objections.

29. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 77.

The critique of responses to information manipulation can be categorized along four lines: 1) the issue is irrelevant, the real problem lies elsewhere; 2) the proposed solutions are not efficient; 3) these solutions are counterproductive, and even dangerous; 4) other arguments of a more polemical, yet nonetheless common sort.

A. An irrelevant cause?

"Nothing new under the sun": the political use of information is an age-old practice. What is happening today is nothing new when compared to the Cold War period.

→ The current situation presents at least three fundamental differences in comparison with the past and, in particular, the Cold War years:

- social networks ramp up the effects of information manipulation (speed of propagation, scale and diversity of audiences reached; high impact for very low costs);
- the objective today is no longer the defense of a particular ideology or system (the USSR) but the denigration of the West and the polarization of societies;
- non-state actors play a crucial role in the present phase: they interact with one another and with States in a manner that is at once more systematic and more diluted (see Vladimir Putin's statements on the "Russian patriots" online).

The role of disinformation in recent crises (Brexit, American elections) has been overstated. There is no conclusive research demonstrating that fake news has a direct and tangible impact on internet users. Conversely, by responding to disinformation in a conspicuous manner, we risk granting the stories undue importance.

→ Recent experience has demonstrated, on the contrary, that it is important to not underestimate the seriousness of information manipulation. The Lisa Case has had very real consequences on the rise of anti-migrant sentiment in Germany and such effects are often irreversible, despite later efforts to restore the truth.

The Obama Administration chose, for a variety of reasons, not to alert the public to the information manipulation campaign targeting the country, thereby easing the course of an ongoing democratic destabilization effort. On the other hand, the German Chancellor referred publicly to the manipulation threats in the wake of the 2015 attack on the Bundestag. It

was the latter model that France followed during the "Macron Leaks" and is a model that has proven itself effective.

Digital platforms are the ideal scapegoats to blame for the evils of society. However, technology is neutral, these platforms are nothing but spaces without preferences within which internet users can express themselves freely.

→ To use the words of the whistleblower who revealed the Cambridge Analytica scandal: "the knife may be neutral, but it can be used to cook —or to kill somebody." This very neutrality requires strong principles and clear rules to prevent it from being diverted towards malicious goals or from serving projects that are hostile to our democracies and our citizens' welfare. It is high time that platforms take responsibility and that governments draw all the lessons from this type of scandals.

B. Ineffective solutions?

The proposed solutions (media literacy, promotion of quality content) will only impact those who are already convinced and will have no impact on those audiences who are most exposed to disinformation (conspiracy theorists, radical groups, etc.).

→ Contemporary information manipulation campaigns succeed in sowing seeds of doubt in a variety of audiences—not just conspiracy theorists, alternative and radical communities. Measures that support media literacy, fact-checking and quality journalism reinforce the resilience and immunity of the wider public to manipulation threats. We are conscious of the fact that the most radical or pro-conspiracy theory segments of public opinion will not be convinced, but they are a minority and must remain so.

Counter-productive effects: projects (such as RSF's) aimed at ranking and indexing reliable sources of information may backfire: public distrust of "the establishment" might actually encourage many internet users to seek their information from any source except those officially designated as reliable.

→ In the current state of information chaos, it is essential for the public to have at their disposal objective references with which to assess the reliability of information sources. Initiatives led by non-governmental and independent organizations such as RSF, that seek to create consensus

within the profession on objective criteria for quality journalism (working methods, cross-checking information, error correction procedures, media governance, etc.) are very valuable in this context. In order to avoid counter-productive effects, ranking and labeling schemes must offer guarantees of the transparency of the process, the quality of the criteria, and demonstrate the inclusivity and diversity of those assessing these criteria.

The diversion argument: the topic of information manipulation makes the media headlines and thus diverts attention from more substantive topics, in particular the concentration of media ownership in the hands of private interests.

→ Giving due consideration to the grave issues raised by information manipulation does not entail turning a blind eye to the other dimensions of an apparently profound crisis of political communication in the 21st century. The French President, in his New Year's address to the press, on 4 January 2018, referenced the issue of conflicts of interest between shareholders and editorial boards and suggested some possible courses of action by which to guarantee the full editorial independence of the media.

C. A threat to liberties?

The threat to freedom argument: beneath the cover of the fight against fake news, we are witnessing a reassertion of state control over the field of information, which threatens our freedom of expression. In Egypt, the regime ordered the closure of 21 information websites under the accusation of spreading fake news. Among these censored sites was MadaMisr, an independent, progressive newspaper who had voiced opposition towards the current regime.[30] *The cure is therefore worse than the disease.*

→ In France, the parliamentary bill against information manipulation currently under consideration offers many guarantees. Its provisions are time-limited, applying only to electoral campaigns. The bill also relies on a reinforcement of the powers of the ordinary judge, the guardian of liberty, and the powers of the CSA, the independent public authority responsible for ensuring freedom of audiovisual expression. The fundamental goal of this legislative proposal is simply to protect the honesty and integrity of the ballot, so that it faithfully reflects the popular will. It is not, therefore, about creating a "Ministry of Truth."

30. Tourya Guaaybess, "*Fake news :* de l'instrumentalisation d'un terme à la mode ou les nouveaux visages du 'Schmilblick'," *The Conversation*, 11 February 2018.

→ Media and civil society actors are involved in the new legislation's drafting process, which acts as a guarantee that the State will not infringe upon civil liberties in the process of fighting information manipulation.

The boomerang effect: the denunciation of fake news hurts journalists themselves. The fake news anathema has become a convenient tool with which dictators and illiberal regimes justify censorship.

→ This is a real risk and one that we take very seriously. We made a conscious decision to respond to information manipulation in a transparent and democratic manner, by cooperating with civil society and the media. Grounded as it is in the rule of law and in the values of open societies, our response is by nature more difficult to flip around in an authoritarian setting. In tackling information manipulation, we turn (as described above) either to the ordinary judge, who is the guardian of liberty, or to the CSA, an independent regulation authority whose mission is to protect freedom of audiovisual expression. France will remain vigilant, at every stage of the response, to ensure that the potential risks to civil liberties in an illiberal/authoritarian context are duly taken into account. Standing alongside the Swedish MSB, "we advocate vigilance, not paranoia."[31]

Concerns regarding the pluralism of information. In our keenness to define "good information" and to promote "quality content," we run the risk of reducing the diversity of sources and of effectively homogenizing them.

→ This is a bogus accusation: the fundamental principles of freedom of expression and opinion as well as our democratic attachment to the pluralism of information remain unchanged. The various initiatives mentioned in this report aim at fostering quality content, not at censoring biased or false content.

D. Polemical arguments

Double standards: you accuse RT and Sputnik of propaganda, yet Al-Jazeera, CNN, the BBC and France 24 do exactly the same thing.

→ We are not talking about propaganda, but about information manipulation. Al-Jazeera, CNN, the BBC or France 24 contribute to the

31. James Pamment *et al.*, *Countering Information Influence Activities*, *op. cit.,* p. 9.

influence of Qatar, the United States, the United Kingdom or France, but these media outlets retain their editorial independence and respect professional journalistic standards. Furthermore, they do not resort to the methods frequently used by RT and Sputnik, such as the fabrication of facts and the falsification of documents, translations and interviews, the use of edited photos, or fake experts. It is these instances of information manipulation, and these alone, that we denounce; not the fact that these outlets have a particular point of view.

The scapegoat argument: you blame Moscow for all of the Western world's evils.

→ Those actors who are behind information manipulation campaigns—and who are oftentimes easily identifiable—are not the source of our societies' evils, but they do amplify them. They deliberately identify the fault-lines intrinsic to each society (religious and linguistic minorities, historical issues, inequality, separatist tendencies, racial tensions, etc.) and then seek to further polarize public opinion around these divisive issues.

→ The fight against information manipulation must also take into account other actors, potential or known, who are likely to undertake information manipulation campaigns.

Your response proves that you take your citizens for fools who are unable to "think correctly."

→ Our approach does not involve any value judgment: our citizens are entirely free to make their own choices and form their own opinions. We are an open and pluralist society, and herein lies our strength. Nevertheless, our duty is to protect our democratic institutions and our national interests from hostile information manipulation as well as to foster the development of programs by civil society and public institutions, enabling citizens and young people, in particular, to fully exercise their critical thinking in the field of information.

You are not innocent: Western nations, and France in particular, did not hesitate to resort to state propaganda in the colonial context.

→ Like all democracies, France is open to any discussion of its past behavior so long as that discussion is scientifically rigorous. This is the

remit of historians who study and shall continue to study all the chapters of our national history. Today, we are faced with a new, specific challenge, which we must tackle not only by drawing upon the lessons of the past, but also by looking towards the future.

BIBLIOGRAPHY

This list is not exhaustive and is intended as a reference only.

Written sources

AALTOLA Mika, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Aurocratic Meddling*, FIIA Briefing Paper 226, November 2017.

ADEMSKY Dima, *Cross-Domain Coercion*, Institut français des relations internationales, November 2015.

AIELLO Luca Maria *et al.*, "People Are Strange When You're a Stranger: Impact and Influence of Bots on Social Networks," *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* 697, 2012, p. 10-17.

ALAPHILIPPE Alexandre *et al.*, *Disinformation detection system: 2018 Italian elections. Case report,* EU Disinfo Lab, 1 June 2018.

— *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, July 2018.

ALBERT Jean-Marie, *La Désinformation* (Vol. 1 and 2), Triomphe, 2015.

ALLCOTT Hunt and GENTZKOW Matthew, "Social Media and Fake News in the 2016 Election," *Journal of Economic Perspectives*, 31:2, 2017, p. 211-236.

ALLEN T. S. and MOORE A. J., "Victory without casualties: Russia's information operations," *Parameters,* 48:1, Spring 2018.

ARO Jessikka, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View*, 10 May 2016.

ASSOCIATION DES ANCIENS DE L'ÉCOLE DE GUERRE ÉCONOMIQUE, *Désinformation et révolution technologique*, 2006.

AUDINET Maxime, "Soft power russe : l'information au cœur," *in* MONTBRIAL Thierry de and DAVID Dominique (eds.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017.

BADOUARD Romain, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, FYP éditions, 2017.

BAUMARD Philippe, *Le Vide stratégique,* CNRS éd., 2015.

— and col. BENVENUTI J. A., *Compétitivité et systèmes d'information,* InterÉditions, 1998.

BAZZELL Michael, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information,* CreateSpace Independent Publishing Platform, 2016.

BENASAYAG Miguel and AUBENAS Florence, *La Fabrication de l'information,* La Découverte, 2007.

BERNAYS Edward, *Propaganda,* ed. H. Liveright, 1928.

BERTOLIN Giorgio (ed.), *Digital Hydra: Security Implications of False Information Online,* NATO Strategic Communications Centre of Excellence, November 2017.

BLOCH Marc, "Reflections of a Historian on the False News of the War", *Michigan War Studies Review*, 2013-051, translation by James P. Holoka, Eastern Michigan University, 1 July 2013.

BOGHARDT Thomas, "Operation Infektion: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, 53:4, 2009, p. 1-24.

BOYER Bertrand, *Cybertactique : conduire la guerre numérique*, Nuvis, 2014.

—, "Les opérations sur l'environnement : la nouvelle guerre de l'information," *in* TAILLAT Stéphane, CATTARUZZA Amaël and DANET Didier (eds.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 209-218.

BRADSHAW Samantha and HOWARD Philip N., *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Working paper No. 2017.12, University of Oxford, July 2017.

BRATTBERG Erik and MAURER Tim, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," *Carnegie Endowment for International Peace*, 23 May 2018.

BRONNER Gérald, *La Démocratie des crédules*, PUF, 2013.

BULINGE Franck, *Maîtriser l'information stratégique : Méthodes et techniques d'analyse,* De Boeck, 2014.

CADIER David, "L'Europe centrale et la désinformation russe," *in* MONTBRIAL Thierry de and DAVID Dominique (eds.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 172-178.

— and LIGHT Margot (eds.), *Russia's Foreign Policy: Ideas, Domestic Politics and External Relations,* Palgrave Mcmillan, 2015.

CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS), *Who Said What? The Security Challenges of Modern Disinformation*, *World Watch: Expert Notes*, series publication No. 2018-02-01, February 2018.

CENTRE FOR INTERNATIONAL RELATIONS, *Information Warfare in the Internet. Countering Pro-Kremlin Disinformation in the CEE Countries,* June 2017.

CHEKINOV Sergei and BOGDANOV Sergei, "Asymmetrical Actions to Maintain Russia's Military Security," *Military Thought*, Vol. 1, 2010.

CHOMSKY Noam and HERMAN Edward, *Manufacturing Consent, The Political Economy of the Mass Media* (1988), Random House, 2002.

CHOMSKY Noam and MCCHESNEY Robert W., *Propagande, médias et démocratie,* Écosociété, 2005.
CHOMSKY Noam and BARSAMIAN David, *Propaganda and the Public Mind* (2001), Haymarket Books, 2015.
COLLECTIVE, "L'Ère de la désinformation," *Courrier international*, Special issue 63, October 2017.
COMMUNICATIONS SECURITY ESTABLISHMENT, *Cyber Threats to Canada's Democratic Processes,* Government of Canada, 2017.
CONNELL Mary Ellen and EVANS Ryan, "Russia's Ambiguous Warfare and Implications for the U.S. Marine Corps," *MCU Journal*, Vol. 7, 2016.
CONSEIL NATIONAL DU NUMÉRIQUE, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable,* May 2014.
COOK John and LEWANDOWSKY Stephan, *The Debunking Handbook*, University of Queensland, 2012.
CORDIER Anne, *Grandir connectés, les adolescents et la recherche d'information*, C&F éditions, 2015.
CORKER Bob *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, A Minority Staff Report prepared for the use of the Committee on Foreign Relations, United States Senate, 10 January 2018.
CRAWFORD Krysten, "Stanford study examines fake news and the 2016 presidential election," *Stanford News*, 2017.
D'ALMEIDA Fabrice, *La Manipulation* (4th ed.), PUF, "Que sais-je," 2017.
DAMARAD Volha and YELISEYEU Andrei, *Disinformation Resilience in Central and Eastern Europe*, Disinformation Resilience Index (DRI), 2018.
D'ANCONA Matthew, *Post-Truth: The New War on Truth and How to Fight Back,* Ebury Press, 2017.
DARCZEWSKA Jolanta, "The Devil is in the Details. Information Warfare in the light of Russia's Military Doctrine," *Point of View*, 50, OSW (Centre for Eastern Studies), May 2015.
DARNTON Robert, "The True History of Fake News," *The New York Review of Books*, 13 February 2017.
DEPREZ Fabrice, *"Fact-Checking" et "vérification," quel rôle et quels outils pour le veilleur ?,* Netsources, 2015.
DIEGUEZ Sebastian, *Total Bullshit ! Au cœur de la post-vérité*, PUF, 2018.
DOMENACH Jean-Marie, *La Propagande politique*, PUF, 1965.
DUPAQUIER Jean-François, *Politiques, militaires et mercenaires français au Rwanda, chronique d'une désinformation*, Khartala, 2014.
DURANDIN Guy, *L'Information, la désinformation et la réalité,* PUF, 1993.
ELKJER NISSEN Thomas, *Social Media's Role in "Hybrid Strategies,"* Riga NATO Strategic Communications Centre of Excellence, 2016.
ELLUL Jacques, *Propaganda: The Formation of men's Attitudes*, Random House, 1965.
EL-OIFI Mohammed, "Désinformation à l'israélienne," *Le Monde diplomatique*, 2005.
EUROPEAN COMMISSION, *A Multi-Dimensional Approach to Disinformation, Report of the Independent High Level Group on Fake News and Online Disinformation*, March 2018.
EUROPEAN VALUES, *The Prague Manual. How to tailor national strategy using lessons learned from countering Kremlin's hostile subversive operations in Central and Eastern Europe,* Kremlin Watch Report, 30 April 2018.

EUvsDISINFO, "The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign," 27 June 2018.
FARWELL James P., "Countering Russian Meddling in US Political Processes," *Parameters,* 48:1, Spring 2018.
FINNISH GOVERNMENT, *Security Strategy for Society. Government Resolution*, The Security Committee, 2 November 2017.
FRANKE Ulrik, *War by non-military means. Understanding Russian Information Warfare,* Swedish Defense Research Agency (FOI), March 2015.
—, *Information Operations on the Internet: A Catalog of Modi Operandi*, FOI Totalförsvarets forskningsinstitut, March 2013.
FRAU-MEIGS Divina, "*Fake news* : engager enfin un débat public confisqué…," *The Conversation,* 8 January 2018.
—, "Développer l'esprit critique contre les 'infaux'," *Courrier de l'UNESCO,* July-September 2017.
FREEDOM HOUSE, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, November 2017.
FRIED Daniel and POLYAKOVA Alina, *Democratic Defense Against Disinformation,* Atlantic Council, Eurasia Center, 2018.
GAGLIANO Giuseppe, *Désinformation, désobéissance civile et guerre cognitive*, VA Press, 2016.
GALEOTTI Mark, "An Unusual Friendship: Bikers and the Kremlin (Op-Ed)," *The Moscow Times*, 19 May 2015.
—, "The Gerasimov Doctrine and Russian Non Linear War," *Blog in Moscow's Shadows*, July 2014.
GARRIGOU Alain, "Ce que nous apprennent les 'fake news'," *Le Monde diplomatique*, February 2018.
GASTINEAU Pierre and VASSET Philippe, *Armes de déstabilisation massive. Enquête sur le business des fuites de données*, Fayard, 2017.
GÉRÉ François, *Dictionnaire de la désinformation*, Armand Colin, 2011.
GILES Keir, *Handbook of Russian Information Warfare*, Fellowship Monograph 9, NATO Defense College Research Division, November 2016.
—, *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, 2016.
GU Lion, KROPOTOV Vladimir and YAROCHKIN Fyodor, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*, A Trendlabs Research Paper, Trend Micro, 2017.
GUEHAM Farid, *Le Fact-Checking : une réponse à la crise de l'information et de la démocratie,* Fondapol, 2017.
HARBULOT Christian, *Les Fabricants d'intox, La guerre mondialisée des propagandes*, Lemieux, 2016.
—, *La France peut-elle vaincre Daech sur le terrain de la guerre de l'information ?* École de guerre économique, 2015.
— and LUCAS Didier, *La Guerre cognitive,* Lavauzelle, 2002.
HARREL Yannick, *La Cyberstratégie russe,* Phebe, 2013.
HARSIN Jayson, "Un guide critique des *Fake News* : de la comédie à la tragédie," *Pouvoirs*, 164, January 2018, p. 99-119.
HELLMAN Maria and WAGNSSON Charlotte, "How can European states respond to Russian information warfare? An analytical framework?," *European Security*, 26:2, 1 March 2017, p. 153-170.

HELMUS Todd C. *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, 2018.
HENIN Nicolas, *La France russe*, Fayard, 2016.
HENROTIN Joseph, *Techno-guérilla et guerre hybride : le pire des deux mondes*, Nuvis, 2014.
HOLEINDRE Jean-Vincent, *La Ruse et la Force. Une autre histoire de la stratégie*, Perrin, 2017.
HOLIDAY Ryan, *Croyez-moi, je vous mens : Confessions d'un manipulateur des médias*, Globe, 2015.
HUYGHE François-Bernard, "Que changent les *fake news* ?," *La Revue internationale et stratégique*, 110, February 2018, p. 79-87.
—, *Fake news : la grande peur*, VA Press, 2018.
—, *DAECH : l'arme de la communication dévoilée*, VA Press, 2017.
—, *La Désinformation : les armes du faux*, Armand Colin, 2016.
—, "Désinformation : armes du faux, lutte et chaos dans la société de l'information," *Sécurité globale*, 2:6, 2016, p. 63-72.
—, KEMPF Olivier and MAZZUCHI Nicolas, *Gagner les cyberconflits : au-delà du technique*, Economica, 2015.
INTERNEWS-UKRAINE, *Words and Wars. Ukraine Facing Kremlin Propaganda,* 2017.
IRELAND (Government of), *First Report of the Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation*, prepared by the Department of the Taoiseach, June 2018.
ISSUE (Institute for Security Studies–European Union), *Strategic Communications. East and South,* Rapport No. 30, July 2016.
JACK Caroline, *Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute, 2017.
JANDA Jakub, "Why the West is Failing to Counter Kremlin Disinformation Campaigns," *The Observer*, 30 December 2016.
JEANGÈNE VILMER Jean-Baptiste, "La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande ?" *Revue Défense Nationale*, 801, June 2017, p. 93-105.
—, *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks*, CSIS Briefs, June 2018.
—, *The Macron Leaks: A Post-Mortem Analysis*, CSIS Europe Program, Washington D.C., September 2018.
JULIEN Claude (ed.), "L'art de la désinformation," *Le Monde diplomatique*, includes 13 articles, May 1987.
KAJIMOTO Masato and STANLEY Samantha (eds.), *Information disorder in Asia—Overview of misinformation ecosystem in India, Indonesia, Japan, the Philippines, Singapore and South Korea,* Journalism & Media Studies Centre of the University of Hong Kong, 12 April 2018.
KIRSCH Hervé (col.), "Guerre de l'information et opérations militaires," *Conflits*, 18, July-August-September 2018, p. 58-61.
KREKÓ Péter *et al.*, *The Weaponization of Culture: Kremlin's traditional agenda and the export of values to Central Europe,* Political Capital Institute, 4 August 2016.
KRÓL Aleksander, "Russian Information Warfare in the Baltic States—Resources and Aims," *The Warsaw Institute Review*, 3/2017.
KOYRÉ Alexandre, *Réflexions sur le mensonge*, Allia, 2004.
LANGE-IONATAMISVILI Elina (ed.), *Russia's Footprint in the Nordic-Baltic Information Environment,* NATO Strategic Communications Centre of Excellence, 2016-2017.

LAZER David *et al.*, *Combating Fake News: An Agenda for Research and Action*, Harvard University, 2017.

LE DRIAN Jean-Yves, Minister of Europe and Foreign Affairs, *Discours de clôture de la conférence internationale "Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information,"* Paris, 4 April 2018.

LENOIR Théophile, *Désinformation : la faute (seulement) aux réseaux sociaux ?,* Institut Montaigne, 2018.

LEWANDOWSKY Stephan, ECKER Ullrich K. H. and COOK John, "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era," *Journal of Applied Research in Memory and Cognition*, 6:4, 2017, p. 353-369.

LEWANDOWSKY Stephan *et al.*, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest*, 13:3, December 2012, p. 106-31.

LIMONIER Kevin, "Internet russe, l'exception qui vient de loin," *Le Monde diplomatique*, August 2017, p. 22-23.

—, "La Russie dans le cyberespace : représentations et enjeux," *Hérodote*, 152-153, 1st and 2nd trimesters 2014, p. 140-160.

LIPPMAN Walter, *Public opinion*, Greenbook Publications, 1922.

LUCAS Edward and POMERANTSEV Peter, *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*, CEPA's Information Warfare Project/Legatum Institute, August 2016.

LUCAS Edward and NIMMO Ben, *Information Warfare: What Is It and How to Win It?*, CEPA Infowar Paper 1, November 2015.

LUTSEVYCH Orysia, *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood,* Chatham House, April 2016.

MACRON Emmanuel, President of French Republic, *Discours du président de la République Emmanuel Macron à l'occasion des vœux à la presse,* 4 January 2018.

MARANGÉ Céline, *Les Stratégies et les pratiques d'influence de la Russie,* IRSEM *Étude* 49, March 2017.

MARINI Lorenzo, "Fighting fake news: Caught between a rock and a hard place," *European Council on Foreign Relations*, March 2018.

MATTIS James N. and HOFFMAN Frank, "Future Warfare: The Rise of Hybrid Wars," *Proceedings Magazine* (U.S. Naval Institute), 131:11, November 2005, p. 18-19.

MCGEEHAN Timothy P., "Countering Russian Disinformation," *Parameters,* 48:1, Spring 2018.

MCKELVEY Fenwick and DUBOIS Elizabeth, *Computational Propaganda in Canada: the Use of Political Bots,* Computational Propaganda Research Project, University of Oxford, Working Paper 2017.6, 2017.

MÉGRET Maurice, *La Guerre psychologique*, PUF, "Que sais-je," 1963.

—, *L'Action psychologique,* Arthème Fayard, 1953.

MERCIER Arnaud (ed.), *Fake news et post-vérité : 20 textes pour comprendre la menace,* The Conversation France, 2018.

MILO Daniel and KLINGOVÁ Katarína, *Countering Information War Lessons Learned from NATO and Partner Countries: Recommendations and Conclusions*, Globsec, 2016.

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE, Direction du numérique pour l'éducation, *Infopollution : Hoax, rumeurs et désinformation*, Vol. 1, 2016.

MOROZOV Evgeny, *To Save Everything, Clich Here: The Folly of Technological Solutionism*, PublicAffairs, 2014.

—, "Les vrais responsables des fausses nouvelles," *Le Monde diplomatique,* 2017.

NATO STRATCOM COE & THE KING'S COLLEGE LONDON, *Fake News. A Roadmap,* February 2018.

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, *Internet Trolling as a tool of hybrid warfare: the case of Latvia. Results of the study*, 2016.

NIMMO Ben *et al.*, "Hashtag Campaign: #MacronLeaks. Alt-right attacks Macron in last ditch effort to sway French election," *Atlantic Council's Digital Forensic Research Lab*, 6 May 2017.

NOCETTI Julien, "Comment l'information recompose les relations internationales," *in* MONTBRIAL Thierry de and DAVID Dominique (eds.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 138-144.

—, "Internet renforce-t-il l'autoritarisme ?" *in* MONTBRIAL Thierry de and DAVID Dominique (eds.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 162-166.

—, "Contest or Conquest: Russia and Global Internet Governance," *International Affairs,* 91:1, 15 January 2015, p. 111-130.

NYSSEN Françoise, Minister of Culture, *Discours prononcé à l'occasion des Assises internationales du journalisme,* Tours, 15 March 2018.

NYST Carly and MONACO Nick, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, Institute for the Future, 2018.

O'CARROLL Eoin, "How information overload helps spread fake news," *The Christian Science Monitor,* 27 June 2017.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections*, Washington DC, January 2017.

OH Sarah and ADKINS Travis L., *Disinformation Toolkit*, InterAction, June 2018.

O'NEIL Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Crown, 2016.

PACEPA Ion Mihai (general), *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, 2013.

PALMERTZ Björn, *Theoretical Foundations of Influence Operations: A Review of Relevant Psychological Research*, Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, n.d.

PAMMENT James *et al.*, *Countering Information Influence Activities: The State of the Art,* Department of Strategic Communication, Lund University, research report, version 1.4, 1 July 2018.

PARISER Eli, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2011.

PASQUALE Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information,* Harvard University Press, 2015.

PAUL Christopher and MATTHEWS Miriam, *The Russian "Firehose of Falsehood" Propaganda Model—Why It Might Work and Options to Counter It*, Expert insights on a timely policy issue, RAND Corporation, 2016.

PÉTINIAUD Louis and LIMONIER Kevin, "Cartographier le cyberespace : le cas des actions informationnelles russes en France," *Les Champs de Mars*, 30, Vol. 2 (supplement), 2018, p. 317-326.

POLYAKOVA Alina and BOYER Spencer P., *The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition,* Brookings, March 2018.

POMERANTSEV Peter, *Nothing is True and Everything is Possible: The Surreal Heart of the New Russia*, PublicAffairs, November 2015.

POMERANTSEV Peter and WEISS Michael, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Interpreter, a project of the Institute of Modern Russia, 2014.

POPPER Karl, *Open Society and Its Enemies*, *Vol. II: The High Tide of Prophecy* (5th ed.), Princeton University Press, 1971.

QUESSARD Maud, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information ?*, IRSEM Research Note 54, 30 April 2018.

REPORTERS WITHOUT BORDERS, *Online Harassment of Journalists: Attack of the trolls*, 2018.

RILEY Michael, ETTER Lauren and PRADHAN Bibhudatta, *A Global Guide to State-Sponsored Trolling*, Bloomberg, 19 July 2018.

RIOCREUX Ingrid, *La Langue des médias : destruction du langage et fabrication du consentement*, L'Artilleur, 2016.

ROBINSON Linda *et al.*, *Modern Political Warfare. Current Practices and Possible Responses,* RAND Corporation, 2018.

ROSENFELD Louis, MORVILLE Peter and ARANGO Jorge, *Information Architecture*, O'Reilly, 2015.

SALAÜN Jean-Michel and HABERT Benoît, *Architecture de l'information : Méthodes, outils, enjeux,* De Boeck, 2015.

SANOVICH Sergey, *Computational Propaganda in Russia—The Origins of Digital Misinformation*, Working Paper, Computational Propaganda Research Project, Oxford Internet Institute, 2017.

SCHMITT Olivier, *Pourquoi Poutine est notre allié. Anatomie d'une passion française,* Hikari Éditions, 2017.

—, "'Je ne fais que poser des questions'. La crise épistémologique, le doute systématique et leurs conséquences politiques," *Temps présents,* 15 June 2018.

SCHOEN Fletcher and LAMB Christopher J., *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Center for Strategic Research, Institute for National Strategic Studies National Defense University, June 2012.

SÉNÉCAT Adrien, "Le Décodex, un premier pas vers la vérification de masse de l'information," *Le Monde*, 2017.

SERMONDADAZ Sarah, "Google et Facebook déclarent la guerre aux fausses informations. Avec quels moyens ?," *Sciences et Avenir*, 2016.

SERRES Alexandre, *Dans le labyrinthe : évaluer l'information sur internet,* C&F Éditions, 2012.

SMYRNAIOS Nikos, *Les GAFAM contre l'internet : une économie politique du numérique,* Institut national de l'audiovisuel, 2017.

STIEGLER Bernard *et al.*, *La toile que nous voulons*, FYP éditions, 2017.

SUNSTEIN Cass R. and VERMEULE Adrian, "Conspiracy Theories: Causes and Cures," *The Journal of Political Philosophy*, 17:2, 13 April 2009, p. 202-227.

SUN TZU, *L'Art de la guerre*, Mille et Une Nuits, 1972.

SZWED Robert, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, NATO Strategic Communications Centre of Excellence, May 2016.

TATHAM Steve, *The Solution to Russian Propaganda Is Not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate Its Effects in Targeted Populations*, Policy paper, National Defence Academy of Latvia, Center for Security and Strategic Research, July 2015.

TENENBAUM Élie, *Le Piège de la guerre hybride*, Focus stratégique 63, IFRI, October 2015.

THE INTEGRITY INITIATIVE, *Framing Russian meddling in the Catalan question*, October 2017.

THE HAGUE CENTRE FOR STRATEGIC STUDIES, *Inside the Kremlin House of Mirrors. How Liberal Democracies can Counter Russian Disinformation and Societal Interference,* 2017.

THE WARSAW INSTITUTE REVIEW, *Report: Disinformation in CEE,* 3, special edition, 2017.

THOM Françoise, "La désinformation," *Commentaire*, 40, Winter 1987-88, p. 675-680.

TOUCAS Boris, "Exploring the Information-Laundering Machinery: The Russian Case," Commentary, CSIS, 31 August 2017.

—, *"L'Affaire russe" : la démocratie américaine ébranlée*, Notes de l'IFRI, Potomac Papers 32, December 2017.

TUFEKCI Zeynep, "YouTube, the Great Radicalizer," *The New York Times*, 10 March 2018.

TWOREK Heidi, "Responsible Reporting in an Age of Irresponsible Information," Alliance for Securing Democracy (GMF) Brief 2018, 009, March 2018.

UK HOUSE OF COMMONS (Digital, Culture, Media and Sport Committee), *Disinformation and "fake news": Interim Report, Fifth Report of Session 2017-19*, 29 July 2018.

US DEPARTMENT OF JUSTICE, *Report of the Attorney General's Cyber Digital Task Force*, July 2018.

VAISSIÉ Cécile, *Les Réseaux du Kremlin en France*, Les Petits Matins, 2016.

VANDERBIEST Nicolas, "Les institutions démocratiques : l'influence des réseaux sociaux durant une élection présidentielle," *in* TAILLAT Stéphane, CATTARUZZA Amaël and DANET Didier (eds.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 181-188.

VENTRE Daniel (ed.), *Cyberwar and Information Warfare,* Wiley, 2011.

VICHOVA Veronika and JANDA Jakub (eds.), *The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, European Values, Kremlin Watch Report, 30 April 2018.

VOLKOFF Vladimir, *Désinformation, flagrant délit*, Éd. du Rocher, 1999.

—, *Petite Histoire de la désinformation*, *Du cheval de Troie à Internet*, Éd. du Rocher, 1999.

—, *La Désinformation vue de l'Est*, Éd. du Rocher, 2007.

VOSOUGHI Soroush, ROY Deb and ARAI Sinan, "The spread of true and false news online," *Science*, 359:6380, 9 March 2018, p. 1146-1151.

VOLKOFF Vladimir, POLIN Claude and MUCCHIELLI Roger, *La Désinformation : arme de guerre,* L'Âge d'homme, 1986.

WALTZMAN Rand, *The Weaponization of Information—The Need for Cognitive Security*, RAND Corporation, 2017.

WARDLE Claire and DERAKHSHAN Hossein, *Information disorder: Toward an interdisciplinary framework for research and policy making*, European Council, 2017.

WATZLAWICK Paul, *La Réalité de la réalité. Confusion, désinformation, communication*, Éd. du Seuil, "Points," 1978.

French speaking TV/radio sources

2016 dans les médias : post-vérité, "fake news" et crise du "fact checking," France Culture, 31 December 2016.
"Fact-checking" : fondement du journalisme ou miroir aux alouettes ?, France Culture, 10 November 2012.
Fake news : jeux de mains, jeux de vilains, 28 minutes, Arte, 2017.
Fake news : le vrai du faux de Frédéric Lordon, France Culture, 19 January 2018.
Guerre de l'info : au cœur de la machine russe, Paul Moreira, Arte thema, 2018.
La Désinformation et les fabricants d'intox, 5e conférence Puissance 21, École de guerre économique, March 2016.
Mensonge ou vérité, comment repérer les "fake news" ?, Xenius, Arte, 2017.
Moscou : l'info dans la tourmente, Alexandra Sollogoub*,* Arte, 2017.
Poutine contre les USA (1 and 2), Michael Kirk, Arte thema, 2017.
Runet, la bataille de l'Internet russe, Arte, web serie, 10 episodes, 2018.

PRESENTATION OF THE AUTHORS

Jean-Baptiste Jeangène Vilmer is director of the Institute for Strategic Research (IRSEM) at the Ministry for the Armed Forces, after having served as Policy officer on "Security and Global Affairs" at the Policy Planning Staff (CAPS) of the Ministry for Foreign Affairs (2013-2016). Trained in three disciplines—philosophy (Bachelor, Master, Ph.D.), law (Bachelor, LL.M., post-doctorate) and in political science (doctorate)—, he held positions at the Faculty of Law at McGill University in Canada (2011-2013), at the department of War Studies of King's College in London (2010-2011), at the MacMillan Center for International and Area Studies of Yale University (2008-2009), at the French Embassy in Turkmenistan (2007-2008) and at the University of Montreal (2005-2007). Auditor of the 68th national session on "Defense Policy" of the Institute for Higher National Defense Studies (IHEDN), member of the Academic Advisory Board of the NATO Defense College, lecturer at Sciences Po and the ENS Ulm, he has authored some one hundred articles and about twenty books, and has received several awards (including the "Maréchal Foch" prize from the Académie française in 2013, and being nominated a Munich Young Leader in 2018). On the topic of information manipulation, he has also written a CSIS report (*The Macron Leaks: A Post-Mortem Analysis*, forthcoming in the Fall 2018).

Contact: jbjv.com / jean-baptiste.jeangene-vilmer@irsem.fr / Twitter @jeangene_vilmer

Alexandre Escorcia, career diplomat, is the Deputy Head of Policy planning (CAPS) at the Ministry for Europe and Foreign Affairs. Previously an adviser to the Minister for Foreign Affairs and International Development Jean-Marc Ayrault (2016-2017), he also served at the French embassy in Germany (2013-2016) and as an exchange diplomat to the German Ministry of Foreign Affairs (2012-2013). Before working as Deputy Political Advisor to NATO's first French Supreme Allied Commander Transformation in Norfolk, Virginia, USA (2009-2012), he had been a desk officer at the Directorate of Strategic Affairs, Security and Disarmament and the Directorate for Political Affairs (Foreign and Security Policy) of the Ministry of Foreign Affairs (2005-2009). An alumnus of the École normale supérieure and graduate from Sciences Po Paris, he has authored publications on European foreign policy and defense and on NATO.

Marine Guillaume is a Policy officer on "Cybersecurity and Digital Affairs" at the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and a lecturer at the École Polytechnique. Holding a doctorate in Political Science from Columbia University and Sciences Po Paris, she was previously both a Lecturer at the School of International Public Affairs (SIPA), and a Lecturer at Sciences Po Paris. She was also an Associate Consultant for Bain & Company (May 2015–August 2016).

Janaina Herrera is a career diplomat, and was until recently a Policy officer on "Multilateral Affairs, Latin America and Human Rights" at the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs (2015-2018). She is now the French Consul General in Alexandria, Egypt. A graduate from Sciences Po and alumnus from the École Nationale d'Administration (ENA), she founded an independent think tank in Beirut dedicated to research on the Arab Spring (2011-2015), after having notably worked as the First Secretary at the French embassy in Lebanon, in charge of Regional and Multilateral issues (2007-2010), and as a desk officer for the Department for the EU Common Foreign Security Policy (CFSP) and for the Departement of the United Nations and International Organizations on environmental issues.

Acknowledgments

We would like to warmly thank all of our interlocutors, in France and abroad, as well as our colleagues who were eager to help us in the preparation of this report, through specific contributions or careful proofreading (Jean-Pierre Bat, Emmanuel Bloch, Lucie Delzant, Emmanuel Dreyfus, Jean Dubosc, Émilien Legendre, Kevin Limonier, Benjamin Pajot, Maud Quessard, Marie Robin, Boris Toucas), as well as Élodie Ternaux for the cover, Chantal Dukers for the mockup, and Mickaela Churchill, Aziliz Gouez and Diana Reisman for the English translation.

Information manipulation is not a new phenomenon, but its renewed media attention has resulted from a combination of two factors: the unprecedented capacity of the internet and social networks to diffuse information and render it viral, and the crisis of confidence that our democracies are currently experiencing, which devalues public debate to such an extent that the notion of truth itself is relativized. This phenomenon has manifested itself in recent years through various electoral interferences which threaten national security. The Policy Planning Staff (CAPS) and the Institute for Strategic Research (IRSEM) have thus joined forces to study this issue.

This report is the product of field research (around a hundred interviews in twenty countries) in order to develop a better understanding of the nature of the problem and identify good practices put in place by States and civil society. Our research is equally based on the abundant scientific literature on the subject.

Precluding the vague and controversial notion of fake news, among others (propaganda, influence, disinformation, etc.) which are often either too narrow or too broad to apply to this specific issue, this report uses the term "information manipulation" to describe the intentional mass dissemination of false or biased news for hostile political ends.

We begin by exploring the causes of information manipulation, which exist partly at the level of the individual and are rooted in psychology and epistemology (cognitive weaknesses and a crisis of knowledge). Causes also exist at the collective level as information manipulation is linked to our social lives (a crisis of trust in institutions, a crisis of the press and disillusionment with the digital world). We then proceed to identify the beneficiaries of these activities, i.e. the actors carrying out information manipulation. We focus specifically on States that manipulate information outside their territory or, in other words, who interfere in the domestic affairs of other States.

This report then proceeds to examine the consequences of information manipulation, by exploring the distinctive features of recent information manipulation campaigns and identifying some common characteristics—both in terms of vulnerability factors and the methods employed. We also explore information manipulation in regions other than the post-Soviet space, Europe and North America—which are the best known—by turning our attention to several case studies in the Middle East, Africa and Latin America.

In the third part, devoted to the responses to information manipulation, we summarize the countermeasures adopted by all actors: States, international organizations, civil society and private actors. We begin by looking at the interference attempts in the latest French presidential election ("Macron Leaks") and the lessons learned from this event.

To conclude, this report attempts to anticipate future challenges—technological challenges, future trends in Russian "information warfare" and possible future scenarios. We propose 50 recommendations, operating on the assumption that information manipulation will remain a problem in the future and that it will constitute a long-term challenge for our democracies. In the face of this challenge, democracies must provide a participatory, liberal response that respects fundamental rights.

Authors: Jean-Baptiste Jeangène Vilmer, researcher, director of the IRSEM; Alexandre Escorcia, diplomat, deputy head of the CAPS; Marine Guillaume, researcher and policy officer at the CAPS and Janaina Herrera, diplomat, previously policy officer at the CAPS.

The Policy Planning Staff (CAPS) is the Center for analysis, prevision and strategy of the Ministry for Europe and Foreign Affairs. The IRSEM is the Institute for Strategic Research of the Ministry for the Armed Forces.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
MINISTÈRE DES ARMÉES

August 2018.